Leakage of Information Through Technical Channels and a Set of Risk-Oriented Indicators of Its Security for Modern ITS

Serhii Ivanchenko[1], Oleksii Gavrylenko[2], Anatolii Holishevskyi[3], Vasyl Bondarenko[4], Oleh Rushchak[5], Yevhen Prokopenko[6]

[1,5,6]*Institute of Special Communications and Information Protection of National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, 03056, Ukraine*
[2]*The Department of Information Technology Security, National Aviation University, Kyiv, 03058, Ukraine*
[3]*State Scientific and Research Institute of Cybersecurity Technologies and Information Protection, Kyiv, 03142, Ukraine*
[4]*State Service of Special Communication and Information Protection of Ukraine, Kyiv, 03110, Ukraine*

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.

Keywords

Informational security; security risk; technical protection of information; information leakage.

1. Introduction

One of the threats to information security, which violates the confidentiality of information, is its leakage through technical channels formed during the operation of modern information and telecommunications systems (ITS) as a result of a number of undesirable parasitic effects (Figure 1).

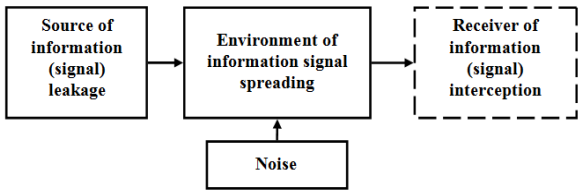

Figure 1: Technical information leakage channel

Such effects are the side electromagnetic radiation of information signals into the environment, their guidance on extraneous conductors and lines beyond the control of the object, the infiltration of signals into the grounding and power supply circuits, etc. [1 - 4].

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. It is considered that the protection measure should correspond to the value of the protected information. Exceeding this measure over the value of information is impractical.

State information resources are public information that requires its circulation in cyberspace and involves the use of modern ITS, which are constantly evolving and improving. Thus, today the pace of development of information and telecommunications technology is such that due to its obsolescence, the feasibility of replacing old tools with new ones comes quite quickly after they enter the market. This rather high rate does not allow the

ISIT 2021: II International Scientific and Practical Conference «Intellectual Systems and Information Technologies», September 13–19, 2021, Odesa, Ukraine
EMAIL: soivanch@ukr.net (A. 1); gavrylav@gmail.com (A. 2); 380937029549@ukr.net (A. 3); bbazil@ukr.net (A. 4); oruschak@gmail.com (A. 5); htc79@i.ua (A. 6)
ORCID: 0000-0003-1850-9596 (A. 1); 0000-0002-9552-5832 (A. 2); 0000-0001-9981-7771 (A. 3); 0000-0002-7578-3236 (A. 4); 0000-0001-6504-6315 (A. 5); 0000-0002-7582-8772 (A. 6)

implementation of proper provision, as was done for the equipment of previous years, for which this period was decades. With the development of ITS, the speed of data processing increases, the amount of memory increases, the range of signals used expands, and new functionalities appear that allow the introduction of new technologies [5].

Thus, modern ITS are software-controlled systems, where they are controlled automatically with minimal user involvement. They independently choose routes for data transmission, independently adjust the noise immunity of channels, making redundant data, independently repeat processing and transmission sessions, independently without notifying the user of the system perform backup data and so on. All this significantly affects the complexity of protection of information in ITS from leakage through technical channels and requires consideration when justifying the conditions of safe use of cyberspace for information circulation and ensuring protection of information from leakage through technical channels [6, 7].

This threat is relevant to public information in terms of information with limited access, which includes classified, official and confidential information. Accordingly, the secret information with limited access is divided into state, banking, professional secrets and the secret of the pre-trial investigation and other secrets provided by law. A separate category of information for which the threat of leakage through technical channels may be relevant is personal data. Its owners also have the right to ensure confidentiality with any level of protection. This distinction is made in the legal field of the state, takes into account the affiliation of information, their importance and value, ensures the interests of man, society and the state [5, 8].

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 [9].

Therefore, there is an urgent task to substantiate the totality of risk-oriented indicators that will characterize the protection of ITS from information leakage through technical channels and will allow the assessment and analysis of information security risk at the objects of information activities.

2. A set of risk-oriented indicators of its security for modern ITS

Let the information security risk be set according to an international standard for information security management, for example, ISO/IEC 2700x or other standards. Security risk quantifies the potential danger that leads to losses, and can be represented as the product of the probability of realization of the threat p_r and *Price* consequences of it [10]:

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

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 $R_{\max.allow}$, It is possible to implement a risk-oriented approach to protect information, including from leakage through technical channels. The convenience of implementing this approach in relation to the previous one, as it was done for the technology of previous years, 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 be set by the owner of information, information resources, as an entity interested in the necessary degree of protection and effective management of information security of own resources [5]. 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 (1):

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

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

Let the limit of probability of risk $p_{r.\max.allow}$ be set – safety condition of information with limited access, which must be fulfilled in technical channels by means of technological indicators within its calculated limits. These indicators in their structured combination will

represent a system of risk-oriented indicators that characterize the protection of ITS from information leakage through technical channels.

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 by such a characteristic of the channel as bandwidth – the maximum amount of information that can be allowed to flow through the technical channel of leakage [10].

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

where C_{max} – is the maximum bandwidth of the technical channel of leakage.

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

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

where *h* (…) – is the entropy function:

$$h(p) = \frac{1}{p}\log_2 \frac{1}{p} + \frac{1}{1-p}\log_2 \frac{1}{1-p}. \quad (5)$$

From formulas (4) and (5) you can find the maximum allowable value for the probability of error in the channel, which should provide camouflage interference:

$$p_{\text{max.allow.}} = h^{-1}(C_{\text{max.allow.}} - 1) \quad (6)$$

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 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.

Thus, the following three situations can be considered for information interception:

1. The attacker is quite interested in obtaining information, has unlimited ability to intercept it and monitors the source of leakage continuously.
2. The attacker is quite interested in obtaining information, but to intercept it has a limited ability to observe the source of leakage indefinitely.
3. The attacker is not very interested in obtaining information, interception is carried out in fragments, sporadically.

Obviously, the second situation takes into account the real possibilities of interception, and therefore should be the most common in relation to other situations. However, here, when assessing security, it is necessary to have specific data about the receiver and its capabilities. Obviously, this is a challenge. It is also obvious that if the receiver is changed to a more efficient one, the information may become less secure and may not leak through the technical channel of leakage.

The third situation indicates that the owner has overestimated the importance (value) of his information or the information is narrow and interesting only to a limited group of attackers and of little interest to everyone else. In this case, the protection system requires a review, otherwise its use will be associated with excessive spending.

The first situation takes into account the potential for interception and is somewhat idealized in terms of reception. This situation has the least chance of prevalence. However, it is most in demand for justification of security. It is the best for interception and the worst in terms of protection, while covering the second and third situations, which mainly occur in practice. Its main disadvantage is that reasonable protection in the first situation for the other two acts with a margin and causes overspending. However, in order to ensure proper reliability of protection, it is necessary to sacrifice somewhere.

Let the first situation underlie the justification of information security. Interception is carried out constantly and in the best way. We find a condition for the environment in which, given the given security risk, interception will become impossible. At the same time we will consider that if in technical channel of leakage interception is not carried out and the receiver is absent, the channel all the same will take place with a certain representation of the receiver as if this receiver is present (Figure 1).

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

$$\delta = \frac{1}{2}\sqrt{\frac{P_\Delta T}{N_0}} = F^{-1}(p), \qquad (7)$$

where P_Δ – is the power of the difference signal:

$$P_\Delta = \frac{1}{T}\int_0^T s_\Delta^2(t)dt, \qquad (8)$$

$s_\Delta(t)$ – difference signal:

$$s_\Delta(t) = s_1(t) - s_0(t), \qquad (9)$$

$s_0(t)$ and $s_1(t)$ – implementation of logical «0» and «1», T – pulse duration,

$F^{-1}(\ldots)$ – inverse function to the Laplace function:

$$F(x) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x}\exp\left\{-\frac{\eta^2}{2}\right\}d\eta. \qquad (10)$$

In the case of imbalance of information signs, which can sometimes occur in modern ITS, for example, the number of logical "1" exceeds the logical "0" or conversely, the ratio for find the desired signal-to-noise ratio (7) will be somewhat complicated. The error probabilities will be determined on average by all information signs x_r. For binary systems [4, 9, 10 - 13]:

$$p = p(x_0)p(y_1/x_0) + p(x_1)p(y_0/x_1), \qquad (11)$$

where $p(x_0)$ and $p(x_1)$ – probabilities of information signs x_0 and x_1, for example, logical "0" and "1";

$p(y_1/x_0)$ and $p(y_0/x_1)$ – conditional probabilities of transitions in the channel of input information signs x_0 and x_1 to the output signs y_1 and y_0 accordingly:

$$p(y_1/x_0) = F\left(-\delta + \frac{1}{4}\frac{1}{\delta}\ln\frac{p(x_1)}{p(x_0)}\right) \qquad (12)$$

and

$$p(y_0/x_1) = F\left(-\delta - \frac{1}{4}\frac{1}{\delta}\ln\frac{p(x_1)}{p(x_0)}\right). \qquad (13)$$

It is obvious that finding the signal-to-noise ratio δ from relations (12) and (13) is much more difficult than from (7). However, with the help of modern computer technology and technology, this is possible in real time.

In case of imbalance of signs the graphic dependence on Figure 2 in quadrant III. This shows that with a fixed signal-to-noise ratio and with an increase in the predominance of some probabilities in the distribution of the source over others, the probability of error and protection of information from leakage will decrease. In this case, according to relations (3) and (4), the channel bandwidth and security risk will increase.

Thus, if the owner of the information wants to secure his information with the maximum allowable risk $R_{max.allow}$ then the required signal-to-noise ratio can be established using a set of the following indicators:

1. *the probability of security risk* – p_r;
2. *bandwidth of technical channel of leakage* – C;
3. *the probability of error in the technical channel of leakage* – p;
4. *signal / noise ratio at the input of the receiver of the interception means* – δ.

These indicators can be used as mandatory for the calculation of each ITS in order to ensure the leakage of information through the technical channel of leakage. Relationships (2), (3), (6) and (7) establish a relationship between the maximum allowable values of these indicators, which can be used to create an appropriate calculation methodological apparatus.

The principle of calculation can be represented by graphs arranged by quanrants, as shown on Figure 2.

On the axis of risks R (axis of ordinates of the first quantum), the value of admissible monetary losses $R_{max.allow.}$ The admissibility of these losses is established by the subject to whom the information belongs, who also manages the security of the object as a whole and its risks.

With the help of the graph is the maximum allowable value of the probability of risk $p_{r\ max.allow.}$, which is matched by the bandwidth of the channel $C_{max.allow.}$. Using the graph of the second quadrant on $C_{max.allow.}$ – is the maximum allowable probability of error in the channel $p_{max.allow.}$ and using the graph of the third quadrant – the required maximum allowable value of the signal-to-noise ratio $\delta_{max.allow.}$ Execution of the received relation $\delta_{max.allow.}$ at the input of the receiver interception in the technical channel of leakage, will ensure a given security risk $R_{max.allow.}$.

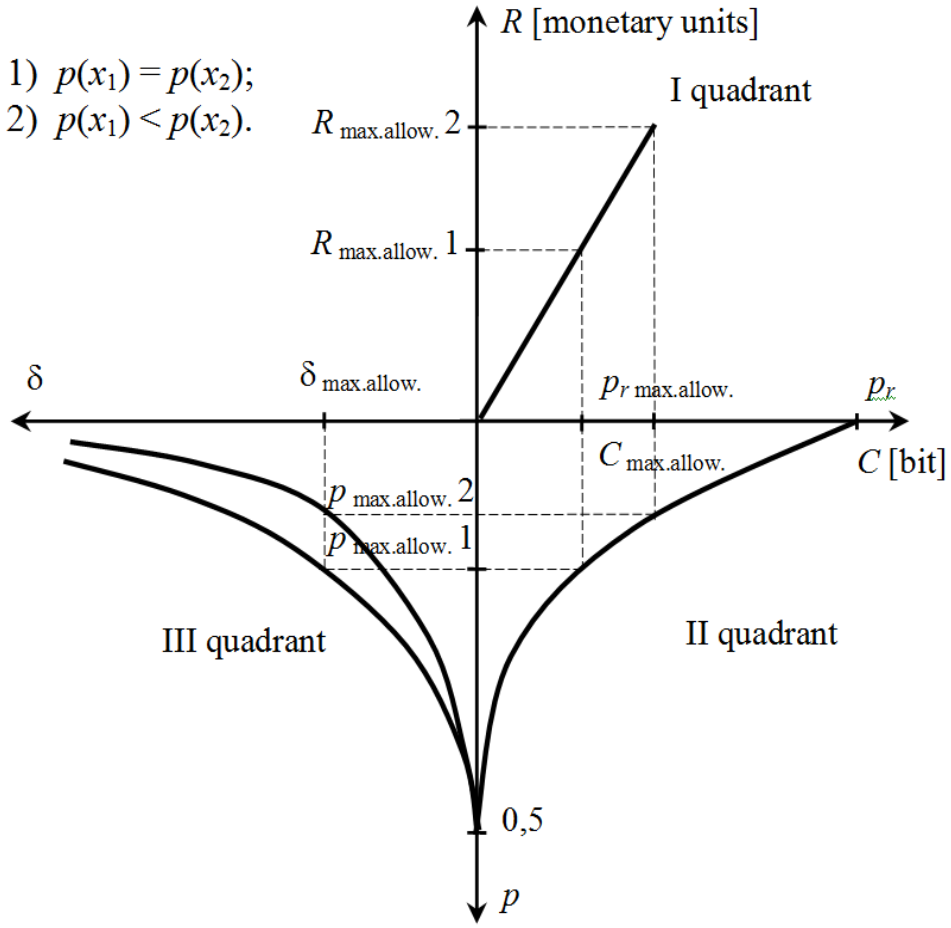

Figure 2: Graphical representation of the principle of calculating the set of risk-oriented indicators of information security from leakage through technical channels

These indicators represent a certain hierarchical structure, where the indicators of the lower levels ensure the implementation of the indicators of the upper levels of the hierarchy.

$$\delta \to p \to C \to p_r \to R\,, \tag{14}$$

and the established restrictions of indicators of the top levels create conditions for finding of admissible limits of indicators of the lower levels of hierarchy.

$$R_{max.allow.} \to p_{r\ max.allow.} \to C_{max.allow.} \to \\ \to p_{max.allow.} \to \delta_{max.allow.}. \tag{15}$$

A special convenience of using the proposed set of indicators is that they allow the use to protect information from leakage of technical channel of leakage not only the traditional method of noise, but also other methods, such as methods of random coding, randomization and more.

Indicators of information security with the use of modern means of receiving physical media and processing their values during the work of object of information activity allow automation of their control, analysis and adjustment, and risk management – information security management in general.

3. Conclusions

The set of risk-oriented indicators of information security from leakage through technical channels for modern ITS is substantiated. This set represent a certain 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. Risk is a measure of information security at the object of information activity at the general upper level of the hierarchy, at the lower, physical level – the signal-to-noise ratio. The indicators of the lower levels ensure the implementation of the indicators of the upper levels of the hierarchy, and the maximum admissibility of the indicators of the upper levels determines the degree of admissibility of the indicators of the lower levels of the hierarchy.

The set of reasonable risk-oriented security indicators take into account the imbalance of signs and allow their automated control, analysis, adjustment and management of information security. The obtained relationships that establish a relationship between indicators can be implemented by real means, in real time.

4. 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] 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, (2002) http://www.cl.cam.ac.uk/techreports.

[4] 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.

[5] Decree Law of Ukraine "On Information" (1992).

[6] Law of Ukraine "On Basic Principles of Cyber Security of Ukraine" (2017).

[7] Decree of the President of Ukraine №392 / 2020 On the Decision of the National Security and Defense Council of Ukraine of September 14, 2020 "On the National Security Strategy of Ukraine".

[8] Law of Ukraine "On Personal Data Protection" (2010).

[9] Information technology. Security techniques. Information security management systems. Requirements [ISO/IEC 27001:2013].

[10] Ivanchenko, S.O.: Justification safety risk information about its security from leaking by technical channels. Scientific and technical digest "Legal, regulatory and metrological support of information security in Ukraine", NTUU "KPI" SRC "Tezis": Kyiv, № 1 (31), pp. 9 – 13 (2016).

[11] Fink L. M.: The theory of transfer of discrete messages [2-d edition], Sov. Radio: Moskva, (1970).

[12] Bronshtein, Y.N., Semendiaev, K.A.: Handbook on mathematics for engineers and students of high schools. Nauka: Moskva, Ch. ed. Phys-Math. Lit. (1986).

[13] Ivanovsky, R.I.: Theory of probability and mathematical statistics. BHV: Petersburg (2008).