The Throughput of Technical Channels as an Indicator of Protection Discrete Sources from Information Leakage

Igor Korobiichuk[1*[0000-0002-5865-7668]], Serhii Ivanchenko[2[0000-0003-1850-9596]], Oleksandr Roma[2[0000-0001-9074-6137]], Anatolij Golishevsky[3[0000-0001-9981-7771]], Ruslan Hryshchuk[4[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, proffesor69@ukr.net
[3]National scientific research institute of special communications and information protection of Ukraine, Kyiv, 03142, Ukraine
tolyan207@ukr.net
[4]Sergey Korolyov Zhytomyr Military Institute, Cybersecurity Department of the Research Center, Zhytomyr, 10004, Ukraine
dr.hry@i.ua

Abstract. Considered the theoretical conditions of discrete information sources security, analyzed the throughput as an indicator of its protection from information leaks. Introduced the notion of throughput limit values of information leaks channel, proposed its use as a security norms. The resulting values establish a connection of specified index with the desired probability of error in the channel.

Keywords: information, information security, security risk, safety of information, technical channels of information leakage, technical information protection.

1. Introduction

One of the tasks of information security management [1, 2], as determined Deming-Shewhart cycle, is a security risk analysis, including risk of a breach of information security from leaking by technical channels. It is known, that work of technical means and systems of processing and transmission of information is almost always accompanied by a list of adverse effects [3-12]. These are unwanted radiation of electromagnetic fields to the environment, emission and leakage of electric current to taking off conductors. These carriers may arise from information sources and uncontrolled spread the dangerous signals outside the controlled area.

It is known, that the criterion of protection is the condition of impossibility extract semantic content from intercepted message [1, 2], that at the point of interception is

determined certain of energy terms – norm the signal/noise ratio. In turn, a quantitative norm of this measure must provide authentically needed probability of error in technical leakage channel and, in accordance, previously specified security risk [1, 12-14]. For substantiation of dependence signal/noise ratio with probability of error in work [13, 14] was based on the Kotelnikov's optimum receiver [15-18]. In its relation was found the assessment of lower limit of the probability of errors in the channel, determined by allowable signal/noise ratio and does not depend from choose of interception receiver. As is evident, determining the desired probability of error in the technical leakage channels requires certain studies and solutions.

So, the main task of this article is justification the technical channel throughput as indicator of protection discrete sources from information leakage, and also justification the dependency of this throughput with the necessary probability of error in the technical leakage channel, that will provide a given state of information security risk by given parameters.

2. Materials and methods of research

To resolve this specified task, consider the channel of leakage, as discrete channel, which connects a source of information and enemy receiver with some non-fixed, but different from zero probability of error (Fig. 1).

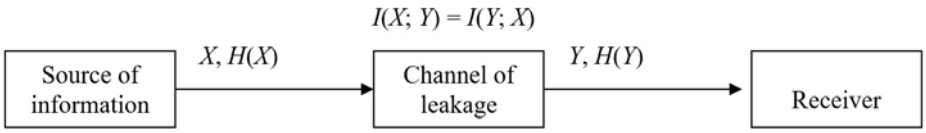

Fig. 1. Discrete channel of information leakage

Suppose at the input channel of information sources gets some information sequence data X^n_k, for ease, binary symbols, where k – number of combination (k = 1, 2, 3,…, 2^n) with probability $p(X^n_k)$. The specified probability $p(X^n_k)$ – is a priori probability, which characterizes the chances of guessing by enemy before it is transmitted through the channel.

In the channel under the influence of noise sequence X^n_k transformed into some consistency Y^n_l the same length and the same alphabet symbols, where l – number of combination (l = 1, 2, 3,…, 2^n). Noise is random nature, that's why this transformation can be described by conditional probability $p(Y^n_l/X^n_k)$, which is a measure that determines possibility of transition sequences X^n_k to Y^n_l. In this case a posteriori probability, which determines the chances of guessing the information signs by enemy, after taking its continuous implementation, can be expressed by the Bayes formula:

$$p(X_k^n / Y_l^n) = \frac{p(X_k^n)p(Y_l^n / X_k^n)}{p(Y_l^n)}, \quad (1)$$

where

$$p(Y_l^n) = \sum_{k=1}^{2^n} p(X_k^n) p(Y_l^n / X_k^n) \tag{2}$$

– the probability of sequence Y^n_l at the output of channel.

For the given channel its throughput is defined as the maximum amount of information for all possible its implementation for all probability allocations, which can be transmitted through the channel, [19 - 22]:

$$C = \max_X I(X;Y), \tag{3}$$

where

$$I(X;Y) = H(X) - H(X/Y) = H(Y) - H(Y/X) = I(Y;X) \tag{4}$$

– mutual channel information quantity,

$$H(X) = \mathrm{M}\left[\frac{1}{n}\log_a \frac{1}{p(X_k^n)}\right] = \lim_{n\to\infty}\frac{1}{n}\sum_{k=1}^{2^n} p(X_k^n)\log\frac{1}{p(X_k^n)} \tag{5}$$

– the average amount of information that produces source for one binary sign - absolute source entropy X,

$$H(X/Y) = \lim_{n\to\infty}\frac{1}{n}\sum_{k=1}^{2^n}\sum_{l=1}^{2^n} p(X_k^n, Y_l^n)\log\frac{1}{p(X_k^n/Y_l^n)} \tag{6}$$

– conditional source entropy for a binary sign,

$$H(Y) = \lim_{n\to\infty}\frac{1}{n}\sum_{l=1}^{2^n} p(Y_l^n)\log\frac{1}{p(Y_l^n)}, \tag{7}$$

– unconditional entropy of channel output Y for one binary sign,

$$H(Y/X) = \lim_{n\to\infty}\frac{1}{n}\sum_{k=1}^{2^n}\sum_{l=1}^{2^n} p(Y_l^n, X_k^n)\log\frac{1}{p(Y_l^n/X_k^n)} \tag{8}$$

– conditional entropy of channel output for one binary sign or conversion $X^n_k \to Y^n_l$.

If $k = l$, then the combination of sequences $X^n_k = Y^n_l$ and, in accordance, the transmission in the channel occurred unmistakably. It is not difficult to make sure, that $H(Y/X) = 0$ bit, and C = 1 bit. In other cases there is an error and if it is probability higher, than higher the difference between X^n_k and Y^n_l, than greater distorted of symbols and information lost. In this case $H(Y/X) \to 1$ bit, and C $\to$ 0 bit. It should be noted, that equality of latter achieved by conditions of equal probability and statistic errors independence, but statistical dependence of mistakes, even i by conditions of Its equal probability will result to increased throughput [15-18].

Shannon's information theory also known, that information can freely pass through the channel only on condition, if $C \geq H(X)$. If $C < H(X)$ information through the channel may partially pass and partially lost. On condition, if $C = 0$ bit, than channel condition is provided as "channel breakage" or "no channel".

Condition of "channel breakage" is theoretically idealized condition, which is desirable for all technical information leakage. But in practice it is difficult to reach, and even at all impossible. Typically, ensure of that conditions for the safe processing and transmission of information requires the creation specific objects and building constructions, it is associated with the creation of large-scale controlled areas, using highly efficient surge protector, or autonomous power sources, etc. All it requires large financial and energy costs, which sometimes may not be appropriate because of their dominance over most information precious. Because safety of information should include a balance between deliberately spent and acceptable lost.

In order to optimize the costs of securing technical information leakage requires a list of scientific-technical justifications and solutions, associated with providing small but nonzero values of through. This indicator must take into account the variety of modes of technical processing and transmission items, of which information leakage, features of group transmission channels that combine information from different sources with different properties, the possibility of automated regulation of noise immunity channels, etc.

Considering this throughput of technical leakage channels C_{tlc} can be attributed to indicators of the evaluation of information security. For example, if asked acceptable information security risk, then it possible to put accordance of the limit allowable maximum throughput of technical leakage channel $C_{\text{tlc l.a.}}$. The presence of of this rule allows to find the probability of error in the leakage channel and power conditions in the point of possible interception – the signal/noise ratio, which will ensure the security of information with given permissible risk.

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).

Obviously, that due to the fragmentation of sources for each one, dangerous signal spreading by the same environment, which provides the same signal/noise ratio at the intercept receiver input, technical leakage channel can create different throughput. It is also obvious, if leakage of information from each source consider separately, then shown on Fig. 2 technical channel may consist of several technical channels, generated from different sources with its throughput. But for all of these channels takes place only one receiver, for which need to justify condition of impossibility of information interception.

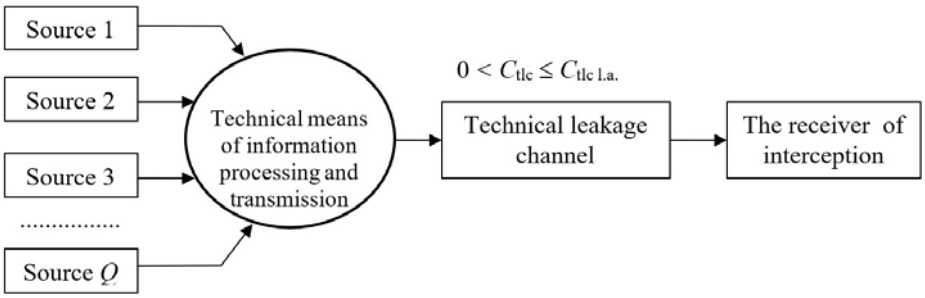

Fig. 2. Typical technical channels of information leakage
for modern technical means of information processing and transmission
with the given limit allowable throughput

Suppose that in leakage channels have a place an errors, the presence of which is guaranteed by noise of environment spreading of dangerous signals. All errors in the channel are statistically independent and are characterized by probability, which is not below some certain of intercept receiver features.

Based on the used in article the definition of throughput, which is expressed by ratios (3), (4), (5), (6), (7) and (8), throughput of technical leakage channel, that calculated on average per one binary sign, may be expressed by the formula [15, 16]:

$$C_{\text{tlc}} \underset{H_{\max}(X)}{=} 1 - H(Y/X) \text{ [bit]} . \tag{9}$$

One of the approaches for ensure the guaranteed safety, is calculation the indicators of security for the worst case in terms of security. In this case protection will be ensured and in the the worst case and in all other cases, with the creation of a certain reserve.

Determining of worst case is requires the inspection of conditions security for all of leakage sources. Therefore, will expression the technical leakage channels throughput as averaging of each source throughput and select among from last limit allowable maximum, which will apply as an indicator of security:

$$C_{\text{tlc}} = \frac{1}{Q}\sum_{r=1}^{Q} C_r . \tag{10}$$

On the other hand, considering (9) and (8) specified throughput will look like:

$$C_{\text{tlc}} = 1 - \lim_{n\to\infty}\frac{1}{n}\sum_{k=1}^{2^n}\sum_{l=1}^{2^n} p(Y_l^n, X_k^n)\log\frac{1}{p(Y_l^n / X_k^n)} . \tag{11}$$

Is necessary to find identity of ratios (10) and (11) and select in throughput of technical leakage channels a maximum component C_r and to accept it as the norm for C_{tlc}.

To do this will analyze of probability in ratio (11).

In view of the independence of errors, mentioned probabilities can be expressed in the form of next ratios.

Conditional probability, which characterizes the possibility of sequence at the output of channel Y^n_l, if at the input came X^n_k:

$$p(Y_l^n / X_k^n) = p(y_1 / x_1)p(y_2 / x_2) \times ... \times p(y_i / x_i) \times ... \times p(y_n / x_n). \quad (12)$$

where $p(y_i/x_i)$ – the probability of in i- grade of sequence Y^n_l the sign - y at the output of channel, If at the input came sign x_i of sequence X^n_k in the same grade.

It is not difficult to notice, that the probability $p(y_i/x_i)$ of additive channel can be expressed as

$$p(y_i/x_i) = p(y_i - x_i) = p(e_i). \quad (13)$$

In view of the (13) the ratio (12) for conditional probability can be expressed in terms of the multiplication of errors probability $p(e_i)$, which taking values within the limits $0 < p(e_i) < ½$ [7].

$$p(Y_l^n / X_k^n) = p(e_1)p(e_2) \times ... \times p(e_i) \times ... \times p(e_n). \quad (14)$$

Compatible probability, which describes the possibility of simultaneous existence on the channel input a sequence X^n_k and on the channel input Y^n_l, equals:

$$p(Y_l^n, X_k^n) = p(X_k^n)p(Y_l^n / X_k^n) = \left[p(x_1)p(x_2) \times ... \times p(x_i) \times ... \times p(x_n)\right] \times \\ \times \left[p(y_1 / x_1)p(y_2 / x_2) \times ... \times p(y_i / x_i) \times ... \times p(y_n / x_n)\right] \quad (15)$$

and considering (13) will view as:

$$p(Y_l^n, X_k^n) = \left[p(x_1)p(x_2) \times ... \times p(x_i) \times ... \times p(x_n)\right] \times \\ \times \left[p(e_1)p(e_2) \times ... \times p(e_i) \times ... \times p(e_n)\right], \quad (16)$$

where $p(x_i)$ – probability of x_i - sign on the channel output.

Inserting (14) and (16) to (11) and simplifying its, we get next:

$$C = \lim_{n \to \infty} \frac{1}{n} \sum_{i=1}^{n} \left[1 + \sum_{e} p(e_i) \log_2 p(e_i)\right] = \lim_{n \to \infty} \frac{1}{n} \sum_{i=1}^{n} C_i, \quad (17)$$

where C_i – channel throughput for i- information sign.

Equating $Q = n$, we get the required identity, where

$$C_{\text{tlc l.a}} = \max_{i,n,Q} C_i = 1 + \sum_e p(e_i) \log_2 p(e_i) \tag{18}$$

It should be noted, that the ratio (14), which expresses technical leakage channels throughput, is multidimensional convex downwards function of the probability of errors $p(e_i)$. It is not difficult to verify, taking by all arguments the second derivative and identifying a sign. The specified can be shown graphically for arguments $p(e_i)$, having fixed everyone else in the range from 0 to 1/2 (Fig. 3):

$$p(e_j) = \text{const}, \; 0 < p(e_j) < 1/2 \text{ for all } j = 1, 2, \ldots, n, j \neq i. \tag{19}$$

As seen from the graphical representation of throughput, ensuring its limit allowable value $C_{\text{l.a.}}$ for different values i can be determined different values of errors probability.

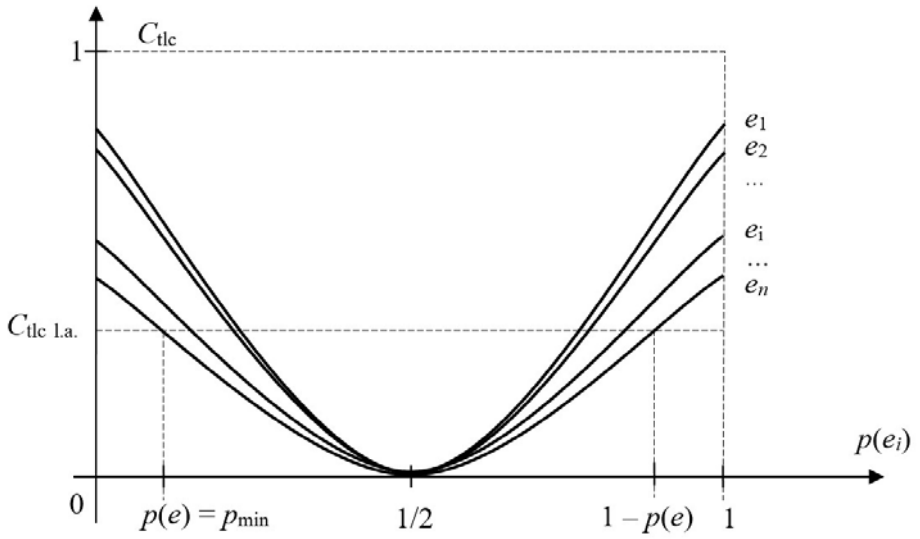

Fig 3. Graphs of dependence of throughput leakage sources from errors probability in the technical channel

Assertion. If asked a discrete binary channel for which presence of errors is guaranteed, all errors are statistically independent and their probabilities for all i ($i = 1, 2, \ldots, n$) are within the limits $p_{\min} \le p(e_i) \le 1 - p_{\min}$, then its throughput by average does not exceed limit allowable value as expressed by the ratio:

$$C_{\text{l.a}} = 1 + p_{\min} \log_2 p_{\min} + (1 - p_{\min}) \log_2 (1 - p_{\min}) \ge C \tag{20}$$

The proof. If you know the errors probability $p(e_i)$, then throughput channel for i-information signs may be expressed by ratio:

$$C_i = 1 + \sum_e p(e_i)\log_2 p(e_i) = 1 + p(e_i)\log_2 p(e_i) + \\ +(1 - p(e_i))\log_2(1 - p(e_i)) = 1 - h(p(e_i)) \quad (21)$$

where $h(p) = p\log_2\frac{1}{p} + (1-p)\log_2\frac{1}{(1-p)}$ – entropy function of the argument p.

From the convexity properties of entropic function $h(p)$ and its symmetry from $p = 1/2$ it follows that for argument $p \in (p_{\min}; 1 - p_{\min})$ its value is limited from below:

$$h(p) \geq h_{\min} = p_{\min}\log_2\frac{1}{p_{\min}} + (1 - p_{\min})\log_2\frac{1}{(1 - p_{\min})}, \quad (22)$$

and throughput from top

$$C_i \leq C_{\text{gr.d}} = 1 + p_{\min}\log_2 p_{\min} + (1 - p_{\min})\log_2(1 - p_{\min}). \quad (23)$$

Inserting inequality (19) to the value (14) we obtain upper limit, or limit allowable channel throughput for a given $p_{\min}$:

$$C = \lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n} C_i \leq C_{\text{гр.д}} = 1 + p_{\min}\log_2 p_{\min} + \\ +(1 - p_{\min})\log_2(1 - p_{\min}) \quad (24)$$

that had to prove.

Therefore, based on Shannon information theory provided considered theoretical security of discrete sources analysis throughput as an indicator of security from leaking by technical channels. The concept of limit allowable throughput leakage channel and suggested its to use as a security norms.

Conclusions

Obtained analytical ratios, establishing communication of norms given index with the necessary of errors probability in the channel. In establishing consistency between the set of security risks and necessary limit allowable throughput of the technical leakage channel, using of these ratios allows determining the desired probability of error in the channel and in the next -desired signal/noise ratio in the point of possible information interception.

Obtained results in the article is the development of the theory of information security from leaking by technical channels, and also could form the basis for the implementation in standards of information security series ISO/IEC 27000.

References

1. Information technology. Security techniques. Information security management systems. Requirements [ISO/IEC 27001:2013].
2. The Law of Ukraine "About protection of information in telecommunication systems". http://www.zakon.rada.gov.ua/go
3. Buzov G.A., Kalinin S.V., Kondratev A.V. Protection of information from leaks through technical channels, Goryachaya liniya: Moskva, Telecom (2005)
4. 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, vol 3 (58), pp. 160-181. (2018) doi: 10.15622/sp.58.7
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 (2002) http://www.cl.cam.ac.uk/techreports
6. Kuhn, M.G.: Electromagnetic eavesdropping risks of flat-panel displays. Lecture Notes in Computer Science, 3424, pp. 88-107 (2005)
7. 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
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. Lenkov, S.V., Peregudov, D.A., Horoshko, V.A.: Methods and means of information protection. Tom I. Unauthorized receipt of information, Ariy: Kyiv (2008)
10. 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
11. 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)
12. 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
13. 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", Kiev, NTUU "KPI" SRC "Tezis", vol 1 (31), pp. 9 – 13 (2016)
14. 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
15. Fink L. M.: The theory of transfer of discrete messages [2-d edition], Sov. Radio: Moskva, (1970)
16. Kulkarni, A.N., Bukate, R.R., Nanaware, S.D.: Study of Various Attacks and Routing Protocols in MANETS. 2018 International Conference on Information, Communication, En-

gineering and Technology, ICICET 2018, art. no. 8533696 (2018) doi: 10.1109/ICICET.2018.8533696
17. Burachenko, D.L., Zavarin, G.D., Klyuyev, N.I. et. al.: General theory of communication, VAS: Leningrad (1970)
18. 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
19. Ivanovsky, R.I.: Theory of probability and mathematical statistics, BHV: Petersburg (2008)
20. 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
21. Gallagher R. G.: Information theory and reliable communication, Sovetskoe radio: Moskva (1974)
22. Qian, Y., Zhou, X., Li, J., Shu, F., Jayakody, D.N.K.: A Novel Precoding and Impulsive Noise Mitigation Scheme for MIMO Power Line Communication Systems. IEEE Systems Journal (2018) doi: 10.1109/JSYST.2018.2880962