Yevhen PELESHOK[1], Oleksii GAVRYLENKO[2], Vasyl NEKOZ[3], Kostyantin GERASIMOV[4]

Scientific supervisor: Serhii IVANCHENKO[5]

WAYS TO JUSTIFY THE PROTECTION OF INFORMATION FROM LEAKAGE BY TECHNICAL CHANNELS FOR MODERN ITS

Abstract: The ways of substantiation of information leakage protection by technical channels for modern information and telecommunication systems are reviewed. The features of these pathways, their advantages and disadvantages were analyzed and recommendations were made for the use of one of them. Theoretical substantiation of security provides protection according to ISO / IEC 27000 and has been proven to provide a guarantee of reliability.

Keywords: informational security; technical protection of information; information leakage; technical channel of leakage

SPOSOBY UZASADNIENIA OCHRONY INFORMACJI PRZED WYCIEKIEM KANAŁAMI TECHNICZNYMI DLA NOWOCZESNYCH ITS

Streszczenie: Przeanalizowano sposoby uzasadnienia ochrony przed wyciekiem informacji kanałami technicznymi dla nowoczesnych systemów informatycznych i telekomunikacyjnych. Przeanalizowano cechy tych ścieżek, ich zalety i wady oraz sformułowano zalecenia dotyczące

[1]PhD Eng (Mathematical modeling and computational methods), Deputy Chief of the Scientific and Research Center, Institute of Special Communication and Information Protection, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute" pel85@ukr.net
[2]PhD Eng (Mathematical modeling and computational methods), Associate Professor, IT-Security Academic Department, National Aviation University, gavrylav@gmail.com
[3]Senior Research Fellow of the Scientific and Research Center, Institute of Special Communication and Information Protection, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute" nvs20141987@gmail.com
[4]Senior teacher of the department Institute of Special Communication and Information Protection, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute" gerasimov7@ukr.net
[5]Dr Eng (Information security), Professor,Chief of the Scientific and Research Center, Institute of Special Communication and Information Protection, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute" soivanch@ukr.net

wykorzystania jednego z nich. Teoretyczne potwierdzenie bezpieczeństwa zapewnia ochronę zgodnie z ISO / IEC 27000 i udowodniono, że zapewnia gwarancję niezawodności.

Słowakluczowe: bezpieczeństwo informacji; techniczna ochrona informacji; wyciek informacji; kanał wycieku technicznego

1. Introduction

One type of information resource that involves the use of cyberspace is sensitive information, which has limited access. Depending on the importance and value of this information, information and data may have different degrees of access and, accordingly, may be subject to different security methods, taking into account the list of threats, the degree of security protection and the complexity of implementation.

It is known that the work of modern ITS, ensuring the functioning of cyberspace, is almost always accompanied by a number of side effects, characteristic for electrical engineering, which contribute to the formation of technical channels of information leakage [1, 2]. In addition to the essential feature of modern ITS, which can affect the deterioration of the protection of information against leakage, is the automated self-management of internal processes with minimization of operator participation.

Therefore, the search for ways to justify the protection of information from leakage by technical channels for modern ITS is relevant and requires specific research and solutions.

2. Basicstudies

According to international standards for information security management, namely the ISO / IEC 27000 series, the central concept is security risk [3]. Risk is a potential possibility of danger that leads to losses. It is a combination of the likelihood of the realization of the threat and its consequences. Therefore, this indicator in the technological part of the implementation of the threat can be considered as the probability that some of the information will still leak through the technical channels. If there is such a permissible part of this information in which the leakage does not break or breach the material, then it can be taken as a norm of safety and put in accordance with the maximum permissible risk probability.

This maximum permissible probability is the starting value for the calculation of all other technological regulatory indicators that characterize the effect of counteracting the threat. The consequences of the realization of the threat are a matter of choosing the scale of losses and the price of divides. These probabilities and consequences should be determined with the participation of the owner of the information and be declarative or normative.

Within the framework of this justification for the protection of information from leakage by technical channels, the following solutions may be available:

- complete, with an intuitively accepted stock of liquidation of prerequisites of information leakage;
- sufficiently partial neutralization of technical channels based on theoretically sound security;

- sufficiently partial neutralization of technical channels with practical justification of protection against existing interception means.

The elimination of the prerequisites for information leakage at the sites is related to ensuring that there are no dangerous signals in the places of possible interception. Generally, this is achieved by creating large enough control areas where their boundaries should reach hundreds of meters and kilometers so that complete signal scattering takes place. This is the absence of any galvanic connections of the outgoing circuits to the outside world. This is an autonomous power supply of hardware and information processing and transmission systems, etc. At the same time, this is a complete guarantee of leakage of information through technical channels.

Obviously, this approach is quite suitable for practical implementation. However, it has difficulty, especially when locating objects in densely populated areas. This is first and foremost due to the need to occupy (rent) large enough territories and a high cost of living. These are significant restrictions on staffing, such as the prohibition of urban and mobile workplace use, the Internet, other household matters, and so on. All this creates inconvenience and often inability to apply this approach.

Sufficiently partial neutralization of technical channels on the basis of theoretically sound information security allows saving costs in comparison with the previous approach [4]. Its essence is that the channel contains such conditions under which the signal can still be intercepted, and the information is gone. After all, detecting media features is not yet a fact of data interception; the extent of the interception of the signal and the extent of information received from it are not directly proportional. This is due to the uneven distribution of information on the time and frequency elements of the signal; these are meaningful links between them that make variations in stats when intercepted, and so on.

Despite the simplification and cheapening of practical application in relation to the complete elimination of technical channels of information leakage, this approach has the difficulty of theoretical substantiation of security. After all, proving the conditions of sufficiency with partial neutralization of the channel requires appropriate mathematical calculations, acceptance of restrictions and assumptions, as well as appropriate experiments.

However, cost savings when used on site are of considerable benefit to this approach because it is devoid of unreasonable but intuitive security stock and the need to maintain it. And the complexity of mathematical justification for the security of information and its norms can be ensured using modern computer technology, which has quite high capabilities.

A sufficiently partial approach to neutralize technical channels with a practical justification for the protection of information from leakage against existing interceptors can allow for even greater cost savings. However, the complexity and validity of security in this approach have their own peculiarities.

First of all, its implementation requires: availability of the most up-to-date spectral analysis tools with appropriate antenna and sensor equipment; providing the most “clean” conditions for simulating technical channels of information leakage; conducting a number of experiments to find the norms of the practical sufficiency of protection with partial channel neutralization.

Secondly, the guarantee of such protection is conditional and is based on the results of the experiment with respect to specific models of technology.

Third, providing the right level of guarantee requires constant periodic adjustments to security standards, which are linked to the development of science, technology and technology.

3. Conclusions

The ways of substantiation of information security for modern ITS from leakage by technical channels are reviewed. It is shown that security can be justified by complete elimination of the technical channel, by sufficiently partial elimination with theoretically substantiated security and with its practical justification with respect to the interception means. The disadvantages and advantages of the mentioned ways are indicated, from which it follows that the most appropriate for use in today is a rather partial approach of neutralization of technical channels on the basis of theoretically justified security [4]. This approach has proven to provide the right amount of risk in accordance with the international standards for information security management of the ISO / IEC 27000 series, guarantee the security of the security set and be applicable to information of all degrees and types of access restriction.

REFERENCES

5. KUHN G.: Compromising emanations: eavesdropping risks of computer displays. This technical report is based on a dissertation submitted June 2002 by the author for the degree of Doctor of Philosophy to the University of Cambridge, Wolfson College. [Электронный ресурс]. – Режим доступа: *http://www.cl.cam.ac.uk/techreports*.
6. ЛЕНКОВ С. В.: Методы и средства защиты информации. Том I. Несанкционированное получение информации / С. В. Ленков, Д. А. Перегудов, В. А. Хорошко – К. : Арий, 2008. – 464 с.
7. Information technology. Security techniques. Information security management systems. Requirements [ISO/IEC 27001:2013].
8. ІВАНЧЕНКО С. О.: Обґрунтування ризику безпеки інформації щодо її захищеності від витоку технічними каналами / Сергій Олександрович Іванченко // Науково-технічний збірник “Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні”. – Київ, НТУУ “КПІ” НДЦ “Тезис”, 2016. – № 1 (31) – С. 9 – 13.