Anatolii HOLISHEVSKYI [1], Oleh RUSHCHAK[2], Yevhen PROKOPENKO[3], Vasyl NEKOZ[4]

Scientific supervisor: Serhii IVANCHENKO[5]

DOI: https://doi.org/10.53052/9788366249868.06

WSKAŹNIKI OCHRONY INFORMACJI PRZED WYCIEKIEM PRZEZ KANAŁY TECHNICZNE DLA NOWOCZESNEGO ITS

Streszczenie: System został opracowany w celu scharakteryzowania ochrony nowoczesnych systemów informatycznych i telekomunikacyjnych za pośrednictwem serii kanałów informatycznych. Zaproponowano zbiór wskaźników ryzyka. Elementy tego zbioru tworzą pewną struktura hierarchiczną, która pozwala na analizę ryzyka i bezpieczeństwa informacji.

Słowa kluczowe: informacji, analiza ryzyka, techniczny kanał wycieku danych, wskaźniki bezpieczeństwa

INDICATORS OF INFORMATION PROTECTION FROM LEAKAGE THROUGH TECHNICAL CHANNELS FOR MODERN ITS

Summary: The set of risk-oriented indicators that will characterize the protection of modern information and telecommunication systems from information leakage through technical channels has been substantiated. The set is a hierarchical structure and allows information security risk analysis.

Keywords: informational security, security risk, information leakage, technical leakage channel, security indicators

[1] PhD Eng (Information security), senior designer, State Scientific and Research Institute of Cybersecurity Technologies and Information Protection, 380937029549@ukr.net

[2] Deputy Head of the Special department № 4, Institute of Special Communication and Information Protection, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", oruschak@gmail.com

[3] Deputy Head of the Department of information and telecommunication systems and technical information protection, Institute of Special Communication and Information Protection, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", prokopenko1111111@gmail.com

[4] Researcher 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

[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

1. Introduction

The main threat to information that violates its confidentiality is its disclosure, which in the processing and transmission of information by technical means can be realized through electromagnetic radiation and guidance, infiltration of dangerous signals into the power supply and grounding, etc. (Figure 1). The propagation of dangerous signals in this way beyond the control of the object is carried out over a relatively short distance and leads to the formation of technical channels of information leakage. With the help of modern means of spectral analysis and control and measuring techniques, these signals can be intercepted, and their processing leads to unauthorized receipt of information [1 - 3].

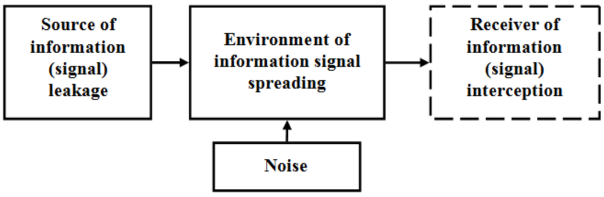
Source of information (signal) leakage
Environment of information signal spreading
Receiver of information (signal) interception
Noise

Figure 1. Technical information leakage channel

Particularly in the center of contamination є those who have been declared effective є by the natural manifestation of the physical center, decease the information. Ensuring information throughout the round, make sure that the localization of the effect is not connected with the minimization of the localization, and we absolutely cannot help it. The whole threat, the seizure of what may be without a bribe, a joke for a compromise to help in the value and value of information resources and vitrates for those who want to get it. It is accepted to respect that the world will be able to learn the value of information, so that he will be seized. The revision of the world over the price of information is insufficient.

With the development of the ITS, there will be improved indicators of data processing, increased memory, the spectrum of vicious signals will expand, new functional possibilities will appear, which will allow the introduction of new technologies [3]. So, the current ITS is software-kerovan systems, de management of them will be automated from the minimum backs of the koristuvach. The stench of self-robbing routes for transmission of data, self-procuring the availability of channels, self-sustaining repetition of sessions of processing and transmission, self-sufficient reserving of the data is meager. All the price is injected into the accelerated retrieval of information in the ITS through the turn of technical channels and through the use of technical channels when the minds of a safe cyber space are established, and the information is obtained in the information and information channels.

World experience shows that the main indicator of safety is the risk, the permissible limits of which are set by the owner, which in the event of attacks or incidents may suffer damage. Obviously, the risk depends on the indicators of information security, which require periodic monitoring and analysis, and the required values for the indicators are from the specified risks [4]. Thus, there is an urgent task to substantiate the indicators that will characterize the protection of ITS from information leakage through technical channels and will allow the assessment of information security at the objects of information activities.

2. A set of indicators of information security for modern ITS

According to the international standard for information security management, for example, ISO/IEC 2700x or other standards set the risk of information security. Security risk quantifies the potential hazard that leads to losses and can be presented as the product of the probability of the threat p_r and rates *Price* effects of it [4]:

$$R = p_r \times Price\ . \tag{1}$$

In essence, risk is a general indicator of quality that quantitatively characterizes the degree or level of protection. If you set its maximum allowable value $R_{\text{max.allow}}$, then it is possible to implement a risk-oriented approach to ensure the protection of information, including from leakage through technical channels. The convenience of implementing this approach is that on the basis of automated processing it allows to increase the efficiency of analysis, adjustment and management of information security.

Obviously, the price of possible losses *Price* and risk limits $R_{\text{max.allow}}$, should establish the owner of information, information resources, as an entity that is interested in the necessary degree of protection and effective management of information security of its own resources [4]. The maximum allowable probability of risk $p_{r.\text{max.allow}}$ is a technological indicator that should provide a protection system and can be found from formula (2):

$$p_{r.\text{max.allow}} = R_{\text{max.allow}}/Price\ . \tag{2}$$

The protection system will be effective if its indicators are reliable $p_{r.\text{max.allow}}$ and thus this system is proven to guarantee information security with a given risk.

Security risk is a failure to meet its quality requirements, and therefore for the leakage of information through technical channels it can be considered as a leakage risk. Its maximum allowable value can be matched to such a characteristic of the channel as bandwidth C – the maximum amount of information that can be allowed to flow through the technical channel of leakage (TCL) [3,5].

$$C_{\text{max.allow}} = p_{r\ \text{max.allow}} \times C_{\text{max}} \tag{3}$$

where C_{max} – maximum throughput of TCL.

The bandwidth of the channels is determined by the interference of the environment of the distribution of physical media. Interference in the channel causes the probability of error p, which limits the channel's ability to pass information. For discrete symmetric binary channels, the bandwidth is expressed by the formula:

$$C = 1 - h(p) \tag{4}$$

where h (…) – is the entropy function.

From formula (4) you can find the maximum allowable value for the probability of error in the channel, which should provide camouflage interference:

$$p_{\text{max.allow}} = h^{-1}(C_{\text{max.allow}} - 1)\ . \tag{5}$$

Errors in the channel are formed as a result of incorrect reception of signals at the output of the channel. They depend not only on the properties of the environment of distribution of physical media, where there are interference, but also on the methods of processing information signals at the reception, their decision schemes, algorithms and so on.

Assuming that Gaussian normally distributed white noise with spectral density acts as a noise in the medium N_0 and interception is performed using an ideal receiver, the required maximum allowable signal-to-noise ratio can be found as:

$$\delta = \frac{1}{2}\sqrt{\frac{P_\Delta \times T}{N_0}} = F^{-1}(p). \tag{6}$$

where P_Δ – difference signal power.

These indicators are a hierarchical structure, where the indicators of the lower levels ensure the performance of the indicators of the upper levels of the hierarchy:

$$\delta \to p \to C \to p_r \to R\ . \tag{7}$$

3. Conclusions

The set of indicators of information security from leakage through technical channels for modern ITS is substantiated. This set is a hierarchical structure, where the main risk or probability of risk is a common indicator of information security for all types of information. The other three indicators of technical channel leakage capacity, its probability of error and signal-to-noise ratio at the reception are related to the provision of a given risk on the types of information in their technological processing, circulation in technical means and circulation in the physical environment.

REFERENCES

1. LENKOV, S.V., PEREGUDOV, D.A., HOROSHKO, V.A.: Methods and means of information protection. Tom I. Unauthorized receipt of information. Ariy: Kyiv (2008).
2. BUZOV G.A., KALININ S.V., KONDRATEV A.V. Protection of information from leaks through technical channels, Goryachaya liniya: Moskva, Telecom (2005).
3. IVANCHENKO S., PUCHKOV O., RUSHAK O., HOLISHEVSKYI A.: Leakage by technical channels for modern information and telecommunication systems. International scientific-practical conference: "Information technologies and computer modeling", Ivano-Frankivsk, pp. 179–183 (2019) ISBN 978-617-7468-37-9.
4. Information technology. Security techniques. Information security management systems. Requirements [ISO/IEC 27001:2013].
5. FINK L. M.: The theory of transfer of discrete messages [2-d edition], Sov. Radio: Moskva, (1970).