Protection of Information from Leakage by Technical Channels for Sources with Non Range Distribution of Probability

Igor Korobiichuk[1*[0000-0002-5865-7668]], Serhii Ivanchenko[2[0000-0003-1850-9596]], Oleksii Havrylenko[3[0000-0002-9552-5832]], Anatolij Golishevsky[4[0000-0001-9981-7771]], Serhii Hnatiuk[4[0000-0002-1541-7058]], Ruslan Hryshchuk[5[0000-0001-9985-8477]]

[1]Warsaw University of Technology, Institute of Automatic Control and Robotics, Warsaw, 02-525, Poland
i.korobiichuk@mchtr.pw.edu.pl
[2]National technical university of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Institute of special communication and information protection, Kyiv, 03056, Ukraine
soivanch@ukr.net,
[3]National Aviation University, Kyiv, 03058, Ukraine
gavrylav@gmail.com
[4]National scientific research institute of special communications and information protection of Ukraine, Kyiv, 03142, Ukraine
tolyan207@ukr.net, gnatyk-2@i.ua
[5]Sergey Korolyov Zhytomyr Military Institute, Cybersecurity Department of the Research Center, Zhytomyr, 10004, Ukraine
dr.hry@i.ua

Abstract. Made reasoning of the information protection from leakage through technical channels for uneven distribution of source probabilities and set the negative sequences in case of its non-consideration. Shown relations of probability information security risk conditions with power at the input of intercept receiver and given requires analytical values, which allow to assess the risk relative to the current signal/noise ratio and for the given probability of the safety risk of the required values of the maximum allowable indicators, namely the throughput of the technical channel of leakage, the probability of correct reception with possible interception and the signal/noise ratio. These ratios differ from previously known by those that take into account the uneven distribution of the signs probability on output of the source of leakage. Ratios allow automated analysis of information security risk in real time with the use of modern information systems and technologies.

Keywords: information, security, protection, risk, information leak, technical channel of leakage.

1. Introduction

As is well known, functioning of almost modern technical means and systems of information processing and transfer related with quantized electromagnetic energy which circulating by its circuit implementations using electromagnetic fields, electric currents, optical energy, etc. Its – energy, which is the carrier of discrete data or information in a continuous environment and, actually, within its own properties as energy conservation law, almost always accompanied by a list of adverse effects [1-7]. These effects are: unwanted radiation of electromagnetic fields to the environment, which can spread over long distances from hardware of information processing; the impact of these fields to technical means, which have galvanic and other connections with the world; leakage of information to conductive conductors of electric currents: power supply network, grounding system, connecting lines or subscriber network of free access [8].

During processing of information with restricted access by technical means mentioned above is a certain class of threats, which is implemented by using of special means of interception. These special means may have different degrees of complexity and efficiency depending on the value of the information and the interest in outsiders knowing. The value of information is a determining factor for possible efficiency involved in interception technical means and the degree of protection of information from leakage.

The balance of protection and threats determine the security of information, and a measure of balance – its safety guarantee, which as a result of the natural factors influence may be characterized by a probability of safety risk [9-11]. This probability is an integral part, which is used by the Bayesian criterion for direct risk assessment [12-15]. A separate case of this criterion is the Kotelnikov criterion, which uses the construction of an optimal receiver and the mathematical justification of its decisive scheme as the best of all possible receiver circuits [16-19]. The decisive scheme provides an opportunity to substantiate the relationship of probabilistic indicators of the channel with the energy indices of carriers (the signal/noise ratio) at the input of the idealized receiver. Accordingly, the application of this approach to protecting information from leakage through technical channels may allow the justification of signal/noise ratio limitations that are permissible in places of possible interception and provide the desired probability of a security risk.

However, the existing assessments of receivers quality, as rule, have orientation on communication channels. It is hypothetically considered, that the best channels and channel sources are the sources and channels that respectively produce and transmit the largest amount of information [16, 17]. It is obvious that under these circumstances, the assumption concerning the equivalence of source symbols, which uses the existing substantiation of the solving schemes, is quite feasible and permissible.

For receivers that can be considered as means of interception, such an assumption is inadmissible, since for information leakage channels in comparison with communication channels is set the opposite task, namely, the impossibility of leakage of information [16, 17]. The real sources may have a different probability distribution. There-

fore, the security of information should be based not only on the equivalence of source symbols, but also on uneven distribution.

So, the actual task is analyzing the protection of information from leakage by technical channels for uneven distribution of source probabilities, which should provide reliable protection of modern technical means and systems of information processing and transmission.

2. Materials and methods of research

Let the technical channel of leakage be given as a discrete-continuous one (Fig. 1). Let for simplicity as a source of information leakage is used a binary discrete source X, which produces signs x_r, where $r = 1$ and 2. Each of the signs in the technical processing means is represented by the intermediation of some continuous-time signals implementation $s_1(t)$ and $s_2(t)$. The implementation of each other is different in that, so that the technical means can distinguish them and, accordingly, identify them with signs x_1 and x_2. On the channel scheme on Fig.1 an element of this identification appears by "modulator".

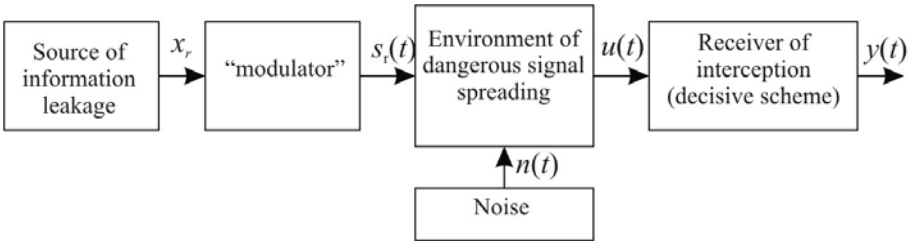

Fig. 1. Discrete-continuous channel as a technical channel of information leakage

Let the implementation $s_1(t)$ та $s_2(t)$ are finite in spectrum and have the same duration T. In the environment of the spreading a dangerous signal, forming a technical channel of leakage, there is a noise that distorts it and prevents interception of information. Noises can have a variety of characters of origin and influence and different degrees of chance and the associated masking properties. The analysis of the literature shows that most distorting effect has additive noise with normal distribution of probabilities [1, 2, 6-8, 14-17]. Unlike the others, this type of noises is quite common in natural environments of signal propagation, has a mathematical description of the density of probability distribution and allows the justification of the security with a proven guarantee of reliability [6, 7, 16, 17].

Other noises also can distort signals, revealing masking property. However, the effect of masking by them is still determined by the proximity with normal distribution law. Otherwise, their presence is defined as a protection margin. Including this, the masking efficiency of these noises is not taken in calculations.

Let the normally distributed noise has additive action to a dangerous signal in the channel, in ideally – white noise $n(t)$. At the output of the channel is formed a mixture which enters the receiver input:

$$u(t) = \mu s_r(t-\tau) + n(t) = c_r(t) + n(t), \tag{1}$$

where $c_r(t) = \mu s_r(t-\tau)$ is attenuated signal with time delay; μ is channel transmission ratio; τ is signal delay time in the channel.

The task of the receiver of interception is to analyze *u(t)* and making a decision y_r about the sign x_r at the output of the leakage source. Obviously, that the more true this solution, then interception will be more effective and the source of information leakage will be less protected.

Probability of security risk $p_{risk.}$ can match the fate of information, that, without violating of information security, is permissible can flow through by technical channels. In accordance, this part can be providing by bandwidth - the ability of the technical channel of leakage, expressed in relative units:

$$p_{risk.} \le \frac{C_{TCL}}{C_{TCL\max}}, \tag{2}$$

where for a discrete symmetric channel with transmission reliability q bandwidth is equal to [16, 17, 20, 21]:

$$C_{TCL} = 1 + q\log_2 q + (1-q)\log_2(1-q)\ [\text{bit}], \tag{3}$$

At that, the maximum bandwidth per expression (3) is achieved on condition q = 1 or q = 0 and equals, minimum, which is desirable for the technical channel of leakage, provided that the probability of the false and correct character transfer is equal 1 – $q = q$ (Fig. 2).

Compliance with minimum transmission reliability q = 0 and the maximum of bandwidth can be explained by the fact that on the receiving side can be used inverter. It will result in the redistribution of arrows on Fig. 2 and will cause compliance $x_1 \to y_2$ and $x_2 \to y_1$. At that q must be replaced $1 - q$ and become equal to 1. Equality same $p = q$ makes the output of the channel completely uncertain, similar to the random character generator.

As follows, having the maximum permissible probability of information security risk, it is possible to determine the maximum allowable bandwidth $C_{TCL\,max.per.}$ the technical channel of leakage and by solving the equation (3) – the maximum allowed probability of correct interception $q_{max.\ per.}$ of one binary sign x_r, r = 1 and 2.

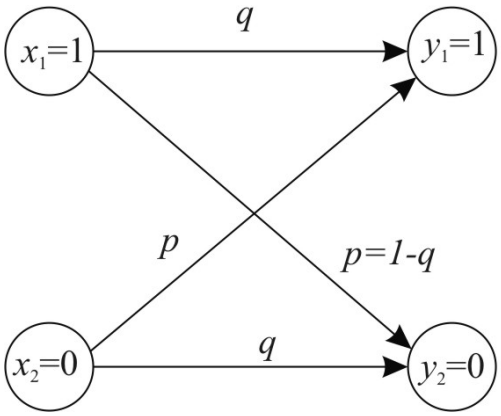

Fig. 2. A graph of states of a discrete symmetric channel without memory

Relative to the decisive scheme of the ideal receiver, by the theory of potential noise immunity for a discrete-continuous channel, the probability of an error, which is determined by the formula:

$$p = F\left(-\frac{1}{2}\sqrt{\frac{P_\Delta T}{N_0}}\right), \tag{4}$$

where $F(...)$ – Laplace integral:

$$F(\zeta) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\zeta}\exp\left\{-\frac{\eta^2}{2}\right\}d\eta, \tag{5}$$

P_Δ is the power of the difference signal $c_\Delta(t) = c_1(t) - c_2(t)$:

$$P_\Delta = \frac{1}{T}\int_0^T c_\Delta^2(t)dt, \tag{6}$$

where N_0 – spectral density of noise in the technical channel of leakage.

In accordance, the authenticity of receiving a binary sign will be based on the formula:

$$q = 1 - p = F\left(\frac{1}{2}\sqrt{\frac{P_\Delta T}{N_0}}\right), \tag{7}$$

But the formula of estimation of probability of error (4) predicts the equivalence of source symbols $p(x_1) = p(x_2)$. As already noted above, for the modern means of

information processing and transmission, such an assumption can not always be performed, and therefore founded by the formula (4) probability is not always correct.

Provided $p(x_1) \neq p(x_2)$ the decisive scheme must be built by implementing inequality:

$$p(x_l)\lambda_{l/0}(u) > p(x_r)\lambda_{r/0}(u), \tag{8}$$

where $\lambda_{kr/0}(u) = \lambda_{r/0}(u_1, u_2, ..., u_k)$ – k-dimensional relation of plausibility:

$$\lambda_{kr/0}(u) = \frac{\omega_k(u / x_r)}{\omega_k(u / x_0)}, \tag{9}$$

where l is the index of the correct decision, x_0 is mark of no sign on the output of the source, $\omega_k(u/x_r) = \omega_k(u_1, u_2, u_3, \ldots, u_k/x_r)$ is conditional k-dimensional density of distribution of counts receiver reading.

If the frequency spectrum of signs realizations is finite in time and is completely concentrated in the band of frequencies F, then by the Kotelnikov theorem, the number of readings counts can be limited to the number $k = 2FT$, therefore:

$$\lambda_{r/0}(u_1, u_2, ..., u_{2FT}) = \frac{\omega(u_1, u_2, ..., u_{2FT} / x_r)}{\omega(u_1, u_2, ..., u_{2FT} / x_0)}. \tag{10}$$

If in the "modulator" for sign x_0 is associated with so-called zero implementation $c_0(t)$, for example, input channel gets nothing, in accordance with the formula (1) at the output there will be only a noise process:

$$u(t) = c_0(t) + n(t) = n(t). \tag{11}$$

Due to the properties of white noise on the statistical independence of its conditional density of its reading counts, the denominator of the ratio (10) can be expressed in the form of a product of one-dimensional densities of the normal distribution law:

$$\omega(u_1, u_2, ..., u_{2FT} / x_0) = \prod_{i=1}^{2FT} \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{u_i^2}{2\sigma^2}} = \frac{1}{(\sigma\sqrt{2\pi})^{2FT}} \exp\left\{-\frac{1}{2\sigma^2}\sum_{i=1}^{2FT} u_i^2\right\}, \tag{12}$$

For r-th implementation using additivity properties of noise in the channel:

$$\begin{aligned}\omega(u_1, u_2, ..., u_{2FT} / x_r) &= \omega(u_1 - c_{r1}, u_2 - c_{r2}, ..., u_{2FT} - c_{r2FT} / x_0) = \\ &= \frac{1}{(\sigma\sqrt{2\pi})^{2FT}} \exp\left\{-\frac{1}{2\sigma^2}\sum_{i=1}^{2FT}(u_i - c_{ri})^2\right\}.\end{aligned} \tag{13}$$

Substituting ratio (12) and (13) into the formula (10), we will get:

$$\lambda_{r/0}(u_1,u_2,...,u_{2FT}) = \exp\left\{\frac{1}{2\sigma^2}\sum_{i=1}^{2FT}u_i^2\right\}\exp\left\{-\frac{1}{2\sigma^2}\sum_{i=1}^{2FT}(u_i - c_{ri})^2\right\}. \quad (14)$$

Taking advantage of the property the noise ergodicity, its dispersion can be replaced by the power expressed in terms of spectral density N_0 in the bandwidth F:

$$\sigma^2 = P_z = N_0 F\,. \quad (15)$$

After inclusion in the ratio (14) replacement (15) and direction $\Delta t \to 0$ the plausibility ratio will look:

$$\lambda_{r/0}(u) = \lim_{\Delta t\to 0}\exp\left\{\frac{1}{N_0}\sum_{i=1}^{2FT}u_i^2\Delta t\right\}\exp\left\{-\frac{1}{N_0}\sum_{i=1}^{2FT}(u_i - c_{ri})^2\Delta t\right\} =$$

$$= \exp\left\{\frac{1}{N_0}\left[\int_0^T u^2(t)dt - \int_0^T (u(t)-c_r(t))^2 dt\right]\right\}. \quad (16)$$

Substituting (16) into inequality (8) and applying a logarithm for the right and left parts of the inequality by a natural logarithm, we get:

$$p(x_l)\exp\left\{\frac{1}{N_0}\left[\int_0^T u^2(t)dt - \int_0^T (u(t)-c_l(t))^2 dt\right]\right\} > p(x_r)\exp\left\{\frac{1}{N_0}\left[\int_0^T u^2(t)dt - \int_0^T (u(t)-c_r(t))^2 dt\right]\right\}$$

or

$$\frac{1}{T}\int_0^T u(t)c_l(t)dt - \frac{P_l}{2} + \frac{N_0}{2T}\ln p(x_l) > \frac{1}{T}\int_0^T u(t)c_r(t)dt - \frac{P_r}{2} + \frac{N_0}{2T}\ln p(x_r)\,. \quad (17)$$

In accordance with the inequality (17) the decisive scheme of an ideal receiver for all r must calculate and compare the right and left parts and for the maximum of found result make a decision y_l about the sign x_l produced by the source. Since the right and left sides of the inequality contain random components, there are probabilities of the existence of this and the opposite inequalities. Obviously, the probability of inequality (17) is the probability of a correct solution, and the probability of the opposite inequality is the probability of error.

The probability of a correct solution on average can be found as a expected value for all realizations r:

$$q = p(x_1)\,p(y_1/x_1) + p(x_2)\,p(y_2/x_2)\,. \quad (18)$$

For a binary source, if the correct solution is x_1, inequality (17) can be converted to the form:

$$\frac{1}{T}\int_0^T c_\Delta(t)n(t)dt > -\frac{P_\Delta}{2} - \frac{N_0}{2T}\ln\frac{p(x_1)}{p(x_2)}$$

or

$$p(y_1 / x_1) = p\left\{\xi > -\frac{P_\Delta}{2} - \frac{N_0}{2T}\ln\frac{p(x_1)}{p(x_2)}\right\}, \tag{19}$$

where $\xi = \frac{1}{T}\int_0^T c_\Delta(t)n(t)dt$ is a normally distributed random variable with expected value $M[\xi] = 0$ and dispersion $D[\xi] = \frac{N_0 P_\Delta}{T}$ [13, 14, 17, 18].

3. The results of research

Let's analyze the nature of throughput for the general case and justify communication of maximum throughput and needed for ensure probability of errors. In this case will suppose, that data, which simultaneously can be processed by technical means and flow by technical channels, can have very different origins, that is generated from Q different information sources with a different syntax and different semantics (Fig. 2).

Expressed with the help of Laplace integrals [19, 20]:

$$p(y_1 / x_1) = F\left(\frac{1}{2}\sqrt{\frac{P_\Delta T}{N_0}} + \frac{1}{2}\sqrt{\frac{N_0}{P_\Delta T}}\ln\frac{p(x_1)}{p(x_2)}\right) \tag{20}$$

and

$$p(y_2 / x_2) = F\left(\frac{1}{2}\sqrt{\frac{P_\Delta T}{N_0}} - \frac{1}{2}\sqrt{\frac{N_0}{P_\Delta T}}\ln\frac{p(x_1)}{p(x_2)}\right). \tag{21}$$

It should be noted that if $p(x_1) = p(x_2)$ the formula (18) in conjunction with (20) and (21) will match the formula (7).

In the case of $p(x_1) \neq p(x_2)$ were obtained the quantitative values of the probability of correct reception for multiply-polar, orthogonal signals and signals with zero realization. The character of the probability dependence of the correct receiving from the attitude $\frac{p(x_1)}{p(x_2)}$ presented on Fig. 3.

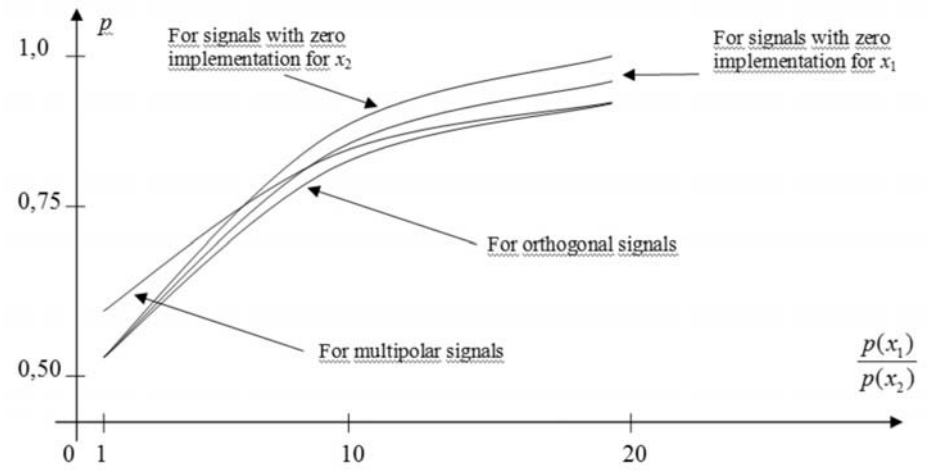

Fig. 3. A graph of the probability of correct receiving of signs related probabilities output source

As can be seen from the graphs, with the same energy conditions on the channel input, provided equal probability symbols on the source output $\frac{p(x_1)}{p(x_2)} = 1$ the security of the multipolar signals is less (the probability of correct receiving is greater) than for orthogonal signals and signals with zero realization. Provided unequal probabilities of signs $\frac{p(x_1)}{p(x_2)} > 1$ there is a tendency to decrease security (increases of probability of correct receiving). At that a large variation of the signs probability, for example $\frac{p(x_1)}{p(x_2)} = 20$ for signals with zero realization, leads to increased probability of correct reception compared to orthogonal and different polar signals. Probabilities is receiving for the last two with this distortion are same.

It should also be noted, that with an increase in the distortion of probabilities of signs of the probability of correct receiving approaching the greater probability of signs. This is not difficult to explain using the formula (18), taking $p\left(y_1/x_1\right) \approx 1$ and $p\left(y_2/x_2\right) \approx 0$. So, according to the formula (18):

$$q \approx p\left(x_1\right) \times 1 + p\left(x_2\right) \times 0 = p\left(x_1\right).$$

An analysis of the dependence of the probability of a correct reception on the signal/noise ratio under the condition of strong distortion of the signs probabilities (Fig. 4).

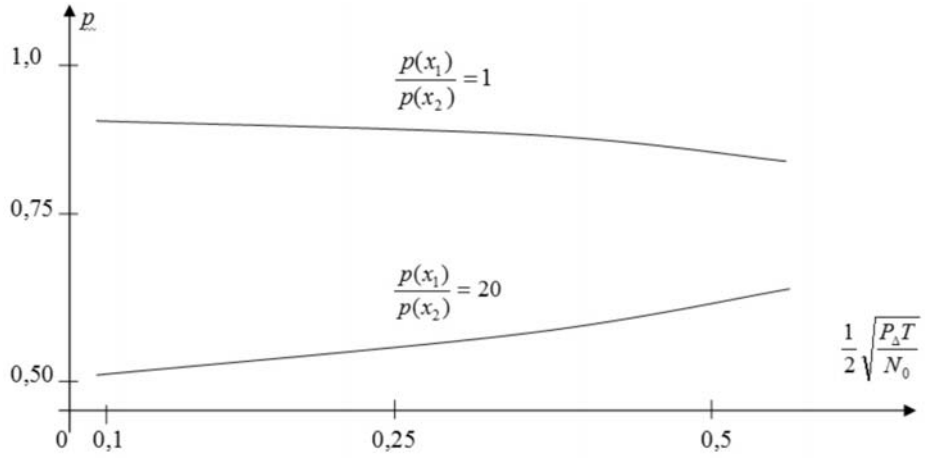

Fig. 4. Graph of the dependence of the probability of correct reception on the signal / noise ratio at the receiver input

It is shown that with increasing the level of noise in relation to the signal under the condition of equal probabilities of signs at the output of the source $\frac{p(x_1)}{p(x_2)}=1$ probability of correct receiving usually decreases. In the case of strong distortion of signs probabilities, for example, when $\frac{p(x_1)}{p(x_2)}=20$, under the same conditions with an increase in the level of noise in relation to the signal there is an opposite effect – increasing of correct receiving probability. That is, with a strong distortion of the signs probability increasing the noise over the signal does not improve the masking of a dangerous signal, but on the contrary - improves the conditions for interception.

Thus, made reasoning of the information protection from leakage through technical channels for uneven distribution of source probabilities and set the negative sequences in case of its non-consideration. Shown relations of probability information security risk conditions with power at the input of intercept receiver and given requires analytical values. These resulting formulas provide for the use of intermediate indicators: the throughput of the technical channel of information leakage and the probability of correct reception of messages relative to the ideal receiver.

The resulting ratios allow estimating the information security risk related on the current signal/noise ratio for the given probability of risk the required values of the maximum allowable indicators, for example, the throughput of the technical channel of leakage, the probability of correct receiving with possible interception and the signal/noise ratio. These ratios differ from previously known by those that take into account the uneven distribution of the signs probability on output of the source of leakage. This unequal signs probability can take place in practice, and therefore should be

taken into account in the calculation of the protection of real hardware, information processing and transmission systems.

Conclusions

Ratios allow automated analysis of information security risk in real time with the use of modern information systems and technologies. Their use has obtained practical results that show the dependence of the probability of true interception from ratio of probabilities of signs at the source output and the signal/noise ratio at the input of the ideal receiver. It is shown that in the case of a strong distortion of the signs probabilities, the masking influence of the noises changes to the opposite than for the equal probabilities of these signs. That is, increasing the level of noise does not increase, but reduces security.

The above is advisable to take into account in the calculation of security information from its leaks.

References

1. Buzov, G.A., Kalinin, S.V., Kondratev, A.V.: Protection of information from leaks through technical channels. Goryachaya liniya, Telecom: Moskva (2005).
2. Parshutkin, A.V., Levin, D.V., Zaytsev, S.A., Egin, A.V.: Application of structural interference for data protection from information Leakage in the stray electromagnetic radiations channel. SPIIRAS Proceedings, 3 (58), pp. 160-181 (2018) doi: 10.15622/sp.58.7
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. Kuhn, M.G.: Electromagnetic eavesdropping risks of flat-panel displays. Lecture Notes in Computer Science, 3424, pp. 88-107 (2005)
5. Kuhn, M.G.: Optical time-domain eavesdropping risks of CRT displays. Proceedings - IEEE Symposium on Security and Privacy, 2002-January, art. no. 1004358, pp. 3-18 (2002) doi: 10.1109/SECPRI.2002.1004358
6. Lenkov, S.V., Peregudov, D.A., Horoshko, V.A.: Methods and means of information protection. Tom I. Unauthorized receipt of information. Ariy: Kyiv (2008)
7. Qiu, J., Li, H., Zhao, C.: Cancelable palmprint templates based on random measurement and noise data for security and privacy-preserving authentication. Computers and Security, 82, pp. 1-14 (2019) doi: 10.1016/j.cose.2018.12.003
8. Korobiichuk, I., Dobrzhansky, O., Kachniarz, M.: Remote control of nonlinear motion for mechatronic machine by means of CoDeSys compatible industrial controller. Tehnički vjesnik/Technical Gazette, Vol. 24/No. 6, pp. 1661-1667 (2017) doi: 10.17559/TV-20151110164217
9. Information technology. Security techniques. Information security management systems. Requirements [ISO/IEC 27001:2013].
10. Korobiichuk I.V., Hryshchuk R.V., Horoshko V.O., Hokhlacheva Yu.E. Self-diagnostics of complex systems with a software-configurable structure. Informatics and Mathematical Methods in Simulation, vol 8, No. 1, pp. 36-47 (2018)

11. Korobiichuk, I., Hryshchuk, R., Mamarev, V., Okhrimchuk, V., Kachniarz, M.: Cyberattack Classificator Verification. International Conference on Diagnostics of Processes and Systems DPS 2017: Advanced Solutions in Diagnostics and Fault Tolerant Control, pp. 402-41 (2018) doi: 10.1007/978-3-319-64474-5_34
12. Ivanovsky, R.I.: Theory of probability and mathematical statistics. BHV: Petersburg (2008)
13. Niyato, D., Hossain, E.: A queuing-theoretic and optimization-based model for radio resource management in IEEE 802.16 broadband wireless networks. IEEE Transactions on Computers, 55 (11), pp. 1473-1488 (2006) doi: 10.1109/TC.2006.172
14. Isakov, V.N.: Statistical theory of radio engineering systems. ARI: Moskva (2007)
15. Couillet, R., Debbah, M.: Random matrix methods for wireless communications. Random Matrix Methods for Wireless Communications, 9781107011632, pp. 1-539 (2011) doi: 10.4324/CBO9780511994746
16. Burachenko, D.L., Zavaryn, H.D., Kliuev, N.Y., et. al.: General Theory of communication. VAS: Leningrad (1970).
17. Lee, M., Neifeld, M.A., Ashok, A.: Capacity of electromagnetic communication modes in a noise-limited optical system. Applied Optics, 55 (6), pp. 1333-1342 (2016) doi: 10.1364/AO.55.001333
18. 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)
19. Duc, A., Faust, S., Standaert, F.-X.: Making masking security proofs concrete: Or how to evaluate the security of any leaking device. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 9056, pp. 401-429 (2015) doi: 10.1007/978-3-662-46800-5_16
20. Fink, L. M.: The theory of transfer of discrete messages. [2-d edition], Sov. Radio: Moskva (1970)
21. Kulkarni, A.N., Bukate, R.R., Nanaware, S.D.: Study of Various Attacks and Routing Protocols in MANETS. 2018 International Conference on Information, Communication, Engineering and Technology, ICICET 2018, art. no. 8533696 (2018) doi: 10.1109/ICICET.2018.8533696
22. Bronshtein, Y.N., Semendiaev, K.A.: Handbook on mathematics for engineers and students of high schools. Nauka: Moskva, Ch. ed. Phys-Math. Lit. (1986)
23. Ram, M., Davim, J.P.: Mathematics applied to engineering. Mathematics Applied to Engineering, pp. 1-210 (2017) doi: 10.1016/C2015-0-06715-6