Akademia Techniczno-Humanistyczna w Bielsku-Białej
WYDZIAŁ BUDOWY MASZYN I INFORMATYKI
Inżynier XXI wieku

XI Inter University Conference „Engineer of XXI Century" – 10 December 2021

Indicators of information protection from leakage through technical channels for modern ITS

Anatolii HOLISHEVSKYI[1], Oleh RUSHCHAK[2], Yevhen PROKOPENKO[3], Vasyl NEKOZ[4]
Scientific supervisor: Serhii IVANCHENKO[5]

[1] *PhD Eng (Information security), senior designer, State Scientific and Research Institute of Cybersecurity Technologies and Information Protection*
[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"*
[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"*
[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"*
[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"*

Abstract

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.

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).

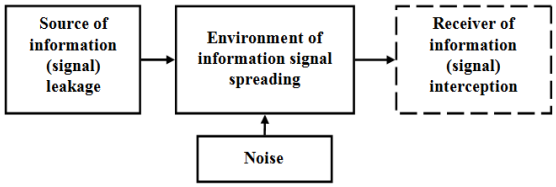

Figure 1: Technical information leakage channel

The peculiarity of this threat is that these effects are a natural manifestation of the physical environment where information is circulated. Securing information from leakage is usually associated with minimizing these manifestations and localizing the effects, and therefore cannot be done completely. This is a threat that can only be protected by finding a compromise between the attentiveness and value of information resources and the costs of protecting them.

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.

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:

$$R = p_r \times Price\ . \quad (1)$$

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 $R_{max.allow}$, 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 $R_{max.allow}$, 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.

The maximum allowable probability of risk $p_{r.max.allow}$ is a technological indicator that should provide a protection system and can be found from formula (2):

$$p_{r.max.allow} = R_{max.allow}/Price\ . \quad (2)$$

The protection system will be effective if its indicators are reliable $p_{r.max.allow}$ 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).

$$C_{max.allow} = p_{r\ max.allow} \times C_{max}\ , \quad (3)$$

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:

$$C = 1 - h(p)\ , \quad (4)$$

where $h(\ldots)$ – 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:

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

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:

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

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:

$$\delta \to p \to C \to p_r \to R\ . \quad (7)$$

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.

Ministerstwo Edukacji i Nauki
Dofinansowano z programu „Doskonała nauka" Ministra Edukacji i Nauki