Information Security of Time-Controlled Signals in Confidential Communication Systems

Nicolay Zakharchenko, Vladimir Korchinsky, Bronislav Radzimovsky

Summary – **The evaluation of information security is given, the probabilities information contents breaking of time-controlled signals are determined.**

Key words – **Time-controlled signal, information security**

I. INTRODUCTION

Counteraction to unauthorized access attempts in confidential communication systems is the most important issue, that is why the search and study of the transmission methods, that let increase the security of signals is of high priority nowadays [1].

II. INFORMATION SECURITY EVALUATION

The paper examines the method of information security increase by using time-controlled signals [2] in a binary communication channel.

The value of the instants of a time-controlled signal modulation, formed at the time interval $T_c = nt_0$ (where n – is the number of unit elements; t_0 – their duration) are different from N-digit signal. They are not divisible to t_0, but t_0 a some base element Δ ($\Delta = t_0/s$; $s = 1, 2, 3, ..., l$ – are whole numbers). The segments of a signal with the duration $t_c = t_0 + k\Delta$ (where $k = 0, 1, 2, ..., s \cdot (n-2)$ are transmitted into a channel. The distances between signal constructions in time-controlled signals are determined by the value $\Delta < t_0$, so the number of their instances N_p at the interval T_c substantially increases in comparison with the N-digit code

$$N_p = \sum_{i=1}^{n} \frac{[(n \cdot s) - [(s-1) \cdot i]]!}{i! \cdot [[(n \cdot s) - [(s-1) \cdot i]] - i]!}, \quad (1)$$

where i – is the number of information instants of modulation.

We can obtain different multitudes of time-controlled signals by changing parameters n, s and i. Each of them will have different durations, that are dependable from n-values, number of base s-elements and the number of i transitions, i.e. from the signal form at the time interval T_c. A substantial increase of information security of time-controlled signals can be reached by the changing of the form. While using even a simple binary code in the transmission system, the information contents can be broken through only by the analysis of the matching instances of a time-controlled signal to N-digit code instances.

The number of comparisons for one instance considering the known n, s and i is determined by the formula (1). But it is necessary to analyze not a single instance but together their some number N_a to determine the information contents.

Fig. 1. shows graphs of the probabilities of information contents breaking of time-controlled signals in dependence from the number of mutually analyzed instances at different n, s and i values. The fig.1 demonstrates that the increase of the set of instances N_p of time-controlled signals and the number of mutually analyzed constructions N_a decreases the probability p_{inf} and their breaking.

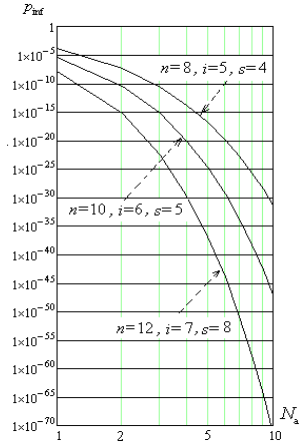

Fig. 1. Graphs of the probabilities of breaking of the information contents of time-controlled signals.

III. CONCLUSION

The results of the researches done showed that the use of time-controlled signals increases the structural and information security of the information transmitted. With this the probability of a signal structure breaking p_{str} can be minimized to 10^{-48}, and the probability of information security p_{inf} – to 10^{-70}. Besides, we can increase the information security of the transmitted messages by coding the time-controlled signals.

References

1. Kupriyanov A.I. Theoretical basics of radioelectronic fighting/ A.I.Kupriyanov, A.V. Sakharov. – M.: Vuzovskaya knyga, 2007. – 356 p.
2. Zakharchenko N.V. Basics of the coding: study guide/ Zakharchenko N.V., Krys'ko A.S., Zakharchenko V.N. – Odessa: USAC named after A.S.Popov, 1999. – 240 p.

Nicolay Zakharchenko, Vladimir Korchinsky, Bronislav Radzimovsky – Lviv Polytechnic National University, S. Bendery Ctr., 12, Lviv, 79013, UKRAINE, E-mail: vladkorchin@rambler.ru