УДК 621.618

V.D. Karlov[1], O.V. Lukashuk[1], S.M. Sholokhov[2]

[1] *Kharkiv Ivan Kozhedub Air Force University, Kharkiv*
[2] *M/U A1906*

ANALYSIS OF METHODS OF DECLINE OF VULNERABILITY OF TELECOMMUNICATION SYSTEMS

The analysis of providing of informative safety of the telecommunication systems is conducted in the article. The conducted analysis allowed to define the circle of questions which methodically must be considered for the decline of vulnerability of the systems at attacks on them, carrying electromagnetic character. The basic types of tasks of intercept of information are resulted due to side electromagnetic radiations.

Keywords: *informative safety, system of telecommunications, priv, hertzian wave, electromagnetic compatibility/*

Introduction

A priv in a computer technique and computer networks has more, than 30-years-old history, therefore to the present tense considerable experience is already accumulated, both theoretical developments of different aspects of the examined problem and practical decision of tasks of defence. However, on Ukraine to the question of priv little attention was spared and popular publications on this subject were not practically. Lately position changed substantially, however may need some time in order that it is possible it was to make the complete enough selection of the proper works [1-3].

As a result of analysis of practical experience of protecting from the loss of information it should be noted that for the telecommunication systems of the special purpose (state, soldiery, industries of industry) development of mechanisms of priv was obligatory, and such mechanisms have all of the systems, indicated higher. In all of the systems mentioned above basic efforts were concentrated on prevention of loss of information due to hindrances and aiming. For these ductings both the norms of protected and necessary for defence facilities are developed. The excessive closed of all of works on a priv resulted in that in the open telecommunication systems on processing of data which make the bulk of the functionings systems, a priv practically absents with all of effluent from here consequences.

Except for it, the telecommunication systems in connection with development of global networks got an additional impulse in the development, technical realization of which within the limits of buildings and apartments got the logical completion as the popular structured cable systems. It is necessary to take into account the enhanceable saturation of environment various radio electronic facilities of the different setting, that results in electromagnetic indignations which can violate integrity of signal.

Therefore in this article one of the possible going is considered near the decision of task of priv technical methods which are very near to the receptions of providing of electromagnetic compatibility of hardwares.

Basic part

There is a necessity and right for an enterprise on defence of the interests in mutual relations with other subjects of market relations. Appropriation machine information, for example, by the intercept of it due to side electromagnetic radiations from a computer technique, office equipment, cable system not characterized as a theft, as a theft is attended with the withdrawal of values from the funds of organization. Machine information is the independent article of уголовно-правовой guard.

Modern level of development of the radio engineering, electronics, computing engineering, methods of analysis, allows cryptographies at favourable terms to select signals, bearings processed the telecommunication system (TS) information, from the general stream of electromagnetic radiations, arising up during work of devices of the computing engineering, and to recover this information by the special methods of treatment of the accepted signals. A loss of information due to side electromagnetic radiations (SER) is one of the basic ductings. Therefore in the whole

world sharply the problem of defence costs processed in TS of information [3].

For the decision of question about the necessary degree of defence and estimation of protected of information from a loss on ductings of SER it is necessary to lean against the model of possible intercept of information. For this purpose it is required to estimate оперативно-тактические, electrodynamic, technical and algorithmic possibilities of intercept of information.

At the construction of model of possible intercept of information it is necessary to take into account circumstance that an effective intercept of information on ductings of SER is a very intricate problem in swingeing majority of cases, both in a technical and in mathematical plan. Therefore to come running to the use of ductings of SER expediently only then, when other, to extract information more accessible methods is not possible.

For the effective intercept of signals in ductings of SER, generally speaking, a receiving apparatus, able to select concrete signals from the devices of personally calcuble machine (PCM) on a background hindrances, being additive mixture of natural and artificial hindrances, is required.

Thus hindrances, created the examined hardware of PCM and nearby with him components of TS, and also by the structured cable system, belong to the last. Such possibilities are possessed by the specialized cross-correlation receivers (which industry sew on practically does not make a country). In a number of cases at an intercept it is required to conduct the accumulation of periodically repetitive fragments of radiation with the purpose of effective selection of useful signals on a background masking hindrances (so-called reception with an accumulation). Such apparatus also behaves to the special. Thus, the serially produced takers-offs in swingeing majority of cases can not be effectively utillized for the decision of tasks of intercept.

However there are cases, when an intercept appears possible by the serial produced apparatus. The first case is an intercept of the information shined on a display by an usual televisional receiver. It is thus possible substantially to improve possibilities of reception by insignificant changes in a televisional receiver. The second case is an intercept of radiations from низкочастотных electromechanics devices with the successive code of information transfer. In this case an intercept can be carried out the narrow-band enough serially produced receiver.

Estimation of algorithmic possibilities

Under algorithmic possibilities possibilities of renewal of processed personally calcuble machine of information are implied on results the intercept of signals in ductings of SER. Here development of algorithms of rough-down of the accepted mixture (useful signal + hindrance) belongs with the purpose of selection of bearings information signals on a background помеховых signals and noise.

Such algorithms are mortgaged in the specialized apparatus of intercept at its planning. Further treatment of results of reception is conducted in accordance with the special algorithms, allowing to recover initial information.

Such work requires except for knowledge the techniques of work with algorithms yet and large experience on their application and good knowledge of problem which the intercepted information behaves to.

Thus, even in the case of application of the imported specialized apparatus of intercept it is necessary to attract a specialist in area of renewal of information on results the reception of signals of SER, well knowing a problem which the intercepted information behaves to.

In the case of intercept of information, represented on displays, by televisional receivers no after-treatment is required is simply read from a televisional receiver.

Maximum possibilities on renewal of information on results an intercept on condition of presence of a priori necessary information, participation of highly skilled specialists and use of the powerful computer systems at one time are appraised, and results are reflected in the proper documents.

Estimation of operatively tactical possibilities

Experience talks that it is possible practically with impunity and swimmingly openly engaged in the intercept of radiations in a direct closeness to territory of enterprise. Only own service safety of owner of information can prevent (as far as it will appear possible within the framework of law) to be engaged in the intercept of SER.

From point of equipment of point of intercept it is possible to say following. Sure, it is impossible fully to eliminate an acquisition of the specialized apparatus option. Such probability is increased in the case of organization of separate private предпринимательств, specialized in area of theft of information on the orders of competitive enterprises. In this case the danger of theft of information rises sharply, because such educations will possess more wide financial possibilities and can utillize specialists both in area of radio intercept and in area of the special mathematical treatment of results of intercept with the purpose of renewal of processed personally calcuble machine of information.

Electrodynamic limitations of intercept of information

Electrodynamic processes and limitations, related to possibility of distribution of hertzian waves (EMW) in the set situation, certain environment, influence on a volume and quality of the intercepted information.

For a management the environment of distribution of EMW and localizations of the electromagnetic field the effective screening must be used, thus not only technical components of the telecommunication systems but also apartments TS is installed in which.

It talks about the complexity of problem of providing of informative safety which must decide on all of the stages of creation of the telecommunication system: from working of its conception to installation and conclusion from the process of exploitation.

The extended understanding of questions of informative safety requires except for consideration of SER, to talk yet about integrity of signal. Evil-minded distortion of informative signal in the telecommunication system can result in the loss of information or its distortion.

These distortions, in same queue, it is relatively simple to cause the injectia of hindrances in the network of feed of the telecommunication system, powerful electrostatic a digit, violation of grounding of the system.

Similar receptions, getting in the hands of malefactors, can result in a substantial loss, and already got the name "Electromagnetic terrorism in western literature".

Conclusion

Thus, on the modern stage appears reasonable to take into account in the model of intercept two possible variants depending on the degree of importance of the hidden information.

For of less importance, information can consider that an intercept is conducted coming from terms with the limited cognitions in area of intercept of SER and not specialized apparatus.

These models are supposed by the adequate measures of defence of the telecommunication system on ceiling of ductings of loss of information due to SER.

References

1. Петраков А.В. Основы практической защиты информации. Учеб. пособие / А.В. Петраков. – М.: Радио и связь, 2000. – 368 с.

2. Электромагнитная совместимость радиоэлектронных средств и непреднамеренные помехи / Составитель Д. Р. Ж. Уайт; В 3-х выпусках. Вып. 2: Внутрисистемные помехи и методы их уменьшения / Сокр. пер. с англ.; Под ред. А. И. Сапгира. - М.: Сов. радио, 1978. – 272 с.

3. Барсуков В.С. Комплексная защита от электромагнитного терроризма / В.С. Барсуков // Системы безопасности связи и телекоммуникаций. – 2000. – № 32, – С. 94 - 98.

Надійшла до редколегії 19.04.2016

Рецензент: д-р техн. наук, проф. Л.Ф. Купченко, Харківський університет Повітряних Сил імені Івана Кожедуба, Харків.

АНАЛИЗ МЕТОДОВ СНИЖЕНИЯ УЯЗВИМОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

В.Д. Карлов, Е.В. Лукашук, С.Н. Шолохов

В статье проведен анализ обеспечения информационной безопасности телекоммуникационных систем. Проведенный анализ позволил определить круг вопросов, которые методически должны быть рассмотрены для снижения уязвимости систем при атаках на них, носящих электромагнитный характер. Приведены основные типы задач перехвата информации за счет побочных электромагнитных излучений.

***Ключевые слова**: автоматизированная система управления, высокоточное вооружение, информационное оружие, радиоэлектронная борьба*

АНАЛІЗ МЕТОДІВ ЗНИЖЕННЯ УРАЗЛИВОСТІ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

В.Д. Карлов, О.В. Лукашук, С.М. Шолохов

У статті проведений аналіз забезпечення інформаційної безпеки телекомунікаційних систем. Проведений аналіз дозволив визначити круг питань, які методично повинні бути розглянуті для зниження уразливості систем при атаках на них, що носять електромагнітний характер. Приведені основні типи завдань перехоплення інформації за рахунок побічних електромагнітних випромінювань.

***Ключові слова:** інформаційна зброя, радіоелектронна боротьба, автоматизовані системи управління, високоточна зброя*