The object of the study is the process of ensuring security during data transmission through information channels. To ensure high-quality indicators of information transmission channels protection, it is necessary to periodically monitor and, when detected, close possible data leakage channels. The effectiveness of measures to protect transmission channels depends on the quality of checking the presence of possible, valid or hidden, data leakage channels. A significant number of signs of information leakage complicates the control process and leads to additional economic costs for the use of control equipment. Therefore, it is necessary to develop a method of synthesis of an information-analytical system for assessing the level of transmission channels protection. It is proposed to develop such a method on the basis of determining the dependence between control signs of the presence of information leakage channels. The proposed method allows to ensure the necessary level of security. The basis of the method for synthesis of the information-analytical system for assessing the level of information transmission channels protection is the equation of the associative connection between the control features. The presence of a connection between control signs indicates the presence of information leakage channels. This is due to the loss of characteristics (for example, voltage or signal strength) of the useful information flow due to the redistribution of data during transmission. The benefit from the application of the obtained results depends on the number of discovered and, accordingly, closed channels of information leakage. Implementation of the proposed method allows to automate the process of finding a data leak in transmission channels. The given research results can be useful in the development of software for expert decision-making systems based on the formation of knowledge bases about the relationship between control features. Implementation of the obtained results will increase the reliability and security of information transmission channels

Keywords: leakage of information, information channel, information and measurement system, information protection, threat model

UDC 623.618.51
DOI: 10.15587/1729-4061.2024.302495

DEVELOPMENT OF A METHOD FOR SYNTHESIZING AN INFORMATION-ANALYTICAL SYSTEM FOR ASSESSING THE LEVEL OF INFORMATION TRANSMISSION CHANNELS PROTECTION

Olexander Shmatko
PhD, Associate Professor
Department of Software Engineering and Management Intelligent Technologies**
Serhii Yevseiev
Corresponding author
Doctor of Technical Science, Professor*
E-mail: Serhii.Yevseiev@gmail.com
Valerii Dudykevych
Doctor of Technical Sciences, Professor
Department of Information Security
Lviv Polytechnic National University
S. Bandery str., 12, Lviv, Ukraine, 79013
Stanislav Milevskyi
PhD, Associate Professor*
Svetlana Solnyshkova
PhD, Associate Professor
Department of Physics and Electronics***
Alla Havrylova
Associate Professor*
Yanina Shestak
PhD
Department of Cyber Security and Information Protection
Taras Shevchenko National University of Kyiv
Volodymyrska str., 64/13, Kyiv, Ukraine, 01601
Serhii Oriekhov
PhD, Associate Professor
Department of Air Defense Forces tactics of the Land Forces
Ivan Kozhedub Kharkiv National Air Force University
Sumska str., 77/79, Kharkiv, Ukraine, 61023
Serhii Korsunov
Associate Professor
Department of Air Defense Forces tactics of the Land Forces***
Serhii Kravchenko
PhD, Associate Professor
Department of Land Forces
The National Defence University of Ukraine
Povitroflotskyi ave., 28, Kyiv, Ukraine, 03049
*Department of Cybersecurity**
**National Technical University "Kharkiv Polytechnic Institute"
Kyrpychova str., 2, Kharkiv, Ukraine, 61002
***Ivan Kozhedub Kharkiv National Air Force University
Sumska str., 77/79, Kharkiv, Ukraine, 61023

Received date 09.02.2024
Accepted date 19.04.2024
Published date 30.04.2024

How to Cite: *Shmatko, O., Yevseiev, S., Dudykevych, V., Milevskyi, S., Solnyshkova, S., Havrylova, A., Shestak, Y., Oriekhov, S., Korsunov, S., Kravchenko, S. (2024). Development of a method for synthesizing an information-analytical system for assessing the level of information transmission channels protection. Eastern-European Journal of Enterprise Technologies, 2 (9 (128)), 36–43. https://doi.org/10.15587/1729-4061.2024.302495*

1. Introduction

To ensure high-quality indicators of information transmission channels protection, it is necessary to periodically monitor and, if available, close channels of possible data leakage [1]. The effectiveness of measures to protect information transmission channels depends on the quality of checking the presence of possible, existing or hidden data leakage

Copyright © 2024, Authors. This is an open access article under the Creative Commons CC BY license

channels. When checking the presence of information leakage channels, special technical means are used, aimed at checking certain signs of the data leakage presence [2]. At the same time, a significant set of signs characteristic of each technical means (check method) is used. A significant number of information leakage signs complicates the control process and leads to additional economic costs for the use of control equipment. At the same time, the effectiveness of identifying data leakage channels largely depends on the experience of the technical means` operator [3]. Thus, ensuring the efficiency of control of information leakage channels requires minimization of control signs and automation of the control process. At the same time, it is necessary to ensure the required reliability of identifying possible channels of data leakage.

For the selection of control signs, it is suggested to use only independent ones from the general nomenclature of signs [4]. At the same time, it should be noted that in the work it is possible to consider independent signs that are not related to each other. The presence of a degree of dependence of control signs will testify to the existence of a channel of information leakage. Dependence of control signs is associated with the separation of data in the information transmission channel, that is, data leakage. Independent signs allow to detect data leakage in the information transmission channel without taking into account the influence of other signs. Therefore, when choosing the optimal composition of control signs, the task of determining dependent signs is relevant, the solution of which allows to identify and eliminate channels of data leakage. Control of data leakage signs must be carried out systematically during the functioning of information transmission channels. The appearance of dependence between the control signs during the transmission of information will signal the presence of data leakage. Therefore, it is proposed to develop an information-analytical system for estimating the level of information transmission channels protection based on the identification of the control signs dependence.

Thus, the development of a method of synthesizing an information-analytical system for estimating the level of information transmission channels protection is an urgent scientific task.

2. Literature and problem statement

The conducted analysis [2, 3, 5] shows that expert methods and the method based on the calculation of the correlation between the characteristics are most often used to determine the dependence between the characteristics [5–18].

In work [5], the problems of information loss during transmission through an optical communication channel are considered. A method of binarization of optical information for suppressing possible interference is proposed. The proposed method makes it possible to increase the reliability of data transmission. However, this method does not allow detecting a possible leakage of information during data transmission.

The work [6] proposes the use of hybrid cryptography to ensure the required level of data transmission reliability. This method allows to hide information in the event of its possible leakage. However, this method not only prevents data leakage during information transfer, but also reveals the fact of the leakage itself.

In work [7], the use of artificial intelligence is proposed to increase the reliability of information transfer. The developed method for assessing the level of intelligence of an information system is characterized by indicators of the share of hardware and software. But the study did not take into account methods for determining data leakage channels during information transfer.

Paper [8] explores the fundamentals of information transmission, which include some or all of the following elements: source of information, encoding of information, transmission of information through a channel, addition of noise, and finally reception and decoding of information. The study examines issues of biological coding and presents examples of coding using nucleic acids and proteins. However, the work does not address the issue of identifying data leakage channels, which would greatly improve the reliability of information transfer.

Paper [9] studies activity detection of reconfigurable smart ground devices for free uplink data transmission in wireless communication networks. In particular, mobile devices located in an area where direct connection to the access point is blocked are considered. A drawback of the research results is the study of a phase shift antenna design that covers the entire blocked area with a wide reflective beam. The proposed method allows to hide the exact location and time of activity of devices when transmitting data. However, the developed method does not allow identifying information leakage channels.

Work [10] presents an analytical model of a wall with a built-in antenna, also called a signal transmitting wall. The analytical model is an attractive alternative to wall modeling that combines individual data transfer characteristics. The model takes into account the proposed antenna element gains and cable losses. However, the proposed analytical model does not allow blocking data leakage channels during information transfer.

Work [11] evaluates the effectiveness of innovative systems for specific information security tasks. At the same time, the issues of identifying channels of possible data leakage have not been given due attention.

The work [12] proposes models for assessing information about the state of the channel in the transmitter and receiver. Identification of data leakage channels is proposed based on an assessment of the capacity value. Channels are blocked when there is attenuation, which is determined by a change in capacitance. However, the proposed method does not work if there is no physical penetration into the information transmission channel in order to obtain data.

Paper [13] presents a methodology for analyzing the effectiveness of primary protection systems for power lines, based on a probabilistic approach to the successful operation of protection systems. The operation of the protection system is represented by reliability graphs and a probabilistic model of distance protection is considered. The successful operation of a system is described by sets of connections, and solutions are obtained through Monte Carlo simulations. System elements are characterized by reliability factors: equipment failure rate and repair time. At the same time, data protection from unauthorized access to information is not considered.

Paper [14] discusses in some detail the costs and benefits of various methods for transmitting serial information. But no attention has been paid to the issues of protecting information from unauthorized access.

The work [15] presents important research carried out in the field of using energy systems for data transmission. The work presents important recommendations that may be useful for transmitting data in information channels. However, the issues of identifying data leakage channels have not been addressed.

In [16], the influence of communication channel delay on line protection functions in the time domain is studied. However, the proposed program of alternative transient processes does not allow identifying channels of possible data leakage.

The work [17] proposes a structural diagram of information exchange based on a description of a weakly formalized process under conditions of non-stochastic uncertainty. The generated production rules for determining appropriate strategies for the planned identification of information leakage channels based on predicted values allow to move on to knowledge processing for the synthesis of an automated decision-making system when managing protection channels. The disadvantage of this work is the inability to assess the level of protection of information data transmission channels.

In [18], a comprehensive method for determining the location of social network agents is developed to ensure the ability to influence information channels. A direction for improving the proposed method could be its integration with complex systems of protection (counteraction) from information influence.

Therefore, it is justified to conduct research to develop a method for synthesizing an information-analytical system for assessing the level of information transmission channels protection.

3. The aim and objectives of the study

The aim of this research is to develop a method for synthesizing an information-analytical system for assessing the level of information transmission channels protection. This method is based on determining the relationship between the control signs of the presence of information leakage channels. The developed method allows to ensure the required level of security.

To achieve the aim of the study, it is necessary to solve the following objectives:

– to develop a procedure for generating multiple control signs of the information leakage channel presence;

– to develop an algorithm for constructing an attributed binary tree to determine the presence of associative similarity of control characteristics;

– to develop a procedure for calculating the value of the dependence coefficients of control characteristics;

– to check the functionality of the developed method.

4. Research materials and methods

The object of the study is the process of ensuring security when transmitting data through information channels.

The research hypothesis was as follows. The presence of a dependency between controlled features, taking into account automated analytical information about the data transmission channel, is proposed to be determined on the basis of generated hypotheses about the presence of dependencies between features with an association quantifier [6]. In this study, by binary association let's understand the relationship between two characteristics A_i and A_j ($i \neq j$) of a data leakage channel presence. The ratio of two signs shows "the coincidence is stronger than the difference," that is, the number of cases in which the signs A_i and A_j simultaneously have or at the same time do not have the required values for the presence of information leakage channels. Moreover, the required values are greater than the number of other cases in which one of them does not have this value [19].

The method for synthesizing an information-analytical system for assessing the level of information transmission channels protection is a consistent solution to research problems. In general, the stages of the proposed method consist of:

– formation of control signs set of the presence of an information leakage channel;

– constructing an attributed binary tree that characterizes the presence of associative similarity of control features;

– developing a procedure for calculating the value of the dependence coefficients of control characteristics.

When developing the procedure for forming a set of control signs of the information leakage channel presence, the theory of research of set-theoretic models was used. When developing an algorithm for constructing an attributed binary tree, graph theory (the study of models in the form of graphs) is used to determine the presence of associative similarity of control features. When developing a procedure for calculating the value of the dependence coefficients of control characteristics and testing the performance of the developed method, a machine learning method based on detection rules is used.

This study introduced a restriction about the accepted condition of technical serviceability of the information transmission channel. When conducting this study, an assumption was introduced about the absence of interference during data transmission by an information channel.

5. Results of developing a method for synthesizing an information-analytical system

5. 1. Formation of the control signs set for the presence of an information leakage channel

Signs of an information leakage channel by set $A_i=\{A_1, ..., A_n\}$, to which unary predicates are assigned based on correspondence functions $\varphi(\tau)=\{\varphi_1(\tau), ..., \varphi_n(\tau)\}$.

Elements of the set of attributes and the set of predicates take three logical values: 1 – "true", 0 – "false" and x – "undefined" [20, 21]. In order to isolate and separate predicates and logical values of control features, the study proposes the following. Let's present the logical value of the control characteristics in parentheses before the predicate. Then the resulting entry (1) $\varphi_i(\tau)$ means that the unary predicate $\varphi(\tau)$ has the value "true". In this case, the presented variable «τ» shows the number of the control sign of the information leakage channels presence.

The function $|\{M\}|$ is formed. This function will determine the intensity (power) of data leakage from multiple information transmission channels $\{M\}$. It is proposed to calculate the coefficients of the number of episodes in which predicates have given values as follows:

$$a_{11}=|\{\tau|(1)\varphi_i(\tau)\wedge(1)\varphi_j(\tau)\}|;$$

$$a_{10}=|\{\tau|(1)\varphi_i(\tau)\wedge(0)\varphi_j(\tau)\}|;$$

$$a_{01}=|\{\tau|(0)\varphi_i(\tau)\wedge(1)\varphi_j(\tau)\}|; \quad (1)$$

$$a_{00}=|\{\tau|(0)\varphi_i(\tau)\wedge(0)\varphi_j(\tau)\}|.$$

The "inverse conjugacy" value r is introduced, which characterizes the numerical value of the association. This value r is calculated as follows:

$$r=(g_{11}\cdot g_{00})/(g_{10}\cdot g_{01}), \quad (2)$$

where $g_{ij} = a_{ij} / m$ – probability of fulfilling the formula (c) $\varphi_i(\tau)\wedge(d)$ $\varphi_j(\tau)$; $c, d\in\{0, 1\}$; $i\neq j$; m – number of features.

The assumption is introduced that any reasonable measure of the dependence of features corresponds to a strictly monotonic function r [22]. Then the calculation of logarithmic conjugacy of the form $\delta=\log(\Delta)$ shows that when $\delta>0$ the dependence is considered positive. Otherwise, when $\delta<0$, the dependence is considered negative. When $\delta=0$ there is no dependence.

Numerical value of the measure of the binary association quantifier $\gamma_{\approx 2}$ represented as a value that is the inverse of Edwards' "inverse conjugate" [20]:

$$\gamma_{\approx 2}=1/r=(g_{10}\cdot g_{01})/ (g_{11}\cdot g_{00})= (a_{10}\cdot a_{01})/ (a_{11}\cdot a_{00}). \quad (3)$$

The value $\gamma_{\approx 2}\in[0...+\infty]$. This value is not defined in two cases:

– when the numerator and denominator are equal ($\gamma_{\approx 2}=1$);

– calculation of the numerator or denominator is impossible, since one of the coefficients is equal to 0.

Then for the hypothesis with a binary association quantifier let's write the relation:

$$\approx_{\gamma\approx 2}[\varphi_i(\tau), \varphi_j(\tau)]. \quad (4)$$

A hypothesis of the form $a\approx_{\gamma\approx 2}[\varphi_1(\tau), \varphi_2(\tau), ..., \varphi_n(\tau)]$ is used. This hypothesis characterizes a multidimensional association that describes the presence of an associative connection between n characteristics $A_1, A_2, ..., A_n$. In this case, it is considered that the number of cases when such characteristics simultaneously correspond or do not correspond to the required values exceeds the number of cases when such characteristics (one or some of them) do not correspond to these values.

5. 2. Construction of an attributed binary tree that characterizes the presence of associative similarity of control features

It is necessary to calculate a numerical measure of the associative dependence of control characteristics. For this purpose, an algorithm has been developed for generating hypotheses with a multidimensional association quantifier of the form $\gamma_{\approx n}$. This algorithm is based on the use of an attributed binary tree, the nodes of which correspond to the coefficients a (Fig. 1).

The resulting tree node is assigned an attribute in the form of a "code". This "code" is represented as a sequence of zeros and ones. The values 0 or 1 correspond to the resulting Boolean values of the unary predicates. For node a_{1101} the resulting code looks like "1101".

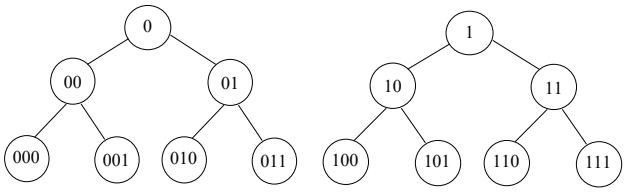

Fig. 1. Representation of nodes of an attributed binary tree

Coding the nodes of a binary tree is necessary to divide the nodes into two equal sets:

– set $\{+a\}$, which corresponds to the presence of associative similarity of parameters;

– set $\{-a\}$, which corresponds to the presence of associative difference.

To determine the numerical measure of a quantifier $\gamma_{\approx n}$ multidimensional association of control signs of the presence of information leakage channels, it is proposed to use this relation:

$$\gamma_{\approx n}=\left(\prod_{i=1}^{n^-} a_i^-\right)/\left(\prod_{i=1}^{n^+} a_i^+\right), \quad (5)$$

where $n=|\{a\}|$ – total number of tree nodes; $n^-=|\{a^-\}|$ – number of associative difference nodes; $n^+=|\{a^+\}$ – number of associative similarity nodes; Π – production operation.

It should be taken into account that $\{a\}=\{a^+\}\cup\{a^-\}$; $n=n^++n^-$; $n^+=n^-=1/2\times n$.

The proposed formula (5) calculates the presence (absence) of a relationship between control characteristics A_{ij}, i. e. determines the coefficient of dependence between characteristics.

Determining the value of set {a} coefficients is produced using formula (5). The results of the analysis of the obtained relations (1)–(5) allow to conclude: the classification of tree nodes depends on the resulting set $\{a^+\}$ or set $\{a^-\}$.

5. 3. Development of a procedure for calculating the value of the dependence coefficients of control characteristics

First it is necessary to calculate the coefficients of the set $\{a^+\}$. Wherein $\{a^-\}=\{a\}\setminus\{a^+\}$. To calculate set $\{a^+\}$ coefficients a set of attributes is used for the nodes of the constructed tree.

When combining all nodes let's get the following relation:

$$\{a\}=\{a_{=1}\}\cup\{a_{=0}\}\cup\{a_{>1}\}\cup\{a_{>0}\}\cup\{a_{0=1}\}.$$

Coefficient n is determined by the formula:

$$n=n_{=1}+n_{=0}+n_{>1}+n_{>0}+n_{0=1}.$$

The set of nodes is be defined $\{a_{=1}\}$, $\{a_{=0}\}$, $\{a_{>1}\}$ and $\{a_{>0}\}$ constructed binary tree as $\{a_\Sigma\}$:

$$\{a_\Sigma\}=\{a_{=1}\}\cup\{a_{=0}\}\cup\{a_{>1}\}\cup\{a_{>0}\}.$$

The intensity of data leakage from the set $\{a_\Sigma\}$ calculated as:

$$n_\Sigma=n_{=1}+n_{=0}+n_{>1}+n_{>0}.$$

The classification of tree nodes is based on the analysis of two conditions:

– coefficient $n_\Sigma=1/2n$;

– coefficient $n_\Sigma>1/2n$.

For the condition when the coefficient $n_\Sigma=1/2n$, then the nodes of the sets $\{a_{=1}\}$, $\{a_{=0}\}$, $\{a_{>1}\}$, $\{a_{>0}\}$ characterize associative similarity, and nodes $\{a_{0=1}\}$ – associative difference:

$$\{a^+\}=\{a_{=1}, a_{=0}, a_{>1}, a_{>0}\}; \{a^-\}=\{a_{0=1}\}.$$

For the condition when the coefficient $n_\Sigma>1/2n$, then to determine associative similarity or difference, the following operations are required.

Union of sets $\{a_{>1}\}$ and $\{a_{>0}\}$ in to set $\{a_?\}$:

$$\{a_?\}=\{a_{>1}\}\cup\{a_{>0}\}.$$

For the set $\{a_?\}$ the nodes that characterize associative similarity are selected. The remaining nodes correspond to nodes of associative difference.

The definitions of nodes that characterize associative similarity are based on the assumption about the frequency of occurrence of features: the more closely the features occur, the greater the associative similarity between them. Then for a^+ nodes with maximum coefficient values are selected. Such nodes correspond to nodes of "possible associative similarity" $\left(a_?^+\right)$. In this case, the number of such nodes is calculated by the formula:

$$n_?^+=\left|\left\{a_?^+\right\}\right|=1/2\ a-n_{=1}-n_{=0}.$$

The remaining nodes correspond to the nodes of "possible associative difference" $\left(a_?^-\right)$. The number of such nodes is calculated as follows:

$$n=\left|\left\{a_?^-\right\}\right|=1/2a.$$

Nodes of type $\{a_{0=1}\}$ proposed to be included in the set $\{a^-\}$:

$$\left\{a^+\right\}=\left\{a_{=1}^+, a_{=0}^+, a_?^+\right\};\ \left\{a^-\right\}=\left\{a_{0=1}, a_?^-\right\}.$$

Analysis of binary trees with nodes of arity 5 or more shows that among the nodes $a_{>1}$ and $a_{>0}$ there are always those that, by the number of ones (zeros), belong to the set $\{a^+\}$. For example, a node a_{11101} has more 1 than a node of the form a_{11100}. Then a node of the form a_{11101} characterizes "associative similarity".

It is proposed to adopt an additional restriction for calculating the numerical measure of associative similarity or difference for nodes with arity greater than or equal to 5 when selecting coefficients in the set $a_?^+$. For this purpose, coefficients Δ_1 and Δ_0 are introduced. Coefficient Δ_1 characterizes the difference between the number of units and the average number of characters (1 and 0) in the node code:

$$\Delta_1=\text{abs}[(0.5c(a)-c_1(a)],$$

where abs(x) – function for determining the absolute value of a number x;

$c(a)$ – number of characters in the node code;

$c_1(a)$ – number of ones in the node code.

Coefficient Δ_0 characterizes the difference between the number of zeros and the average number of characters in the node code:

$$\Delta_0=\text{abs}\ [(0.5c(a)-c_0(a)\ 0],$$

where $c(a)$ 0 – number of zeros in the node code.

If $\Delta_1=\Delta_0$, then for such a case it is proposed to use the general designation Δ.

Next, the coefficient a_{11101} is analyzed. Coefficient values Δ for such a coefficient is calculated using the formula:

$$c(a)=c(a_{11101})=5;\ c_1(a)=4;\ c_0(a)=1;\ \Delta_1=\text{abs}(5/2-4)=1.5;$$

$$\Delta_0=\text{abs}(5/2-1)=1.5.$$

After introducing the coefficient Δ for ease of understanding, node designation $a_{>1}$ and $a_{>0}$ is written in the form:

$$a_{>1}^\Delta \text{ and } a_{>0}^\Delta.$$

The axiom is introduced that the larger the value Δ, the higher the associative similarity between features. Then, the difference between the number of ones and zeros in the node code of the constructed attributed binary tree characterizes the associative similarity between the features.

A rule is formulated for determining the dependence of the telltale signs of the presence of data leakage channels. To form a set $a_?^+$ it is necessary to select nodes with large values Δ.

Minimum value Δ is presented as $\Delta_{\min}$. For an association quantifier of dimension 4, the coefficient Δ is represented it in the form $\Delta=\{0, 1\}$. For an association quantifier of dimension 5, the coefficient Δ is represented it in the form $\Delta=\{0,5; 1,5\}$. At the same time, it is proposed to start finding the difference in the number of ones and zeros in the code with coefficients with $\Delta^*>\Delta_{\min}$:

$$\left\{a_?^+\right\}=\left\{a_{>1}^{\Delta^*}\right\}\cup\left\{a_{>0}^{\Delta^*}\right\}.$$

Calculation of set $\{a\}$ coefficients using the developed attributed binary tree allows to find the values of the dependence coefficients of the controlled features using formula (5). The presence of dependence of the controlled signs characterizes the presence of leakage of data transmission channels.

5. 4. Verification of the developed method's functioning

The application of the developed method for synthesizing an information-analytical system for assessing the level of information transmission channels protection is characterized by such an example.

To make the calculation processes easier to understand, two control signs are used: the results of measuring the voltage in the information transmission channel.

Feature u characterizes the permissible voltage of the information transmission channel in the range 5 V±0.5 V. Feature Δu characterizes the permissible voltage drop when the supply voltage of the information transmission channel changes in the range 0.5 V±0.05 V. Using the proposed method, the value of the associative dependence of characteristics is calculated.

Feature u during normal (standard) operation of the information transmission channel takes the following values:

$$u_1=5-0.5=4.5\ (\text{V});\ u_2=5.0\ \text{V};\ u_3=5.5\ \text{V}.$$

The attribute with the obtained values corresponds to three unary predicates: $\varphi_1(\tau)$, $\varphi_2(\tau)$, $\varphi_3(\tau)$, where τ – number of control voltage measurement in the information transmission channel.

Predicate $\varphi_u(\tau)$ corresponds to the value "true" when $u=u_2$. For values $u=u_1=4.5$ V and $u=u_3=5.5$ V predicate $\varphi_u(\tau)$ corresponds to the value "false".

The values of the range of changes in the characteristic Δu are determined in a similar way:

$$\Delta u_1=0.5-0.05=0.45 \text{ V}; \Delta u_2=0.5 \text{ B}; \Delta u_3=0.55 \text{ V}.$$

The following unary predicates will correspond to the features with the resulting values. Predicate $\varphi_i(\tau)$ corresponds to the value "true" when $\Delta u=\Delta u_2$. When $\Delta u=\Delta u_1$ and $\Delta u=\Delta u_3$ predicate $\varphi_i(\tau)$ corresponds to the value "false".

When checking for data leakage of the information transmission channel, 15 measurements were performed. The following results were obtained:

– at 5 measurements (1) $\varphi_u(\tau)\wedge(1)\ \varphi_{\Delta u}(\tau)$;
– in 4 measurements (0) $\varphi_u(\tau)\wedge(0)\ \varphi_{\Delta u}(\tau)$;
– in 2 measurements (1) $\varphi_u(\tau)\wedge(0)\ \varphi_{\Delta u}(\tau)$;
– in 4 measurements (0) $\varphi_u(\tau)\wedge(1)\ \varphi_{\Delta u}(\tau)$.

Then, the coefficients of the set of obtained features are formed as follows:

$$a_{11}=5;\ a_{00}=4;\ a_{10}=2,\ a_{01}=4;$$

$$\{a\}-\{a_{11}, a_{00}, a_{10}, a_{01}\}-\{5, 4, 2, 4\},\ n-4;$$

$$\{a_\Sigma\}=\{a_{=1}\}\cup\{a_{=0}\}\cup\{a_{>1}\}\cup\{a_{>0}\}=$$
$$=\{a_{11}\}\cup\{a_{00}\}\cup\{\varnothing\}\cup\{\varnothing\},$$

where ∅ – empty set symbol.

Fig. 2 shows a diagram of the distribution of measurements of control characteristics (coefficients a_{ij} of the set of obtained signs $\{a\}$) when checking for data leakage of an information transmission channel.

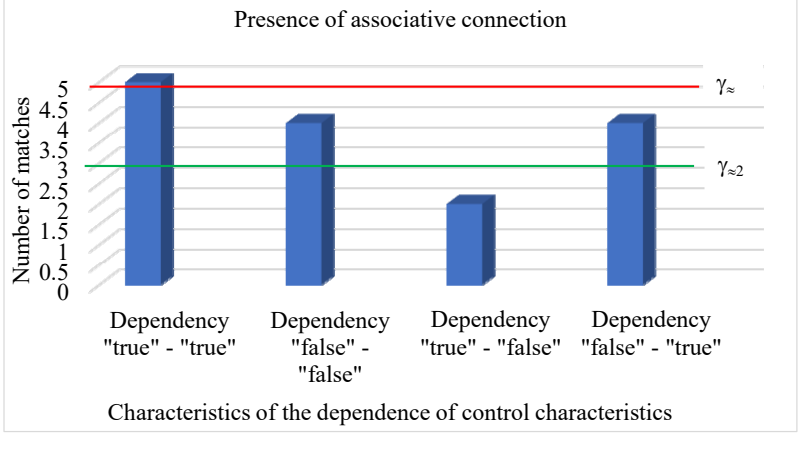

Fig. 2. Control characteristics measurements distribution diagram

The line (red) is a marker of the presence of a relationship between control characteristics, i.e. presence of data leakage (Fig. 2). This line is obtained as the arithmetic average of the number of correspondences "true" – "true" (5 measurements) and "false" – "false" (4 measurements). The line (green color) is obtained as the arithmetic mean of the number of correspondences "true" – "false" (2 measurements) and "false" – "true" (4 measurements). The results of the analysis of the obtained dependencies (Fig. 2) make it possible to identify the presence of an associative connection between control characteristics (green line below red).

Assessing the presence of associative dependence using the proposed method for calculating set {a} coefficients is carried out using the developed attributed binary tree.

Coefficient $n_\Sigma=½,\cdot n=2$, then a set of nodes $\{a_{=1}\}$, $\{a_{=0}\}$, $\{a_{>1}\}$ and $\{a_{>0}\}$ correspond to the nodes of associative similarity of the set $\{a^+\}=\{a_{11}, a_{00}\}$. At the same time, set of nodes $\{a_{0=1}\}$ correspond to the nodes of the associative difference of the set $\{a^-\}=\{a_{10}, a_{01}\}$. Using the proposed expression (5), let's calculate a numerical measure of the dependence of control characteristics u and Δu:

$$\gamma_{\approx 2}=(a_{10}\cdot a_{01})/(a_{11}\cdot a_{00})=(2\cdot 4)/(5\cdot 4)=0.4. \quad (6)$$

The resulting value of the associative dependence $\gamma_{\approx 2}=0.4<1$. This means that there is an associative similarity (dependence) of features u and Δu information transmission channel. This means that the results of the measurements revealed the presence of a data leak in the information transmission channel. In this case, when determining the data leakage channel, it is sufficient to measure the voltage or voltage drop, i.e. one of two signs.

6. Discussion of the results of developing a method for synthesizing an automated decision-making system

The proposed method for synthesizing an information-analytical system for assessing the level of information transmission channels protection made it possible to obtain equations for determining the associative connection between control features. At the same time, the conditions for applying the proposed equations were determined depending on the arity of the nodes of the constructed binary tree.

The obtained results of applying the developed synthesis method make it possible to increase the reliability of determining data leakage in information transmission channels. Thus, the obtained results of determining the relationship between two groups of voltage measurements make it possible to identify associative similarities. The identified relationship between the control signs characterizes the presence of a data leak in the information transmission channel. This conclusion is confirmed by the result of applying formula (6) and condition (5) of the proposed method. The obtained result can be explained physically: the presence of data leakage in the information transmission channel leads to a change (decrease) in the voltage (or power) of the information channel. Such changes are associated with the redistribution of energy between the "main" and "false" channels of information transmission. Thus, the voltage drop in the information transmission channel Δu will be higher than the threshold value when the information transmission voltage u changes in the presence of data leakage. This conclusion is confirmed by the results obtained (calculations using formula (6) and data in Fig. 2), which allows to assert the presence of a data leak in the information transmission channel. The formulated conclusions about the physical justification of the results obtained do not contradict similar conclusions obtained by other authors about the possibility

of detecting data leaks in information systems [2–18]. The proposed algorithm for searching for the associative dependence of control features for quickly identifying the presence of a data leak should be constantly used during the operation of the information transmission channel. Therefore, for a systematic analysis of the control signs of a data leak, a method for synthesizing an appropriate information and analytical system is proposed.

Proposals for the application of the obtained research results are characterized as follows. The proposed method can be used in further research in the field of information security, for example, in continuing research [12, 13, 16]. The study [12] developed models for estimating channel state information in the transmitter and receiver. The use of the proposed method in the development (improvement) of such models will make it possible to detect data leakage separately at the receiver or transmitter. This will allow to quickly identify data leaks without involving the costly procedure of joint analysis of the quality of information transmitted from the transmitter to the receiver. Paper [13] presents a methodology for analyzing the effectiveness of primary protection systems for power lines, based on a probabilistic approach to the successful operation of protection systems. The use of the proposed method in the development (improvement) of the presented methodology will improve the reliability of information transmission channels due to the timely detection of data leaks. In [16], the influence of communication channel delay on line protection functions in the time domain is studied. The use of the proposed method in the development (improvement) of the presented approach will improve the security of information transmission channels.

The limitations of this study lie in the accepted condition of serviceability of the information transmission channel. Therefore, the algorithm for applying the developed method consists of two stages. At the first stage, the technical condition of the information transmission channel is monitored. Provided that the channel is technically sound (the accepted condition for the applicability of the proposed method), the second stage is performed – the synthesis of an information and analytical system for assessing the level of information transmission channels protection.

The disadvantage of this study is the assumption that there is no interference when transmitting data via an information channel. The presence of interference, especially caused by an electromagnetic field, can have a significant impact on the process of determining the dependence of control characteristics. And this will introduce an additional error in determining a data leak in the information transmission channel.

The development of this research consists in substantiating the multi-criteria optimization problem of an algorithm for data leaks searching in an information transmission channel under conditions of strong electromagnetic fields. Solving this problem will make it possible to determine a rational algorithm for filtering out possible "false" positives of associative similarity of controlled features under conditions of strong electromagnetic interference.

7. Conclusions

1. To generate a variety of control signs for the presence of an information leakage channel, it is proposed to use logical values. To do this, the elements of the set of control characteristics are translated into logical values. A hypothesis is proposed that characterizes the multidimensional association of the presence of an associative connection between control characteristics. A feature of the proposed method for synthesizing an information-analytical system for assessing the level of information transmission channels protection is the departure from the classical scheme for identifying correlation dependence between control features. The presented results of the control features formation can be useful in the development of software for expert decision-making systems to increase the reliability and security of information transmission channels.

2. To carry out calculations of the numerical measure of associative dependence of control characteristics, the use of an attributed binary tree is proposed. The nodes of the resulting binary tree are represented as "code". This "code" corresponds to the logical values of the control characteristics. It is substantiated that the classification of nodes of the resulting tree depends on the calculated set, which characterizes the number of nodes of associative difference or similarity.

3. Using the "codes" of an attributed binary tree, a procedure for calculating the value of the dependence coefficients of control characteristics is developed. The proposed coefficient characterizes the associative similarity between control characteristics. A rule for determining the dependence of control characteristics is formulated. The presence of dependence of the controlled signs characterizes the presence of data transmission channels leakage.

4. The results of testing the performance of the developed method allow to characterize the method as practically implementable. The dependence between control features identified using the proposed method makes it possible to identify data leaks in the information transmission channel. The resulting diagram of the distribution of the number of correspondences of measurements to the characteristics of the assumed (introduced by the hypothesis) associative dependence between control characteristics confirms the introduced hypothesis. Confirmation of the hypothesis (graphical and calculation) allows to identify the presence of information leakage. The obtained result is physically justified, which confirms the adequacy of the results obtained.

Conflict of interest

The authors declare that there are no conflicts of interest regarding this study, including financial, personal, authorship or other nature, which could influence the research and its results presented in this article.

Financing

The study was conducted without financial support.

Data availability

The manuscript has no associated data.

Use of artificial intelligence

The authors confirm that they did not use artificial intelligence technologies when creating the presented work.

References

1. Yevseiev, S., Hryshchuk, R., Molodetska, K., Nazarkevych, M., Hrytsyk, V., Milov, O. et al.; Yevseiev, S., Hryshchuk, R., Molodetska, K., Nazarkevych, M. (Eds.) (2022). Modeling of security systems for critical infrastructure facilities. Kharkiv: PC TECHNOLOGY CENTER, 196. https://doi.org/10.15587/978-617-7319-57-2
2. Yevseiev, S., Kuznietsov, O., Herasimov, S., Horielyshev, S., Karlov, A., Kovalov, I. et al. (2021). Development of an optimization method for measuring the Doppler frequency of a packet taking into account the fluctuations of the initial phases of its radio pulses. Eastern-European Journal of Enterprise Technologies, 2 (9 (110)), 6–15. https://doi.org/10.15587/1729-4061.2021.229221
3. Sokolov, A. Y. (1999). Algebraic approach on fuzzy control. IFAC Proceedings Volumes, 32 (2), 5386–5391. https://doi.org/10.1016/s1474-6670(17)56917-7
4. Yevseiev, S., Ponomarenko, V., Laptiev, O., Milov, O., Korol, O., Milevskyi, S. et al.; Yevseiev, S., Ponomarenko, V., Laptiev, O., Milov, O. (Eds.) (2021). Synergy of building cybersecurity systems. Kharkiv: PC TECHNOLOGY CENTER, 188. https://doi.org/10.15587/978-617-7319-31-2
5. Shao, R., Ding, C., Liu, L., He, Q., Qu, Y., Yang, J. (2024). High-fidelity multi-channel optical information transmission through scattering media. Optics Express, 32 (2), 2846. https://doi.org/10.1364/oe.514668
6. Kumar, P., Saxena, V. (2024). Nested Levels of Hybrid Cryptographical Technique for Secure Information Exchange. Journal of Computer and Communications, 12 (02), 201–210. https://doi.org/10.4236/jcc.2024.122012
7. Mikoni, S. V. (2023). Approach to assessing the level of intelligence of an information system. Ontology of Designing, 13 (1), 29–43. https://doi.org/10.18287/2223-9537-2023-13-1-29-43
8. Ramsden, J. (2023). The Transmission of Information. Bioinformatics, 75–91. https://doi.org/10.1007/978-3-030-45607-8_7
9. Laue, F., Jamali, V., Schober, R. (2023). RIS-Assisted Device Activity Detection With Statistical Channel State Information. IEEE Transactions on Wireless Communications, 22 (12), 9473–9487. https://doi.org/10.1109/twc.2023.3271365
10. Vähä-Savo, Lauri, Veggi, L., Vitucci, E. M., Icheln, C., Degli-Esposti, V., Haneda, K. (2023). Analytical Characterization of a Transmission Loss of an Antenna-Embedded Wall. https://doi.org/10.36227/techrxiv.170244520.01558910/v1
11. Elzinga, R., Janssen, M. J., Wesseling, J., Negro, S. O., Hekkert, M. P. (2023). Assessing mission-specific innovation systems: Towards an analytical framework. Environmental Innovation and Societal Transitions, 48, 100745. https://doi.org/10.1016/j.eist.2023.100745
12. Kramer, G. (2023). Information Rates for Channels with Fading, Side Information and Adaptive Codewords. Entropy, 25 (5), 728. https://doi.org/10.3390/e25050728
13. Dos Santos, A., Barros, M. T. C. de, Correia, P. F. (2015). Transmission line protection systems with aided communication channels – Part II: Comparative performance analysis. Electric Power Systems Research, 127, 339–346. https://doi.org/10.1016/j.epsr.2015.05.010
14. Enquist, M., Ghirlanda, S., Lind, J. (2023). Acquisition and Transmission of Sequential Information. The Human Evolutionary Transition, 167–176. https://doi.org/10.23943/princeton/9780691240770.003.0012
15. Menezes, T. S., Barra, P. H. A., Dizioli, F. A. S., Lacerda, V. A., Fernandes, R. A. S., Coury, D. V. (2023). A Survey on the Application of Phasor Measurement Units to the Protection of Transmission and Smart Distribution Systems. Electric Power Components and Systems, 52 (8), 1379–1396. https://doi.org/10.1080/15325008.2023.2240320
16. Ribeiro, E. P. A., Lopes, F. V., Silva, K. M., Martins-Britto, A. G. (2023). Assessment of communication channel effects on time-domain protection functions tripping times. Electric Power Systems Research, 223, 109589. https://doi.org/10.1016/j.epsr.2023.109589
17. Shmatko, O., Herasymov, S., Lysetskyi, Y., Yevseiev, S., Sievierinov, O., Voitko, T. et al. (2023). Development of the automated decision-making system synthesis method in the management of information security channels. Eastern-European Journal of Enterprise Technologies, 6 (9 (126)), 39–49. https://doi.org/10.15587/1729-4061.2023.293511
18. Herasymov, S., Tkachov, A., Bazarnyi, S. (2024). Complex method of determining the location of social network agents in the interests of information operations. Advanced Information Systems, 8 (1), 31–36. https://doi.org/10.20998/2522-9052.2024.1.04
19. Gerasimov, S. V., Slupskiy, P. S., Feklistov, A. A., Chuykov, D. V. (2005). Metod opredeleniya koeffitsientov zavisimosti kontroliruemyh parametrov na osnove atributirovannogo binarnogo dereva. Systemy obrobky informatsiyi, 3 (43), 48–55. Available at: http://nbuv.gov.ua/UJRN/soi_2005_3_9
20. Fedushko, S., Molodetska, K., Syerov, Y. (2023). Analytical method to improve the decision-making criteria approach in managing digital social channels. Heliyon, 9 (6), e16828. https://doi.org/10.1016/j.heliyon.2023.e16828
21. Mookerjee, R., Samuel, J. (2023). Managing the security of information systems with partially observable vulnerability. Production and Operations Management, 32 (9), 2902–2920. https://doi.org/10.1111/poms.14015
22. Marabissi, D., Abrardo, A., Mucchi, L. (2023). A new framework for Physical Layer Security in HetNets based on Radio Resource Allocation and Reinforcement Learning. Mobile Networks and Applications. https://doi.org/10.1007/s11036-023-02149-z