EasyChair Preprint

№ 13078

# Risk-Oriented Indicators of Security for Parallel Data from Leakage Through Technical Channels

Serhii Ivanchenko, Vasyl Nekoz, Anatolii Holishevskyi, Oleksandr Dranovych and Vasyl Bondarenko



April 24, 2024

# Risk-oriented Indicators of Security for Parallel Data from Leakage Through Technical Channels

Serhii Ivanchenko[a], Vasyl Nekoz[a], Anatolii Holishevskyi[b], Oleksandr Dranovych[b], Vasyl Bondarenko[c]

[a] *Institute for Special Communications and Information Protection KPI them Igor Sikorsky, Kyiv, 03056, Ukraine*
[b] *State Scientific and Research Institute of Cybersecurity Technologies and Information Protection, Kyiv, 03142, Ukraine*
[c] *State Service of Special Communication and Information Protection of Ukraine, Kyiv, 03110, Ukraine*

**Abstract**

The justification of a set of risk-oriented indicators of data security against leakage through technical channels with their parallel presentation is carried out. This makes it possible to calculate the required values of the margin of error in the TLC based on the given safety probability, and vice versa.

**Keywords** [1]

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

## 1. Introduction

The operation of technical means of information processing and transmission, including information and communication systems (ICS), as electronic means, is constantly accompanied by a number of undesirable effects. These effects can lead to the formation of technical leakage channels (TLC) of information. As a rule, such effects are side electromagnetic radiation of information-carrying signals, their guidance on external conductors and technical means, leakage of signals into the power supply network and grounding system, etc. The formation of these channels at the objects of information activity (OIA) is a threat regarding the leakage of information during its processing and transmission by technical means and the corresponding violation of confidentiality.

The presence of a threat requires taking the necessary measures to secure information. As is obvious, these measures should be aimed at eliminating (localizing, minimizing) the factors that form TLC, and achieving certain regulatory conditions regarding information security [1-3, 7, 9].

An important feature of this threat is that it cannot be eliminated completely. The formation of TLC on OIA is involuntary. TLC are not provided in technical means constructively, and therefore exist outside the will of the owners of the information. The information-carrying signals in TLC are generally low-level and, due to the nature of their attenuation, propagate over relatively short distances, from units to hundreds of meters. The specified distances, regardless of their size, may exceed the controllability limits of OIA and lead to the danger of information leakage.

The impossibility of ensuring absoluteness requires substantiation of sufficiency and its management in such a way that the overall security indicator, which is the risk, does not exceed a given value. These are world experience in information security management, these are international standards for information security management series ISO/IEC 2700x, and other standards. According

*Information Systems and Technology (IST-2022), November 22-25, 2022, Kharkiv, Ukraine*
EMAIL: soivanch@ukr.net (A. 1); nvs20141987@gmail.com (A. 2); 380937029549@ukr.net (A. 3); o.dranovych@gmail.com (A. 4); bbazil@ukr.net (A. 5)
ORCID: 0000-0003-1850-9596 (A. 1); 0000-0001-5091-0529 (A. 2); 0000-0001-9981-7771 (A. 3); 0000-0002-3120-217X (A. 4); 0000-0002-7578-3236 (A. 5)

to them, the owner of the information determines the permissible limit of risk, which in case of attacks or incidents will ensure his maximum losses.

It is obvious that the risk depends on the indicators that characterize the possibility of passing information on the TLC. They are also indicators of information security against leakage. The specified indicators must provide proof of fulfillment of the specified security risk, allow its analysis and adjustment using automation tools. In order to guarantee the reliability of information protection, security indicators require periodic review, which must be carried out with the development of science and technology.

Thus, in work [4] a set of risk-oriented indicators of information security against leakage through technical channels for consistent data presentation has already been proposed. They are the permissible bandwidth of the TLC, which corresponds to the maximum permissible risk of information security, the probability of error in the channel, which provides the bandwidth, and the signal/noise ratio, which causes the desired probability of error. The signal/noise ratio is obtained using the optimal receiver, which determines the maximum potential capabilities of the world's existing means of reception, including interception.

Having set the permissible risk probability, the ratios obtained in [4] for the sequential presentation of data make it possible to calculate the required bandwidth, error probability, and signal/noise ratio, the implementation of which will reliably ensure the given risk. And the opposite. Based on the actually existing signal/noise ratio, the obtained ratios in [4] allow for the analysis of error probability, throughput and, ultimately, risk probability. In essence, this is a complete Deming-Shewhart cycle, which allows information security management in relation to information leakage through technical channels.

However, the ratios obtained in works [4, 6] make sense only for a serial code, when each cycle of the device corresponds to one bit of the data sequence. Modern ICS use not only serial, but also parallel representation, that is, in each cycle there is not one, but the sum of a certain number of bits that circulate through parallel buses.

It is obvious that the sum of parallel bits in the channel will form an additional uncertainty, which, in relation to the sequential code, can lead to self-masking and saving of protection means.

Therefore, there is an urgent task of substantiating the risk-oriented indicators of data protection against leakage through technical channels with their parallel presentation, which will allow to guarantee the reliability of the protection, provide and carry out an analysis of the risk of information security.

## 2. Main part

Let the information security risk be given. This is a general indicator that quantifies the potential hazard that leads to loss. It can be represented as a product of the probability of threat realization - $p_r$ and the prices - *Price* of its consequences [5, 12]:

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

If you set the maximum permissible risk value *R*max.allow, which will essentially express the level of protection, then knowing the price of one bit of the data sequence, you can express the maximum allowable risk probability for ensuring information protection against leakage, including through technical channels. The value of the price of one digit of the sequence can also be found by the maximum losses, for example, obtained as a result of the alleged leakage of all information.

Using the probability of risk as a general indicator of security allows the introduction of a risk-oriented approach to protecting information from leakage through technical channels. At the same time, for the technical channel, its private informational, probabilistic, and energy indicators must be found, which in aggregate will provide the required security risk. The convenience of implementing this approach lies in the fact that, on its basis, with the use of electronic computing equipment, it allows the automation of information security management and the improvement of the effectiveness of analysis, adjustment and risk management.

Yes, or otherwise, the price of possible damages *Price* and the limits of risks $R_{\text{max.allow}}$, must be set by the owner of information resources. This is the entity that is interested in the required level of

protection [5, 11, 12]. The maximum permissible risk probability $p_{r\ \text{max.allow.}}$ is a technological indicator that must be provided by the protection system and can be found from the formula (1):

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

The protection system will be effective if its indicators are reliably provided pr max.allow and thereby the specified system will prove to guarantee information security with a given risk.

Let the risk probability limit be given $p_{r\ \text{max.allow}}$ – quantitative condition of information security. It should be ensured in TLC through private technological indicators. These indicators, in their structured combination, represent a system of risk-oriented indicators characterizing the security of ICS against information leakage through technical channels.

A security risk is a risk of non-fulfillment of a qualitative security requirement. Therefore, for the threat of information leakage through technical channels, its admissible value can be considered as an admissible risk of leakage, i.e., admissible bandwidth of TLC. This is the maximum amount of information that can admissibly flow through TLC and will not lead to a violation of information security [8, 9-11].

Let's estimate the bandwidth of the specified channel for parallel data presentation $C_{\text{paral}}$. and let's express it in terms of the probability of an error in the channel, based on the fact that the inequality must be satisfied for TLC:

$$C_{\text{paral}} \le C_{\text{paral.max.allow}}, \quad (3)$$

where $C_{\text{paral. max. allow}}$ – the maximum allowable bandwidth of TLC for parallel presentation of data, which should correspond to the maximum allowable probability of information security risk. It can be found by the formula:

$$C_{\text{paral.max.allow}} = p_{r.\text{max.allow}} \times C_{\text{paral.max}}, \quad (4)$$

where $C_{\text{paral. max}}$ – the maximum bandwidth of TLC for parallel presentation of data.

It should be noted that when using parallel data representation in technical means of information processing and transmission, it is not a combination of data, but their sum that enters the TKB. It is thanks to this that additional uncertainty appears in the channel, which, even in the absence of noise distortions, will reduce throughput.

To find the throughput and other private security indicators in TLC when presenting data in the form of a parallel code, consider the technical channel of information leakage as a discrete-continuous channel with n parallel sources of information leakage (Figure 1).

The source produces a sequence of data - signs, to which the modulator matches certain continuous realizations and sums them in portions relative to the number of parallel tracks in the ICS. Total realizations are propagated through a continuous channel, in which the data realizations are affected by additive Gaussian noise, and are received by means of interception [1, 4-6, 13]. At the reception, based on the total realization distorted in the channel, a decision is made by means of the decision scheme about which combination of signs was produced by the source.

Let a discrete source of information produce some message - for simplicity, a sequence of binary characters $X = (x_1, x_2, x_3, \ldots)$, where $x = \{0, 1\}$. The specified data circulates on parallel tracks in the form of continuous implementations of duration $T$, for example:

$$\begin{aligned} x = 1 &\leftrightarrow s_1(t); \\ x = 0 &\leftrightarrow s_2(t). \end{aligned} \quad (5)$$

Obviously, the uncertainty introduced by the above type of modulation will depend on the forms of implementations $s_1(t)$ та $s_2(t)$: unipolar, multipolar, orthogonal or other. Therefore, for the sake of simplicity, let these implementations have a unipolar representation, that is, the absence and presence of a certain signal correspond to "zeros" and "ones".

Let the information entering the TLC circulate simultaneously along n parallel tracks in the ICS. Then the sequence $X$ can be represented as a sequence of segments $X = (X^n_{k1}, X^n_{k2}, X^n_{k3}, \ldots, X^n_{kg}, \ldots)$ in length $n$, where $X^n_{kg} = (x_1, x_2, x_3, \ldots, x_i, \ldots, x_n)$ – the segment numbered g in the sequence $X$, $g = 1, 2, 3, \ldots$, and the number of the binary combination $k$, $k = 1, 2, 3, \ldots, 2^n$.

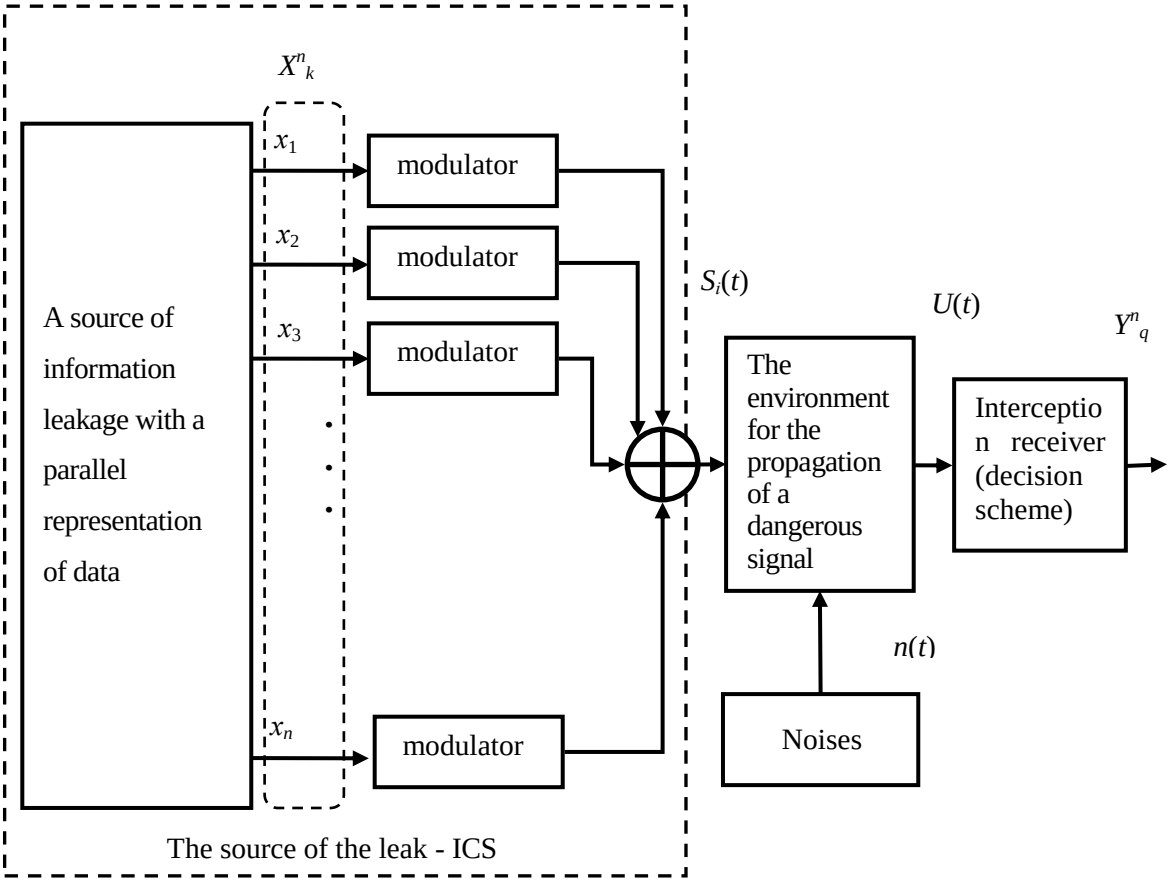


**Figure 1**: Discrete-continuous channel as a technical channel of information leakage from ICS when data is presented in the form of a parallel code

Since with the parallel circulation of information in the ICS for each cycle of segment formation $X^n_{kg}$ of data $g$, the energy of the signals will be added, then some total realization will spread into the continuous medium of TLC $S_i(t)$, i = 0, 1, 2, … $n$, which was formed from the combination $X^n_k$:

$$S_i(t) = \sum_{l=1}^{n} S_{1(2),l}(t). \quad (6)$$

It should be noted that for the selected type of modulation, the amplitude of the realizations of logical "zeros" and "ones" $s(t)$ directly proportional to their values. Therefore, the amplitude of the total realization $S_i(t)$ will be related to weight accordingly wtk of combinations $X^n_k$, which for each $k$ is equal to:

$$wt_k = \sum_{l=1}^{n} x_1, x \epsilon X_k^n. \quad (7)$$

Therefore, in a channel formed by a continuous medium, with a discrete representation, not binary signs, but weights as - $wt_k$, each of which will identify a certain set of combinations $X^n_k$ of the same weight. Such a set is defined by permutations and is equal to [14, 15]:

$$C_n^i = \frac{n!}{i!\,(n-i)!}. \quad (8)$$

Thus, the channel described above (Figure 1) can be represented as two serially connected components that introduce uncertainty into the channel and lead to information loss. This is the

transition of $X^n_k$ into the total realization of $S_i(t)$, which is carried out at the modulation stage and corresponds to the weight $wt_k$ (denote this weight by discrete variables at the channel input as – $S_i$ and at the output of the channel $U_j$, $j$ = 0, 1, 2, … $n$), and the passage of the implementation $S_i(t)$ through the continuous medium of TLC with noises to the receiver in the form of a distorted $U(t)$. Based on the analysis of $U(t)$ the receiver makes a decision in a certain (perhaps the best) way $Y^n_q$, $q$ = 1, 2, 3,…, $2^n$, as to what is the $X^n_k$, that was produced by the source.

The specified transitions of data combinations from the source to the receiver of interception are conveniently depicted using a diagram (Figure 2). Let us express the bandwidth of such a channel, understanding by it the maximum amount of information per one binary character of the sequence over all possible distributions of source probabilities. The specified throughput can be expressed as:

$$C = \sup_{p(x)} I\ (U; S; X), \tag{9}$$

where $I(U; S; X)$ – mutual three-dimensional information linking the outputs of the source of information, the modulator and the output of the medium of propagation of a dangerous signal, to which the alleged adversary has access and thanks to the analysis of which makes a decision about the information produced by the source.

Three-dimensional mutual information can be expressed by the ratio:

$$I\ (U; S; X) = \frac{1}{n}\sum_{j=0}^{n}\sum_{i=0}^{n}\sum_{k=1}^{2^n} p(U_j, S_i, X_k^n)\log_2 \frac{p(U_j, S_i, X_k^n)}{p(U_j)p(S_i)p(X_k^n)}, \tag{10}$$

where $p(U_j, S_i, X^n_k)$ – three-dimensional joint probability,

$p(U_j)$, $p(S_i)$, $p(X^n_k)$ – one-dimensional probabilities.

For find the bandwidth (9) of the channel, it is necessary to analyze the mutual information (10) under the condition of the maximum entropy of the information source $H(X)$, which is achieved by the equality of the signs of the sequence $X$ :

$$p(X_k^n) = \frac{1}{2^n}. \tag{11}$$

Transition probabilities $X^n_k$ в $S_i$ та $S_i(t)$ in $U_j$ in the Figure 3 can be expressed by conditional probabilities, which are respectively equal to [14, 15]:

$$p(S_i/X_k^n) = \frac{C_n^i}{2^n}, \tag{12}$$

$$p(U_j/S_i) = p_{ij}, \tag{13}$$

where $p_{ij}$ – transition probabilities $S_i \rightarrow U_j$ in the Figure 3, which are caused by noises in the environment of the propagation of dangerous signals (Figure 1).

If the leakage channel is symmetric without memory with transmission fidelity q, then the specified probabilities can be represented in the form of a matrix [14, 15]:

$$p_{ij} = \begin{bmatrix} q & p & p & \dots & p \\ p & q & p & \dots & p \\ p & p & q & \dots & p \\ \dots & \dots & \dots & \dots & p \\ p & p & p & p & q \end{bmatrix}^{n\times n}, \tag{14}$$

where $p$ – channel error probability:

$$p = \frac{1-q}{n}. \tag{15}$$

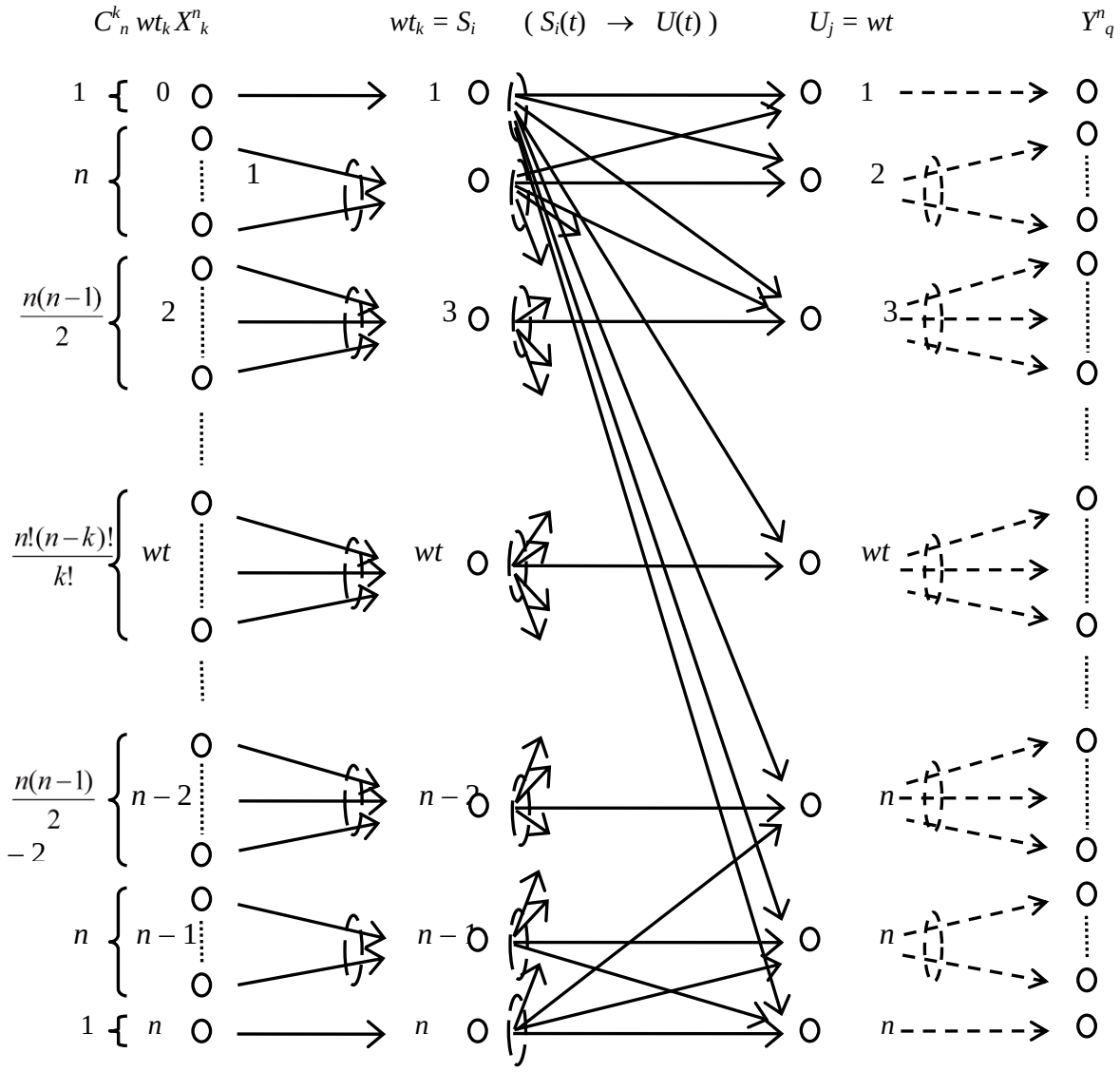


**Figure 2**: Transitions scheme of data combinations from the source to the receiver of interception through TLC during parallel presentation of data in ICS

Let's express the probabilities used in formula (10) for condition (11) and initial data (12) and (13).

1. A three-dimensional probability can be defined by a product:

$$p\left(U_j, S_i, X_k^n\right) = p\left(U_j/S_i, X_k^n\right)p(S_i/X_k^n)p(X_k^n). \quad (16)$$

It should be noted that the conditional probability $p(U_j\ /\ S_i,\ X^n{}_k)$ describes the transition $(S_i,\ X^n{}_k) \rightarrow U_j$, which is completely defined by transitions $S_i \rightarrow U_j$ (Figure 2). Direct transitions $X^n{}_k$ в $U_j$ does not exist, therefore equality will be fair:

$$p\left(U_j/S_i, X_k^n\right) = p\left(U_j/S_i\right). \quad (17)$$

Taking into account (11), (12), (13), and (17), the conditional probability (16) will take the form:

$$p\left(U_j, S_i, X_k^n\right) = \frac{1}{2^{2n}} p_{ij} C_n^i. \quad (18)$$

2. One-dimensional probabilities:

$$p(U_j) = \sum_{i=0}^{n} \sum_{k=1}^{2^n} p(U_j, S_i, X_k^n) = \frac{1}{2^n} \sum_{i=0}^{n} p_{ij} C_n^i, \tag{19}$$

$$p(S_i) = \sum_{k=1}^{2^n} p(S_i / X_k^n) p(X_k^n) = \frac{1}{2^n} C_n^i, \tag{20}$$

where $p(X^n_k)$ – given by the ratio (11).

By substituting (11), (18), (19) and (20) into ratio (10), we find the desired ratio regarding the bandwidth (9) of the technical channel of information leakage with parallel representation of the code using unipolar implementations:

$$C_{\text{ТКВ}} = \frac{1}{n} \sum_{j=0}^{n} \sum_{i=0}^{n} \sum_{k=1}^{2^n} \frac{1}{2^{2^n}} p_{ij} C_n^i log_2 \frac{\frac{1}{2^{2^n}} p_{ij} C_n^i}{\left[\frac{1}{2^n} \sum_{i=0}^{n} p_{ij} C_n^i\right] \times \left[\frac{1}{2^n} C_n^i\right] \times \left[\frac{1}{2^n}\right]}, \tag{21}$$

Ratio (21) can be simplified by shortening the common factors of the fraction and placing the coefficients in front of the sum signs:

$$C_{\text{ТКВ}} = \frac{1}{n} \frac{1}{2^n} \sum_{j=0}^{n} \sum_{i=0}^{n} p_{ij} C_n^i \log_2 \frac{2^n p_{ij}}{\sum_{i=0}^{n} p_{ij} C_n^i}, \tag{22}$$

or

$$C_{\text{ТКВ}} \underset{p(X_k^n)=\frac{1}{2^n}}{=} H_x(U) - H_x(U/S) \tag{23}$$

,

where $H_x(U)$ та $H_x(U/S)$ – The unconditional and conditional entropy of the output of the channel $U$, provided is the equivalence of the source $X$:

$$H_x(U) \underset{p(X_k^n)=\frac{1}{2^n}}{=} \frac{1}{n} \frac{1}{2^n} \sum_{j=0}^{n} \sum_{i=0}^{n} p_{ij} C_n^i \log_2 \frac{2^n}{\sum_{i=0}^{n} p_{ij} C_n^i}, \tag{24}$$

$$H_x(U/S) \underset{p(X_k^n)=\frac{1}{2^n}}{=} \frac{1}{n} \frac{1}{2^n} \sum_{j=0}^{n} \sum_{i=0}^{n} p_{ij} C_n^i \log_2 \frac{1}{p_{ij}}. \tag{25}$$

Thus, according to formula (23), it is not difficult to calculate the bandwidth of the technical channel of information leakage, taking into account the matrix (14) of the probabilities of true and false transmission.

It is also not difficult to check the truth of formulas (22), (23), (24) and (25) for the partial case under the condition $n = 1$, that is, when there is no parallel code, when one discharge flows on one track. Under this condition, the unconditional and conditional entropies defined above will be equal to:

$$H_x(U) \underset{p(X_k^n)=\frac{1}{2^n}}{=} 1 \text{ (bit)}. \tag{26}$$

$$H_x(U/S) = \sum_{j=0}^{n} \sum_{i=0}^{n} p_{ij} \log_2 \frac{1}{p_{ij}} = H_x(U - S) = H(E), \tag{27}$$

where $H(E)$ – entropy of the source of errors in a discrete channel ($S_i \rightarrow U_j$).

At the same time, the bandwidth of the TLC fully coincides with the bandwidth for the sequential data representation code [5]:

$$C_{\text{TLC}} = 1 - H(E). \tag{28}$$

It is not difficult to check that transition probabilities are equal $S_i \rightarrow U_j$, that is, under the condition $p_{ij} = 1/n$ to all $i$ and $j$ unconditional and conditional entropy $H(U)$ and $H(U/S)$ reach equality regardless of the value of $n$, and therefore under these conditions $C_{\text{TLC}} = 0$, that is, the condition of absence of TLC is reached.

According to the condition (5), which must be fulfilled in the technical leakage channel, the maximum permissible error probabilities of the TLC corrected for the parallelism of the code representation, which are equivalent to the maximum permissible probabilities without parallel representation, can be found by equating the bandwidth of the technical information leakage channel with parallel representation of the code (23) with the bandwidth of a discrete channel without memory in general form:

$$C_{\text{TLC}} = 1 - H(U/X). \tag{29}$$

Hence and taking into account (18), the equivalent uncertainty of the channel is expressed by the formula:

$$H(U/X) = \frac{1}{n}\frac{1}{2^n}\sum_{j=0}^{n}\sum_{i=0}^{n} p_{ij} C_n^i \log_2 \frac{\sum_{i=0}^{n} p_{ij} C_n^i}{p_{ij}}. \tag{30}$$

Equating $H(U/X)$ according to formula (30) to the entropy function, which determines the uncertainty of the source of errors for a discrete symmetric channel, with the help of reference data, it is possible to find the equivalent maximum permissible error probability of the TLC corrected for the parallelism of the code representation.

For simplicity, we will find the probability of error p, using the approach as for the worst case from the point of view of security. At the same time, finding this probability will be carried out with respect to the optimal receiver, as the best method of interception that can be used by the enemy.

As is known, the decision circuit of such a receiver is the circuit that most accurately decides what was at the channel input. Therefore, it is built according to the Kotelnikov criterion - the maximum of the posterior probability, which determines the best possibilities of the channel, that is, the possibilities of transmitting the maximum amount of information from the source.

According to the selected approach for evaluating transition probabilities, it is obvious that the worst case when passing through all possible realizations $S_i(t)$ for unipolar signals, there is the one that will be the most unmasking, that is, the most different from zero:

$$S_{\max}(t) = \max_i S_i(t). \tag{31}$$

For unipolar signals, if the logical unit is matched by the presence of a signal $s_{(1)}(t) \neq 0$, and its absence is zero $s_{(0)}(t) = 0$ the maximum and minimum of total realizations will be equal to:

$$\begin{cases} \mathrm{S}_{\max}(t) = ns_{(1)}(t) \\ \mathrm{S}_{\min}(t) = ns_{(0)}(t) = 0 \end{cases}. \tag{32}$$

The total realizations indicated by formula (32) are extremes with respect to their own unmasking features in TLC. All other total implementations, i.e. implementations for all other combinations of data will be within the limits specified by formula (32).

Since two states are taken into account during the passage of information through the technical channel at reception, the following decision scheme [1, 13] can be used to estimate the probability of an error p (Figure 3).

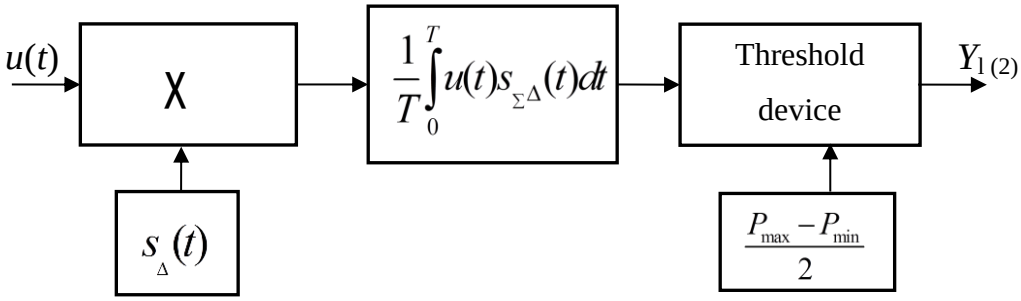


**Figure 3**: Decision scheme of the optimal receiver for determining the binary states of the source with known parameters

The symbols used in Figure 3 have the following meaning:
$S_\Delta(t)$ – difference signal determined by the formula:

$$S_\Delta(t) = S_{\max}(\mathrm{t}) - S_{\min}(\mathrm{t}), \tag{33}$$

$P_{\max}$, $P_{\min}$ – maximum and minimum capacities of total implementations $S_{\max}(t)$, $S_{\min}(t)$:

$$P_{\max} = \frac{1}{T}\int_0^T s_{\max}^2(t)dt, \tag{34}$$

$$P_{\min} = \frac{1}{T}\int_0^T s_{\min}^2(t)dt. \tag{35}$$

It is not difficult to find that:

$$P_{\max} = nP_1 \quad \text{and} \quad P_{\min} = nP_0, \tag{36}$$

where $P_1$, $P_0$ – powers of implementations of logical ones and zeros $s_1$(t) and $s_0$(t):

$$P_1 = \frac{1}{T}\int_0^T s_1^2(t)dt, \tag{37}$$

$$P_0 = \frac{1}{T}\int_0^T s_0^2(t)dt. \tag{38}$$

For the decision scheme in Figure 3, according to the approach as for the worst case, under the condition of equal probability of the source distribution $p(X_k^n) = \frac{1}{2^n}$, $k = 1, 2, 3, \ldots, 2^n$, estimating the probability of error p is reduced to estimating the probability of fulfillment of the inequality:

$$p = \underset{i\neq j}{p_{ij}} = \frac{1}{n}p\left\{\frac{1}{T}\int_0^T u(t)s_{\Sigma\Delta}(t)dt < \frac{1}{2}(P_{\max} - P_{\min})\right\}. \tag{39}$$

Taking into account (36), (37) and (38), the probability of false interception relative to the energy indicators of the technical leakage channel at the point of possible interception will be determined by the relations [4-6]:

$$p_{\text{p}} = F(-\frac{1}{2}\sqrt{\frac{P_{\sum\Delta}T}{N_0}}) \quad \text{or} \quad p_{\text{p}} = F(-\frac{1}{2}\sqrt{\frac{nP_{\Delta}T}{N_0}}), \tag{40}$$

where $F(x) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x} \exp\left\{-\frac{\eta^2}{2}\right\} dn$ – the Laplace integral is determined by the reference data.

$P_{\sum\Delta}, P_{\Delta}$ – powers of difference total realizations $s_{\sum\Delta}(t)$ and realizations $s_{\Delta}(t) = s_1(t) - s_2(t)$:

$$P_{\sum\Delta} = \frac{1}{T}\int_0^T s^2_{\sum\Delta}(t)dt, \tag{41}$$

$$P_{\Delta} = \frac{1}{T}\int_0^T s^2_{\Delta}(t)dt. \tag{42}$$

It is obvious that for unipolar signals, where $s_0(t) = 0$, $P_0 = 0$ and $P_1 = \frac{1}{T}\int_0^T s_1^2(t)dt$, where $s_1(t) \neq 0$, and therefore the relation (40) will turn into a simpler form:

$$p_p = F(-\delta_p), \tag{43}$$

where

$$\delta_p = \frac{1}{2}\sqrt{\frac{nP_1T}{N_0}}.$$

The probability of error *p* for matrix (14) can be found using formula (15), substituting (40) into it, or for unipolar signals (43).

Analytical relations (14), (15), (29) and (30) are obtained, which establish the relationship between bandwidth and the probability of an error in the technical leakage channel and the bit rate of parallel data. To ensure the specified error probability, the justification of its connection with the signal/noise ratio, which is expressed by relations (37) and (43), was carried out. The ratios establish the relationship between the security indicators and provide the possibility of calculating their maximum permissible values:

$$R_{\text{max.allow}} \rightarrow p_{r\,\text{max.allow}} \rightarrow \text{C}_{\text{max.allow}} \rightarrow p_{\text{max.allow.}} \rightarrow \delta_{\text{max.allow}}. \tag{44}$$

and the opposite

$$R_{\text{max.allow}} \leftarrow p_{r\,\text{max.allow}} \leftarrow \text{C}_{\text{max.allow}} \leftarrow p_{\text{max.allow}} \leftarrow \delta_{\text{max.allow}}. \tag{45}$$

## 3. Conclusions

The set of risk-oriented indicators of data security against leakage through technical channels with their parallel presentation, which are private for TLC and when performing their calculated values, provide the necessary risk as a general indicator of information security, is substantiated. The private security indicators that directly characterize information leakage in the TLC are the bandwidth of the TLC, the probability of an error in the channel, and the signal/noise ratio at the receiver input.

Analytical relations have been obtained that relate this bandwidth to the error probability in the channel and the bit rate of parallel data. They make it possible to calculate the required values of the maximum permissible error probabilities in the TLC based on the given probability of a security risk, and the opposite, to estimate the probability of a security risk based on the probability of an error in the channel. Analytical ratios were also obtained, establishing a connection between the signal/noise ratio and the above-mentioned TLC indicators for parallel data presentation. They make it possible to calculate the maximum permissible signal/noise ratios based on the given probabilities of security risk and errors in the technical leakage channel.

The signal-to-noise ratio is the final indicator of the security of information against leakage, which ensures this security in the physical environment of the channel, where data implementations are distributed and received for the purpose of interception of information.

## 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, Ukraine, pp. 179–183 (2019) ISBN 9786177468379.

[5] Ivanchenko S.,Gavrylenko O., Holishevskyi A., Bondarenko V., Rushchak O., Prokopenko Y. Leakage of information through technical channels and a set of risk-oriented indicators of its security for modern ITS. "2nd International Conference on Intellectual Systems and Information Technologies, ISIT 2021", Odesa, Ukraine, 13 September 2021 to 19 September 2021. CEUR Workshop Proceedings. Volume 3126, pp. 143-148 (2021) ISSN 16130073.

[6] Korobiichuk I., Ivanchenko S., Havrylenko O., Golishevsky A., Hnatiuk S., Hryshchuk R. Protection of information from leakage by technical channels for sources with non range distribution of probability (Conference Paper). "2nd International Workshop on Computer Modeling and Intelligent Systems, CMIS 2019", Zaporizhzhia, Ukraine, 15 April 2019 до 19 April 2019, 2019, pp. 992 – 1003. ISSN 16130073.

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

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

[9] Decree of the President of Ukraine № 685/2021 On the Decision of the National Security and Defense Council of Ukraine of October 15, 2021 "On the National Security Strategy of Ukraine".

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

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

[12] National standart of Ukraine. Information technology. Methods of protection. Information security risk management [ISO/IEC 27005:2015].

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

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

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