УДК 004.056

METHODS FOR ASSESSING THE SECURITY OF COMMUNICATION SYSTEMS FOR SPECIAL PURPOSES

Korchynskii V.V., Kildishev V.I., Berdnikov A.M.

O.S. Popov Odessa national academy of telecommunications,
1 Kuznechna St., 65029, Ukraine, Odessa.
vladkorchin@ukr.net

МЕТОДИ ОЦІНКИ ЗАХИЩЕНОСТІ СИСТЕМ ЗВ'ЯЗКУ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Корчинський В. В., Кільдішев В.Й., Бердніков О.М.

Одеська національна академія зв'язку ім. О.С. Попова,
65029, Україна, м. Одеса, вул. Кузнечна, 1.
vladkorchin@ukr.net

МЕТОДЫ ОЦЕНКИ ЗАЩИЩЁННОСТИ СИСТЕМ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Корчинский В. В., Кильдишев В.Й., Бердников А.М.

Одесская национальная академия связи им. А.С. Попова,
65029, Украина, г. Одесса, ул. Кузнечная, 1.
vladkorchin@ukr.net

Abstract. In the conditions of radio electronic conflict it is actual to create special-purpose communication systems able to provide high security of communication channel from means of radio technical reconnaissance and unauthorized access of the enemy. Increasing the protection of such systems is possible when using several levels of protection of transmitted information. Each level of protection is equipped with a certain arsenal of forming signal structure or data transformation. A system of assessing the effectiveness of information protection methods is suggested in this paper. As the main efficiency criteria, the secure indicators are chosen: noise immunity; structural and energy secrecy. The analysis of influence of methods of increasing energy and structural stealth on the noise immunity of the communication system, taking into account changes in the frequency and energy efficiency of the channel is carried out. The proposed system of assessments allows us to carry out the comparative analysis of information protection methods in the channel, taking into account the customer's requirements for noise immunity and data transmission.

Key words: security, secrecy, noise immunity, electronic counteraction, information protection, channels.

Анотація. В умовах радіоелектронного конфлікту актуальним є створення систем зв'язку спеціального призначення, здатних забезпечувати високу захищеність каналу зв'язку від засобів радіотехнічної розвідки і несанкціонованого доступу противника. Підвищення захищеності таких систем можливо при використанні декількох рівнів захисту переданої інформації. Кожен рівень захисту забезпечений певним арсеналом формування сигнальних конструкцій або перетворення даних. У статті запропонована система оцінок ефективності методів захисту інформації, що передається. Як основні критерії ефективності обрані показники завадозахищеності: завадостійкість; структурна й енергетична прихованість. Проведено аналіз впливу методів підвищення енергетичної та структурної прихованості на завадостійкість системи зв'язку з урахуванням зміни частотної та енергетичної ефективності каналу. Запропонована система оцінок дозволяє проводити порівняльний аналіз методів захисту інформації в каналі з урахуванням вимог замовника до завадостійкості і прихованості передавання.

Ключові слова: захищеність, прихованість, завадостійкість, радіоелектронна протидія, захист інформації, канал.

Аннотация. В условиях радиоэлектронного конфликта актуальным является создание систем связи специального назначения, способных обеспечивать высокую защищённость канала связи от средств радиотехнической разведки и несанкционированного доступа противника. Повышение защищённости таких систем возможно при использовании нескольких уровней защиты передаваемой информации. Каждый уровень защиты снабжен определённым арсеналом формирования сигнальных конструкций или преобразования данных. В работе предложена система оценок эффективности методов защиты информации. В качестве основных критериев эффективности выбраны показатели помехозащищённости: помехоустойчивость; структурная и энергетическая скрытность. Проведен анализ влияния методов повышения энергетической и структурной скрытности на помехоустойчивость системы связи с учётом изменения частотной и энергетической эффективности канала. Предложенная система оценок позволяет проводить сравнительный анализ методов защиты информации в канале с учётом требований заказчика к помехоустойчивости и скрытности передачи.

Ключевые слова: защищённость, скрытность, помехоустойчивость, радиоэлектронное противодействие, защита информации, канал.

Communication systems for special purposes and control (SPC) are designed for interaction between military units in conditions of radio electronic warfare (REW) and have to ensure high channel security from radio technical reconnaissance (RTR) and unauthorized access (UAA). Characteristically the most methods of information protection [1] from UAA are implemented mainly at the upper levels of the OSI reference model using various cryptography systems (GOST 28147-89, AES, DES, etc.). However, the process of signal transmission is accompanied with certain risks for its detection and interception. Therefore, in order to counteract RTR means, information protection methods have recently been developed to cover the lower layers of the OSI model: channel and physical [2, 3]. Obviously that increasing the number of levels of protection of transmitted information allows to improve the security of SPC communication systems in general. Taking into account the task to minimize the security risks of transmitted information in the conditions of radio electronic conflict, each level of protection has to pose its own arsenal forming of signal structure and data transformation.

It is known [3] that the efficiency of the information protection methods at the channel and physical levels can be estimated using noise security indicators: secrecy and noise immunity. When choosing methods for information protection, it is necessary to take into account the mutual influence between noise immunity and various indicators of secrecy: energy, structural, information; the nature of REW and the forecast of possible actions of the opposing side [2]. Thus, the search of effective system of assessments for information protection methods in connection with the indicators of noise immunity and secrecy is an actual task.

The aim of the article is to develop a security assessment system for information transmission methods based on secrecy and noise immunity.

The system of security assessments for information protection methods should be implemented on the basis of reasonable criteria of the efficiency that characterize the level of counteraction RTR and UAA. In the course of the REW, various scenarios of counteraction against SPC communication systems are possible. In the simplest case, it is proposed the detection of radio signal by means RTR of the enemy and suppression targeted interference. This counteraction scenario for the opposing side contains the minimum number of tasks.

The more difficult scenario of counteraction requires disclosing the semantic content of confidential information with the greater number of solved tasks: detection of the signal and its interception (recording on a storage medium); pattern recognition signals; message decryption. This scenario can have different development options, taking into account the ultimate goal of counteraction:

1) listening to the message;

2) listening to the message and modifying it aimed to simulate the operation of SPC communication system transmitter.

Depending on the scenario of REW of the enemy, at the stage of designing SPC communication system, a variety of types of stealth can be realized for the task of counteraction: energy, structure, information.

Energy secrecy is realized at the expense of signal structures that possess "masking" properties, which complicate the process of their detection in the radio channel by the RTR enemy. For this task various methods of spreading information narrowband signal range are used [3]: random restructuring of the operating frequency (RROF); direct spreading of the spectra` random sequences (SRS); combined spectrum expansion. The narrowband signal with the signal base $B_{nb} \approx 1$ is converted into a broadband signal with a base $B_{wb} >> 1$.

Obviously the masking effect from such spreading of spectrum is observed when the amplitude of useful signal frequency decreases to the level of the Gaussian noise in the channel.

Let us estimate the relationship between the condition of ensuring the required reliability of transmission and the energy secrecy of signal structures for the method of direct spreading spectrum SPS. Consider Shannon's theorem on the channel capacity [3]:

$$C = \Delta F \log_2\left(1 + \frac{P_s}{P_n}\right), \tag{1}$$

where ΔF – is the frequency band for data transmission; P_s – power of the signal at the output of transmitter; P_n – power of interference in the channel. It follows from (1) that theoretically information on the channel can be transmitted at any speed that does not exceed the capacity C and with any given reliability.

As can be seen from (1) to keep the transmission rate and provide energy secrecy can be achieved by spreading narrowband signal and decreasing the amplitude of the carrier wave to the level Gaussian noise in the channel, i.e.

$$\begin{cases} B_{wb} = T\Delta F \to \infty, \\ P_s / P_n \to 1. \end{cases} \tag{2}$$

Provided that

$$P_s / P_n < 1, \tag{3}$$

the transmission is carried out by signal structures which amplitude is less than the gaussian noise, i.e. the useful signal becomes "less noticeable" for its detection by means of PTP. Thus, condition (3) shows the possibility of realizing the maximum energy concealment of signal structures.
Obviously conditions (2) and (3) will have force in case providing required reliability and data transmission rate.

Let us find the relationship between the reliability of transmission and conditions (2) and (3), which ensure the energy secrecy of signal structures. From the second part of Shannon's theorem (1) it follows that there is such noise immunity code that is provided high reliability of the transmitted data.

Equity (2) and (3) can prove it if presents random sequence with which the direct extension spectrum of a narrowband signals is carried out as binary error-correcting code elements:

$$n = k + r, \tag{4}$$

where k and r is the number of information and verification elements, respectively. According to the coding theorem, provided that

$$n \to \infty \tag{5}$$

the number of information elements k also tends to infinity, with an insignificant increase in the number of verification elements r. At the same time corrective capacity of code is increased. Suppose that the increase in the number of elements n in a code block on the intervals` time $T = nt_0$ is carried out by adding elements r and decreasing the duration of the elementary premise t_0, then

$$t_0 > t_0^*, \tag{6}$$

where t_0^* is the duration of the sending after the noise immunity coding. Taking into account the code rate $\gamma_к = k/n$ duration

$$t_0^* = \gamma_{cr} t_0. \quad (7)$$

Obviously a decrease in the pulse duration reduces its energy, and the transmission rate decreases in n/k time. Provided that the bandwidth channel ΔF is unlimited, the reliability of the transmission is increased. For clarity table 1 shows the parameters of the cyclic code. It is seen that with the increasing length code block n, corrective ability of code, evaluating by the minimum code distance d_0, increases. At the same time the code rate

$$\gamma_k \quad (8)$$

and the proportion of test elements decreases. The base of the broadband signal coincides with the number of elements in the spreading sequence spectrum, therefore, taking into account (2) and (5)

$$B_{wb} = n \to \infty. \quad (9)$$

Thus, the reliability of the transmission increases with the broadening of the spectrum narrowband signal and depends on the size of the base B_{wb}, which is that we had to prove.

Table 1 – Parameters of the cyclic code

№	n	k	r	d_0	γ_k
1	7	4	3	3	0,571
2	15	11	4	3	0,733
3	31	26	5	3	0,839
4	63	51	12	5	0,810
5	127	113	14	5	0,890
6	255	231	24	7	0,906
7	511	475	36	9	0,930

The positive relationship between the reliability of transmission and the energy secrecy of signal structures in case of narrowband signal spectrum is allowed to conclude that it is expedient to use signals with a large base.

In real communication systems with code division channels as allowed combinations for spreading the narrowband signal spectrum are used orthogonal SPS, for example, the Walsh number is commensurate with the signal base B_{wb}.

Of the total common set of combinations $N_{com} = 2^n$, has chosen only $N_{SPS} = n - 1$ mutually orthogonal SPS. The code distance between any pair of the Walsh sequence unlike the cyclic codes corresponds to the fixed value

$$d_0 = \frac{n}{2}. \quad (10)$$

Multiplicity of error detection for such sequences is $t_0 = d_0 - 1$. Theoretically it means that at the correlation reception for the correct recognition SPS is possible provided that number of distorted bits t_0^* which does not exceed the value of $n/2$.

Detection of signal by means of RTR signifies overcoming the level protection of channel on the physical level, i.e. the problem of energy secrecy is solved. In the second scenario of counteraction in order to disclose the semantic content of the intercepted message, it is first necessary to recognize the design of signal structures. In [6] the method of estimating the potential structural secrecy of signals is described which does not require knowledge of the algorithms` processing by UAA station. Structural secrecy of signals is determined by the number of binary measurements (bin. means), which have to be performed for the task of revealing the structure signal:

$$S = \log_2 A, \quad (11)$$

where A is ensemble of realizations determined by the number of all possible values of signal parameters. These parameters can be carrier frequency, type of modulation, structure of code, time of the arrival signal. Thus, the structural secrecy of signal structures depends on the methods of constructing the particular signal design. Obviously for increasing structural secrecy transmitter should use as much as bigger ensemble of using signals with time-varying parameters.

Increasing the number of signal structures is probably due to the more complex types of modulation of BPSK (FM-2), 4-QAM (KAM-4), 8-QAM, 16-QAM, 32-QAM, etc. Fig. 1 shows the dependence of the structural secrecy S of QAM modulation system on multi-positioning M .

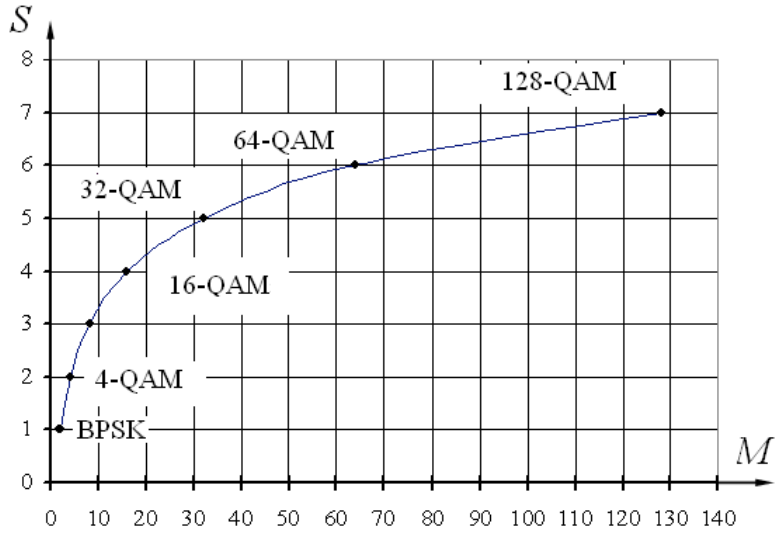

Figure 1 – Dependence of the structural secrecy of modulation types on their multi-position M

Obviously this way increasing structural secrecy leads to the change in ratio resources used of communication channel [3]. The transition to multi-position modulation systems improves the channel's frequency efficiency

$$\gamma = \frac{R}{\Delta F}, \tag{12}$$

however it reduces its energy efficiency

$$\beta = \frac{R}{h_0^2}, \tag{13}$$

where R – the information transfer rate; $h_0^2 = P_s / N_0$ – the ratio of the average signal power at the receiver input to the energy spectrum of the additive white Gaussian noise N_0.

Let us estimate the effect of the redistribution of channel resources on the reliability of the transmitted information and structural secrecy. Fig. 2 shows the results of computer simulation of signals BPSK, 8-QAM, 16-QAM, 32-QAM in ABGS channel.

It can be seen from the dependencies when using more complex types of modulation that the probability error of the binary symbol p_0 decreases. Thus, this method of increasing structural secrecy reduces the reliability of transmission. Further increase in the structural secrecy of signal structures is possible due to the complicating shape of the modulating signal. In paper [3] concerning this problem it was proposed to use timer signal structures in combination with various methods of spreading the signal spectrum [4, 5]. As a rule the security of transmission based on energy secrecy is realized by expanding the spectrum of the initial information signal which worsens the frequency efficiency of the channel, but improves its energy efficiency. Obviously the inconsistency of these indicators channel has just allowed us to solve the problem of extending the power increasing energy secrecy transmission and also improves electromagnetic compatibility with other radio transmitting devices.

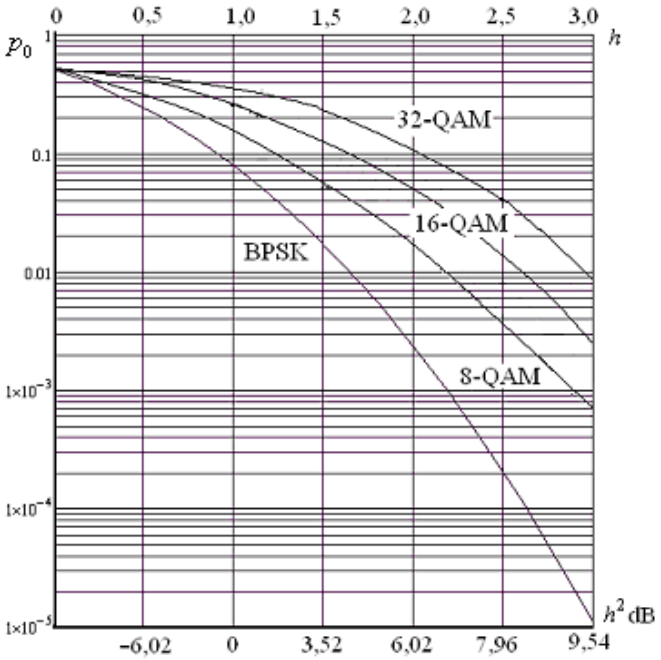

Figure 2 – Dependencies of the error probability of systems with BPSK, 8-QAM , 16-QAM, 32-QAM от h_0^2

Thus, we can formulate the following system of assessing the security of transmission methods, taking into account channel resources:

1) the most energy secrecy is the transmission method which for the given bandwidth of the broadband signal ΔF and the required reliability of the transmission provides a lower signal-to-noise ratio h_0^2:

$$\min h_0^2 = \mathrm{E}\{\Delta F; P_{ue}(n)\}, \tag{14}$$

where $P_{ue}(n)$ – is the probability of an undetected error in the code block n;

2) the most potential structural secrecy is the method for generating signal structures which at the given time interval for constructing signal structures T_{ss} and the required reliability of transmission enables the synthesis of the larger number of combinations of A:

$$\max \mathrm{A} = S\{T_{ss}; P_{ue}(n)\}. \tag{15}$$

It can be seen from (12) and (13) that the essential potential for increasing the secrecy of radio technical objects is the combination of the transmission signal parameters in the time-frequency space which makes it possible to create and use various methods of spectral protection of information with complex structure of signal structures and large broadband signal bases B_{wb}.

Conclusion. The proposed system of assessing the security of communication systems SPC allows us to make a comparative analysis of methods protecting transmitted information based on secrecy and noise immunity indicators, taking into account the expended channel.

REFERENCES:

1. Shangin A.I. Information security of computer systems and networks / Shanguin A.I. – M.: ID Forum: IFRA-M, 2008. – 416 p.
2. Kupriyanov A.I. Theoretical foundations of electronic warfare/ A. I. Kupriyanov, A. V. Sakharov. – Moscow: The University Book, 2007. – 356 p.
3. Noise immunity of radio communication systems with spreading of signals spectrum by modulation of random sequence carrier [V. I. Borisov, V. M. Zinchuk, A. Ye. Limarev i dr.]; ed. V.I Borisov. – M.: Radio and Communication, 2003. – 640 p.
4. Zakharchenko N. V. Multiuser access in transmission systems with chaotic signals / N. V. Zakharchenko, V. V. Korchinsky, B. K. Radzimovsky // Eastern European Journal of Advanced Technologies. – 2011. – No. 5/9 (53). – P. 26–29.

5. Zakharchenko N.V. Increase the secrecy transmission of confidential information on the basis of chaotic signals and timer signal structures / N.V. Zakharchenko, V.V. Korchinsky, B.K. Radzimovsky, V.I. Kildishev // East-European Journal of Advanced Technologies. – 2012. – No. 3/9 (57). – P. 45–49.
6. Zakharchenko N. Information security of Time-Controlled Signals in Confidential Communication Systems / N. Zakharchenko, V. Korchinsky, B. Radzimovsky // Modern problems of radio engineering, telecommunications and computer science: XI International Conference TCSET 2012, (Lviv-Slavske, 21-24 february 2012). – Lviv: Publishing House of Lviv Polyteshnic, 2012. – P. 317.

ЛИТЕРАТУРА:

1. Шаньгин А.И. Информационная безопасность компьютерных систем и сетей / Шаньгин А.И. – М.: ИД «Форум»: ИФРА-М, 2008. – 416 с.
2. Куприянов А.И. Теоретические основы радиоэлектронной борьбы / А. И. Куприянов, А. В. Сахаров. – М.: Вузовская книга, 2007. – 356 с.
3. Помехозащищенность систем радиосвязи с расширением спектра сигналов модуляцией несущей псевдослучайной последовательностью / [В. И. Борисов, В. М. Зинчук, А. Е. Лимарев и др.]; под ред. В. И. Борисова. – М.: Радио и связь, 2003. – 640 с.
4. Захарченко Н. В. Многопользовательский доступ в системах передачи с хаотическими сигналами / Н. В. Захарченко, В. В. Корчинский, Б. К. Радзимовский // Восточно-Европейский журнал передовых технологий. – 2011. – № 5/9(53). – С. 26–29.
5. Захарченко Н.В. Повышение скрытности передачи конфиденциальной информации на базе хаотических сигналов и таймерных сигнальных конструкций / Н.В. Захарченко, В.В. Корчинский, Б.К. Радзимовский, В.И. Кильдишев // Восточно-Европейский журнал передовых технологий. – 2012. – № 3/9 (57). – С. 45–49.
6. Zakharchenko N. Information security of Time-Controlled Signals in Confidential Communication Systems / N. Zakharchenko, V. Korchinsky, B. Radzimovsky // Modern problems of radio engineering, telecommunications and computer science: XI International Conference TCSET 2012, (Lviv-Slavske, 21-24 february 2012). – Lviv: Publishing House of Lviv Polyteshnic, 2012. – P. 317.