In the process of transmission channels functioning, the results of the work of bodies for detecting and blocking information leakage channels are not sufficiently taken into account. Management of information protection channels is actually the collection and display of data followed by the assignment of influence on each information channel separately and is carried out in manual mode. In decision support systems, the tasks of identifying information leakage channels are not solved. There is a contradiction between the requirements for the automation of the management of information protection channels and the possibility of meeting these requirements at the expense of the available automation tools. Classical theory considers the decision-making process as a choice of one of many alternatives. The development of rational forms and methods of managing information protection channels should prevent threats and challenges. Therefore, the object of research is the process of ensuring security during data transmission through information channels. The main threats and challenges are man-made and natural cataclysms, terrorism, aggression by a number of states or individual groups of people, which are not taken into account in the complex in the decision-making system during the management of information protection channels. A structural diagram of information exchange based on the description of a weakly formalized process under conditions of non-stochastic uncertainty is proposed. It is proposed to use the logical-linguistic production model. For a hierarchically organized structure based on classification features, it is proposed to build a hierarchy tree that takes into account the relationships of partially ordered sets. The formed production rules for determining appropriate strategies for the planned detection of information leakage channels based on predicted values allow to proceed to knowledge processing for the synthesis of an automated decision-making system during the management of protection channels

Keywords: information channel, information protection, logical-linguistic model, production rules, information leakage

UDC 623.618.51
DOI: 10.15587/1729-4061.2023.293511

DEVELOPMENT OF THE AUTOMATED DECISION-MAKING SYSTEM SYNTHESIS METHOD IN THE MANAGEMENT OF INFORMATION SECURITY CHANNELS

Olexander Shmatko
PhD, Associate Professor
Department of Software Engineering and Management Intelligent Technologies**
Serhii Herasymov
Doctor of Technical Sciences, Professor*
Yurii Lysetskyi
Doctor of Technical Sciences
General Director
SNT Ukraine
Akademika Palladina ave., 44A, Kyiv, Ukraine, 03142
Serhii Yevseiev
Corresponding author
Doctor of Technical Sciences, Professor*
E-mail: Serhii.Yevseiev@gmail.com
Oleksandr Sievierinov
PhD, Associate Professor
Department of Information Technology Security
Kharkiv National University of Radio Electronics
Nauky ave., 14, Kharkiv, Ukraine, 61166
Tetiana Voitko
Researcher
Research Department
Institute of Information and Communication Technologies and Cyber Defense ***
Andrii Zakharzhevskyi
PhD
The National Security and Defence Strategy Department***
Helen Makogon
PhD, Associate Professor
Department of Armored Vehicles and Military Equipment
Military Institute for Tank Troops of the National Technical University "Kharkiv Polytechnic Institute"
Poltavsky Shlyakh str., 192, Kharkiv, Ukraine, 61198
Alexander Nesterov
PhD, Deputy Chief of the Department
Department of Combat Application of Communication Units
Kruty Heroes Military Institute of Telecommunications and Information Technology
Knyaziv Ostrozkih str., 45/1, Kyiv, Ukraine, 01011
Kyrylo Bondarenko
Postgraduate Student*
*Department of Cybersecurity**
**National Technical University "Kharkiv polytechnic institute"
Kyrpychova str., 2, Kharkiv, Ukraine, 61002
***The National Defence University of Ukraine
Povitroflotskyi ave., 28, Kyiv, Ukraine, 03049

Received date 27.09.2023
Accepted date 15.12.2023
Published date 21.12.2023

How to Cite: *Shmatko, O., Herasymov, S., Lysetskyi, Y., Yevseiev, S., Sievierinov, O., Voitko, T., Zakharzhevskyi, A., Makogon, H., Nesterov, A., Bondarenko, K. (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. doi: https://doi.org/10.15587/1729-4061.2023.293511*

1. Introduction

Decision-making tasks when managing information security channels are not automated at a sufficient level [1, 2]. This leads to the fact that decisions to block information transmission channels are made on the basis of subjective assessments of decision makers (DMs), or using insufficiently complete information models. At the same time, in the process of functioning of information transmission channels, the results of the work of bodies identifying and blocking information leakage channels are poorly taken into account [3, 4].

Thus, managing information security channels now actually means collecting and displaying information about a possible data leak. Then influence (blocking) is assigned to each information channel separately and is carried out, in fact, manually.

In fact, the information coming from different sources to the decision maker is manually summarized, channels of information leakage are identified and possible options for action to manage information security channels are developed. As a result, the time required to make a decision increases and the effectiveness of preventing information leakage decreases [5, 6]. This is due to:

– problems of developing a unified approach to describing the properties of the subject area under consideration and procedures for the logical and analytical activities of decision makers in managing information security channels;

– lack of a systematic approach to the development of information technologies to support decision-making on managing information security channels under uncertainty conditions;

– lack of taking into account the results of a priori logical and analytical activity of the decision maker at the stage of planning the transfer of information through information channels.

An automated system for managing information security channels is needed to effectively use the knowledge acquired at the planning stage when managing information data transmission channels. For this purpose, decision support systems (DSS) are used [7, 8]. However, in classical DSS, problems of this class are not solved. Thus, there is a contradiction between the requirements for automating the management of information security channels and the ability to satisfy these requirements using existing automation tools and information technologies. This contradiction is determined by a contradiction in science. It consists in the absence of an appropriate method for synthesizing an automated decision-making system when managing information security channels to formalize decision-making tasks that meet the requirements of practice. Thus, the development of a method for synthesizing an automated decision-making system for managing information security channels is an urgent scientific task.

2. Literature review and problem statement

The analysis [7, 9, 10] showed that the classical theory considers the decision-making process as a choice of one of many alternatives. At the same time, the process of presenting a decision-making problem remains outside the scope of research. The development of rational forms and methods for managing information security channels should, if possible, forestall threats and challenges [11, 12]. The main threats and challenges in the near future are:

– technological and natural disasters;

– terrorism, aggression (including attacks on information data transmission channels) from a number of states or certain groups of people [13, 14].

Such threats and challenges as a whole are not taken into account in decision-making systems when managing information security channels, especially since there are no such automated systems.

Work [9] explores solutions and provides methods for increasing the confidentiality and security of a wireless communication channel. This work focuses on implementing a beamforming technique combined with a combination of MIMO-OFDM techniques to improve physical layer security in the downlink of a wireless communication link. However, the induced results do not allow to determine possible channels of information leakage during data transmission.

The use of a cascade information transmission channel, considered in [10], is a complex task. This publication [10] is the first to show an analytical transformation for solving the intractable probabilistic constraint of downtime of an information transmission channel. Safe maximization of energy efficiency is chosen as the objective function, and the resulting resource optimization is processed using an alternative maximization framework. However, this approach does not allow identifying indicators (criteria) of the presence of information leakage channels. New meta-optics opens up unprecedented possibilities in optical imaging, information storage and encryption. In particular, recent advances in vector holography based on multi-parameter Jones matrix manipulation have increased the modulation space and information capacity [11]. However, the extreme limit of the fundamental degree of freedom (DoF) in Jones matrix optical encoding space limits the information capacity for highly demanding practical applications. Work [12] uses four T-test based metrics to evaluate the resistance to side-channel attacks. The results based on the correlation coefficient show the correlation between resistance to side-channel attacks and performance. However, the results of the study do not allow managing information security channels under conditions of uncertainty. Work [13] proposes a security authentication scheme that uses predictive mechanisms to detect spoofing attacks. However, this scheme has not been adapted to an automated decision-making system for identifying information leakage channels. Work [14] uses two-factor authentication, in which an authorization code is sent over a separate channel. This approach admittedly incurs significant overhead in terms of both the use of additional channels and the need for additional processing. At the same time, no analysis is carried out of the costs impact on improving security and accessibility when transmitting information. Work [15] considers the security of information transmission at the physical level as an additional level of security that ensures the confidentiality of radio communications. Typical characteristics of a wireless channel (noise, interference) can be used to keep the message confidential from potential eavesdroppers. Coordinated planning of channel switching between different cells using the same radio resources is proposed, based on the use of spatial information. At the same time, the reliability of information transmission is not examined. Research [16] presents a side-channel estimation methodology that offers strong theoretical calculations to determine the reliability of the channels. In this case, effective tools are calculations confirmed by heuristic (sometimes specific to a particular case) methods. The disadvantage of this study is the accepted hypothesis that training information, which ensures the required reliability of information transmission channels, is determined on the basis of hypothetical information for practically significant models. In [17], options for ensuring the reliability of information transmission channels using various types of threat models are considered. A proof of security is shown in the most realistic threat model, the so-called noisy leak adversary. This model well reflects how real attackers operate through side channels. However, possible options for predicting information leakage channels and eliminating such channels are not explored. The work [18] proposed the implementation and testing of a scalable EHR management system based on blockchain. The disadvantage of this work is the two-channel transmission of

information, which does not provide the necessary reliability. The work [19] presents the results of an analysis of the requirements and goals of information leakage analysis for a specific data transmission channel architecture. It is proposed to analyze information leaks using the Microwalk modular side-channel analysis platform, which checks execution traces for leaks through memory access. However, no approach to closing possible channels of information leakage is proposed. Research [20] examined the decision-making process associated with managing digital communities in an ecosystem of digital social channels, especially in the context of antagonistic digital communication and the spread of harmful content. The proposed method is based on the analysis of the information situation in the management of digital communities under conditions of complete uncertainty, antagonistic behavior and partial uncertainty. However, there are no research results on the possible influence of unreliable channels (hacked channels) of information transmission on decision making. Work [21] discusses methods for maintaining the security of information systems, the degree of vulnerability of which is partially observable. In each period, the decision maker needs to make one of three decisions: do nothing, test and implement (fix the vulnerability) if necessary, and implement directly. The disadvantage of the study is the lack of calculation of indicators that will help make this or that decision (there is no ranking of threats). The work [22] explores machine learning methods for creating automated systems for processing huge amounts of data. The proposed results can be used to create automated decision-making systems. The disadvantage of this work is the proposal to create automated decision-making systems without operator participation. This violates the duties of decision makers towards decision-making subjects, duties that are both epistemic and practical. Violations of this kind give rise to compelling reasons to object to the use of opaque decision-making systems.

Thus, the analysis showed that well-known publications in the field of information security and decision-making systems to ensure reliability are aimed at solving narrow problems. The former offer methods for increasing the reliability of data transmission and identifying information leakage channels. The latter are aimed at solving problems of creating decision-making systems using various mathematical approaches. At the same time, the first direction of publications does not allow to eliminate the reasons for the implementation of threats, and the second direction does not provide the required level of reliability when making decisions. Therefore, it is justified to conduct research into the development of a method for synthesizing a system for automating decision-making processes for managing information security channels.

3. The aim and objectives of the study

The aim of this study is to develop a method for synthesizing an automated decision-making system for managing information security channels, which takes into account uncertainty in determining information leakage channels and allows to ensure the required level of security.

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

– to develop a structural diagram of information exchange when managing information security channels;

– to build a logical-linguistic hierarchical production model for determining information security parameters;

– to develop a method for formalizing knowledge to determine appropriate strategies for the planned information security process.

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. To ensure the security of data transmission, the process of managing information security channels (ISC) when eliminating threats and challenges is proposed to be presented in the form of a diagram (Fig. 1). The proposed scheme for managing information security channels to eliminate threats of information leakage and their consequences will allow the development of a DSS. In this case, as a rule, the time available to the relevant management control body T_{av} and the time required to make a decision T_{nec} are related as $T_{av} \leq T_{nec}$ [7].

Ensuring the required efficiency of managing information security channels is achieved by automating management processes [2].

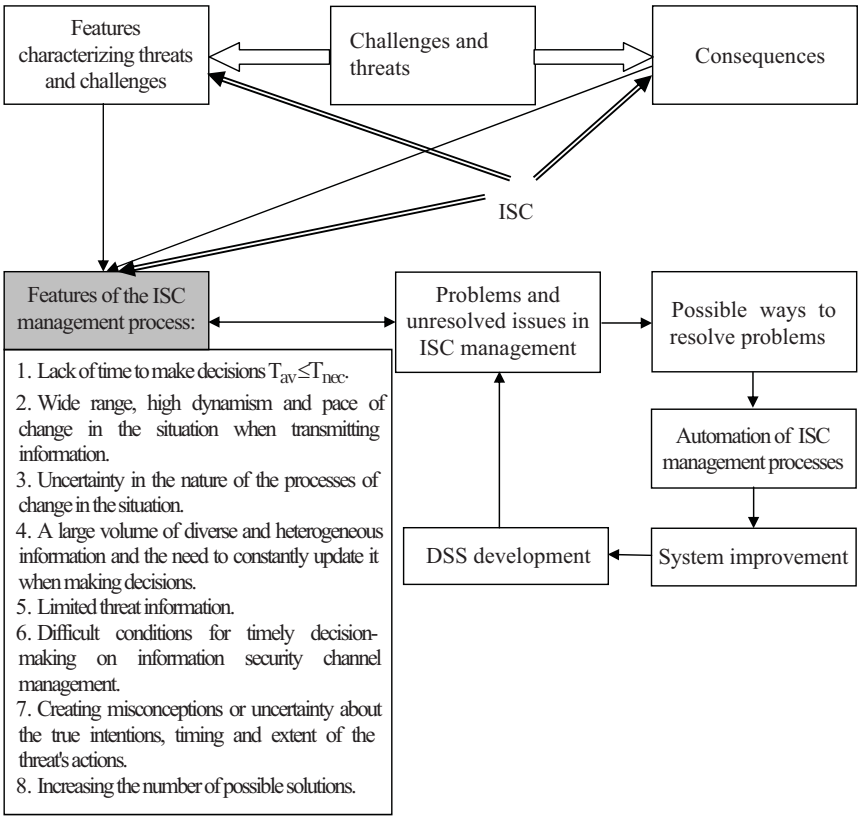

Fig. 1. The process of managing information security channels to eliminate threats of information leakage and their consequences

The method for synthesizing an automated decision-making system for managing information security channels is a consistent solution to research problems. In general, the stages of the proposed method consist of:

– development of a structural diagram of information exchange when managing information security channels;

– constructing a logical-linguistic hierarchical production model for determining information security parameters;

– developing a method for formalizing knowledge to determine appropriate strategies for the planned information security process.

5. Development of a method for synthesizing an automated decision-making system

5. 1. Development of a structural diagram of information exchange when managing information security channels

Managing information security channels includes advance preparation and direct management [3]. Let`s present the block diagram of information exchange when managing information security channels in the form of the following diagram (Fig. 2).

A special feature of the proposed structural diagram is the consideration of both intellectual and technical features when making decisions when managing information security channels. Let's note that by intellectual features it is possible to mean the conclusions and proposals of the decision maker for managing information security channels. It is proposed to include technical features for monitoring information transmission channels and technical means for identifying (blocking) channels of possible information leakage. The proposed structure simplifies further solution of research problems.

The solution to the problem of assigning impacts when managing information security channels to cover information leakage is to determine the possibility of redirecting information through other channels. This decision depends on the method of identifying the channel of information leakage (technical channels of information leakage), the means of information leakage (technical means of espionage), the software speed of information transmission, and the information dissemination program. When solving such a problem, the time required to determine the threat and methods of influence to eliminate it is also calculated [4].

Thus, when assigning impacts on information leakage channels and areas of possible information attacks, this is a difficult logical and analytical task to solve.

The final results of solving the problem of assigning impacts to block information leakage channels are assessed qualitatively – if possible, automated control of information security channels [5].

5. 2. Construction of a logical-linguistic hierarchical production model for determining information security parameters

After determining the parameters that most strongly influence the channels of possible information leakage, many production rules are formed to determine appropriate strategies for the planned information security process [5]. At the stage of direct planning, the DSS offers recommendations on the application of an appropriate strategy for the planned information protection [6]. To solve the problem of forming production rules for determining appropriate information security strategies, expert assessment methods are used [7]. Solving this problem allows to move on to further processing of knowledge to support decision-making when managing information security channels.

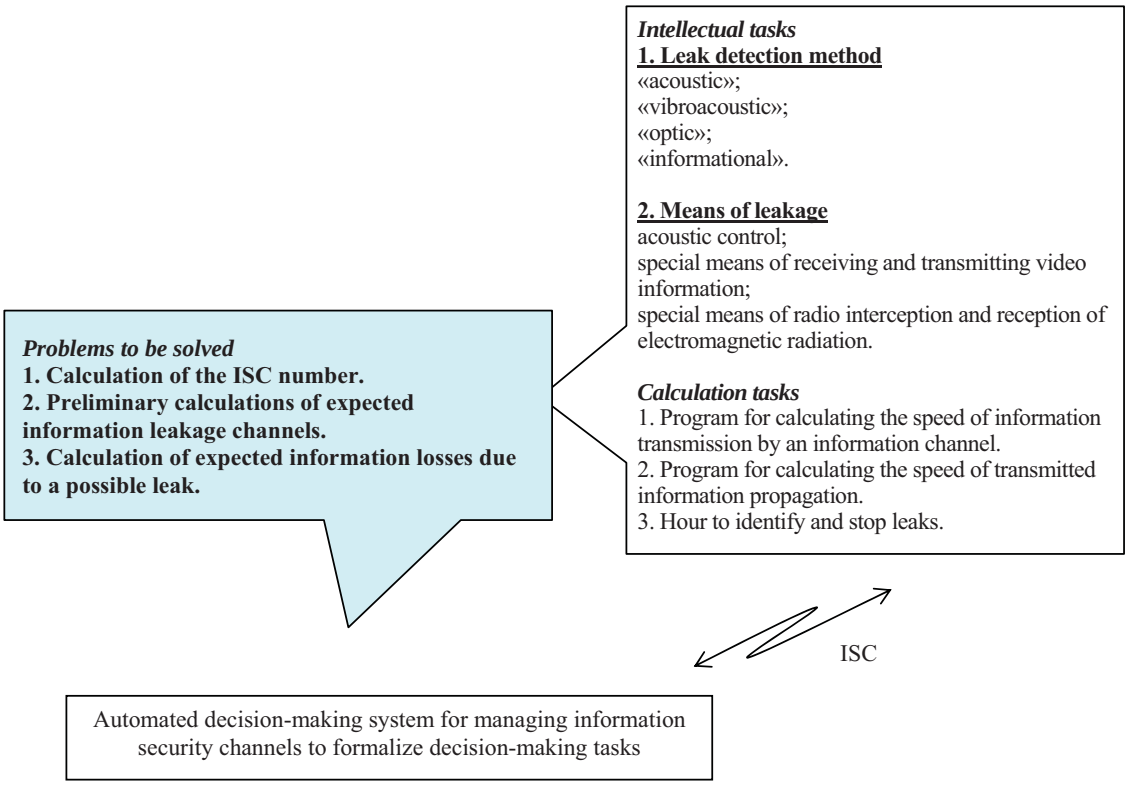

Fig. 2. Block diagram of information exchange when managing information security channels

To describe a weakly formalized process, which is the procedure for determining the parameters of planned information protection under conditions of non-stochastic uncertainty, it is advisable to choose a logical-linguistic production model [8]. For a hierarchically organized structure based on classification characteristics, it is proposed to build a hierarchy tree. It displays the relationships between partially ordered sets. The skeleton of the tree is the hierarchy of tasks solved when developing recommendations for determining information security parameters $L=\{L_0, L_1, \ldots L_m\}$. Each hierarchy level defines its own subset of the system $L_r=\left\{ l_1^{(r)},\ldots,l_k^{(r)}\right\}$ (Fig. 3). Then the logical-linguistic production model has the form:

$$\bigcup_{j=1}^{m_i}\text{conseq}R_{i-1,j}^{(k)}=\text{antec}R_i^{(k)}, \quad (1)$$

where R defined by multiple sets of rules $R=\{r_1, r_2, \ldots, r_n\}$, such that:

$$R:\begin{cases}\text{IF } x_1=\alpha_1^{(1)} \text{ AND } x_2=\alpha_2^{(1)}\ldots\left[\text{AND } x_k=\alpha_k^{(1)}\right]\ldots x_n=\alpha_n^{(1)}\\ \text{THEN } y_1=d_1,\\ \text{IF } \quad x_1=\alpha_1^{(2)} \text{ AND } x_2=\alpha_2^{(2)}\ldots\left[\text{AND } x_k=\alpha_k^{(2)}\right]\ldots x_n=\alpha_n^{(2)}\\ \text{THEN } y_2=d_2,\\ \qquad\qquad\ldots\ldots\ldots\\ \text{IF } x_1=\alpha_1^{(m)} \text{ AND } x_2=\alpha_2^{(m)}\ldots\left[\text{AND } x_k=\alpha_k^{(m)}\right]\ldots x_n=\alpha_n^{(m)}\\ \text{THEN } y_m=d_m.\end{cases} \quad (2)$$

$i=\overline{1,n}$ – number of rules in the set r_i, $i=\overline{1,n}$ (elements in square brackets are optional):

$$R_1:\bigcup_{j=1}^{m_{n0}}L_{0,j}\to L_1,\quad L_0=\left\{l_1^{(0)},l_2^{(0)},\ldots,l_{k_0}^{(0)}\right\};$$

$$R_2:\bigcup_{j=1}^{m_{n_1}}L_{1,j}\to L_2,\quad L_1=\left\{l_1^{(1)},l_2^{(1)},\ldots,l_{k_1}^{(1)}\right\};$$

.....

$$R_M:\bigcup_{j=1}^{m_{n_{m-1}}}L_{m-1,j}\to L_m,\quad L_m=\left\{l_1^{(m)},l_2^{(m)},\ldots,l^{(m)}_{k_n}\right\};$$

$l_{ij}^{(k)}$ – linguistic variables.

The $_n$ number of set rules is in the range $0<k_i\le\prod_{i=1}^{n}card\left(S(x_i)\right),$, where $cardS\left((x_i)\right)$ – power of term-set of variable x_i, $i=\overline{1,n}$.

Let's describe the dynamics of the process of determining information security parameters using interconnected tables of linguistic rules connecting the current and future states of the described process [9]:

$$Y=R(X_{k-1}, X_k), \quad (3)$$

where X_{k-1}, X_k – system state; R – communication relation; k – model sampling step.

An example of the display is presented in Table 1. Using tables of linguistic rules, the knowledge base of the object is described. The tops of the tree of the hierarchical system are tables of linguistic rules, and the arcs are meta-rules, on the basis of which the required table is selected when the current goal of the DSS is changed.

Table 1

Linguistic rules of a weakly formalized process $Y=X_{k-1}\circ X_k$

$X_{k-1}\backslash X_K$	NB	NS	ZE	PS	PB
NB	NB	NB	NB	NS	ZE
NS	NB	NB	NS	ZE	PS
ZE	NB	NB	ZE	PB	PB
PS	NS	ZE	PS	PB	PB
PB	ZE	PS	PB	PB	PB

Movement along the goal tree is determined by the DSS, which models the central decision-making strategy. Let's build tables of linguistic rules based on production rules for determining appropriate strategies for the planned information security process.

Let the term-set S be defined by the set $S=\{$NB, NS, ZE, PS, PB$\}$ of fuzzy variables, where NB – negative big (very bad), NS – negative small (not very bad), ZE – zero (middle element), PS – positive small (not very good), PB – positive big (very good). Fuzzy variables are fuzzy sets with given membership functions. Then the parameters of the synthesized system, representing mappings of fuzzy linguistic variables, can be represented by corresponding tables of linguistic rules for each information transmission channel.

The parameters of the synthesized system are presented in the form of the following mappings of fuzzy linguistic variables:

– "Information transfer rate" (x_1) and "Speed of dissemination of transmitted information in the information space" (x_2) into the fuzzy variables of the linguistic variable "State of information transmission channels" (Y);

– "The value of the information transmitted" (x_3) and "Interest in receiving information from the enemy" (x_4) into "Conditions for the use of information leakage means" (Z);

– "Reliability of information transmission channels" (x_5) and "Ways of information leakage" (x_6) into "Means for detecting information leaks taking into account technical means of espionage" (T);

– "Situation (information field and the influence of transmitted information on it)" (F), "Information leak detection parameters" (D).

Any processes presented in the form of tables of linguistic rules can be adequately described using an algebraic model [10]. Since the linguistic sets of all variables are homogenized, therefore, it is possible to formalize (approximate) products in the form of algebraic constructions.

The goal of creating an algebraic system for linguistic production models is to provide properties similar to the properties of Euclidean spaces (creation of an abstract vector space). Basic term-set $S=\{S_1,\ldots,S_n\}$, unlike the set of Euclidean space, it is finite, and each of its elements has a linguistic meaning.

In general, tables of linguistic rules are mappings of term-sets $S=\{S_1,\ldots,S_n\}$ to themselves $(+:S\times S\to S)$. Based on the principles of constructing algebraic systems, it is necessary to determine on the base term-set $S=\{S_1,\ldots,S_n\}$ of adding operation elements from S, as well as multiplication by elements of a certain set of coefficients Ω.

As a field Ω let's choose an abstract set for which it is possible to define the external composition law:

$$\times:\Omega\times S\to S, \quad (4)$$

and two internal laws:

$$+_{\omega}:\Omega\times\Omega\circledR\Omega, \quad (5)$$

$$\times_{\omega}:\Omega\times\Omega\circledR\Omega. \quad (6)$$

In accordance with the requirements of a linear space, the set S must have the property of an Abelian group with respect to operation (5). To implement this requirement, the corresponding table must be a composition of permutations of rows of the base term set.

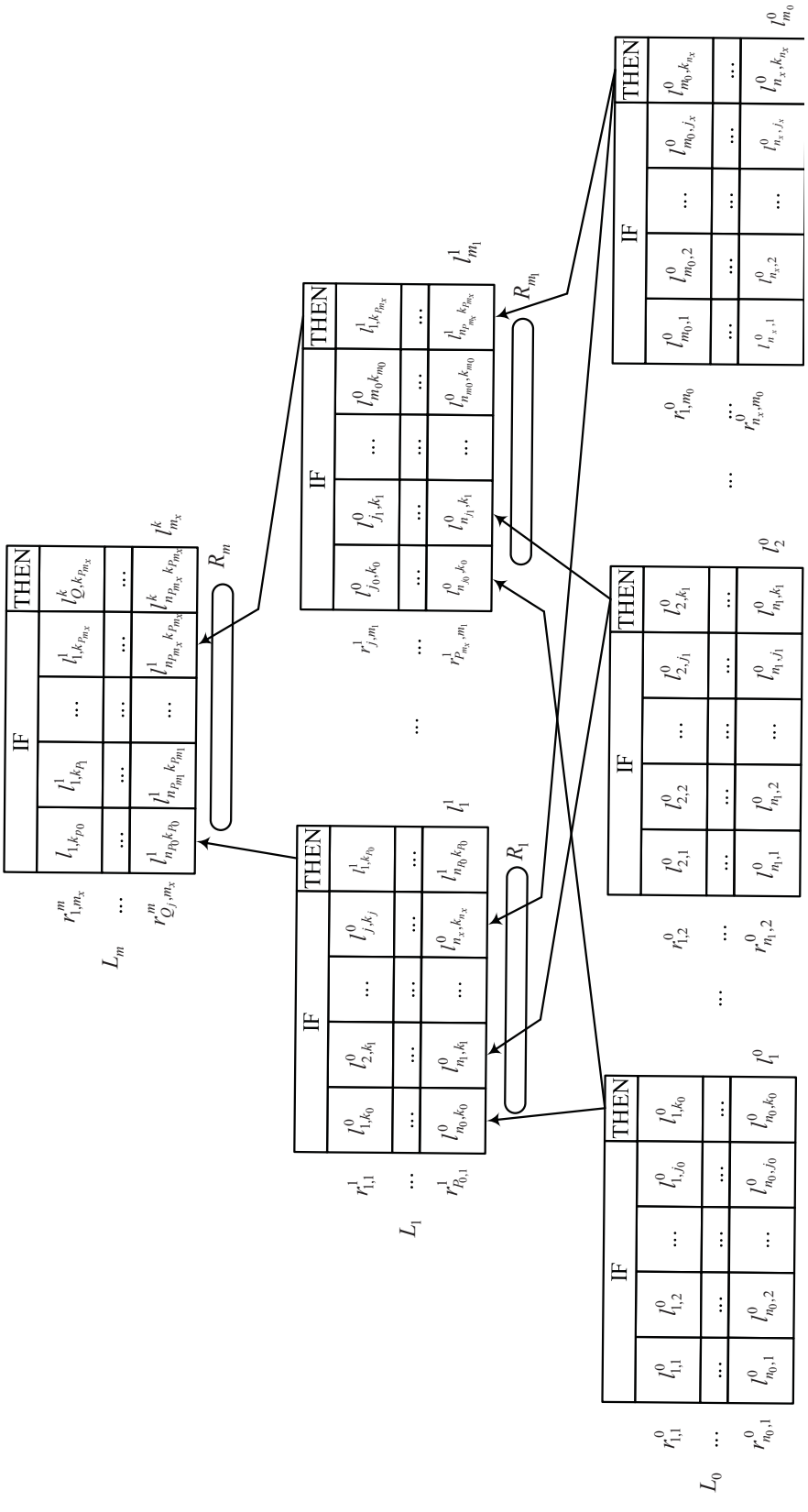

Fig. 3. Logical-linguistic hierarchical production model for determining information security parameters

The linear space S of linguistic variables constructed in this way over the field Ω provides the necessary operations for solving problems of analysis and synthesis of linguistic dynamic systems.

Let`s consider the class of step-by-step linguistic mappings that transfer the system from one level to another. Each hierarchy level determines the state at the i-th step. In m steps the system will go to the state determined by the mapping R_m:$R_{m-1}\{R_{m-2}...R_2([R_1(L_0)]\}\rightarrow L_m$, which can be represented as an algebraic polynomial:

$$R_m = A_0 \cdot L_0 + A_1 \cdot R_1(L_0) + ... + A_{m-1} \cdot R_{m-1}(L_0),$$

where parameters A_i are elements of the set Ω, and the operations of addition and multiplication are understood in the sense of the introduced algebra. The number of polynomials is equal to the number of control objectives.

Thus, the mappings R relate the input variables $X^* = (x_1^*, x_2^*, ..., x_n^*)$, $x_i^* \in [\underline{x_i}, \overline{x_i}]$ and output value $Y=(y_1, y_2, ..., y_m)$. In general, the structure of the rules looks like:

$$\text{IF } \underset{\Im}{\wedge} x = s_{\Im} \text{ THEN } y = s, \qquad (7)$$

where $\Im$ – set of indices of input parameters.

The unified approach proposes to consider not subsets of variables involved in specific rules, but the set of all variables, both in the premise and in the conclusion of the rule. Then mappings (7) can be represented in the form of corresponding linguistic rules. Mapping (7) establishes correspondence in space S^n (n – number of linguistic variables) not only between individual points in space, but also between subspaces of different levels.

5. 3. Development of a method for formalizing knowledge to determine appropriate strategies for the planned information security process

When using models based on a fuzzy representation, there is a transition to the use of abstract mathematical structures that allow to consider the system as a whole at a less detailed level. Simplification is achieved by eliminating unimportant details, and not by reducing the number of variables under study.

Thus, using the algebraic approach, the problem of synthesizing a sequence of rules has been solved. Obviously, it would be difficult to make such a conclusion by examining the tables of linguistic rules that describe the process of determining information security parameters directly.

Production rules have been formed for determining appropriate strategies for the planned identification of information leakage channels based on predicted values. Such rules allow to move on to knowledge processing for the synthesis of an automated decision-making system when managing information security channels to formalize decision-making tasks when identifying information leakage channels. To do this, it is needed to complete the following steps:

1. Analysis of input information: a vector of values of input variables $X^* = (x_1^*, x_2^*, ..., x_n^*)$ is fixed and fuzzy variables of linguistic variables are determined by the values of the features $\langle x_1^*, S_1, ... \rangle ... \langle x_n^*, S_j, ... \rangle$, where $S_j = \{NB, NS, ZE, PS, PB\}$ – term-set of parameter x_n.

2. Determining the values of membership functions for the values of input variables x_i^*, $i = \overline{1,n}$.

3. Application of the algebraic approximation procedure in determining the parameters of the planned information security process in the form of production rules.

4. Application of the fuzzy identification method, which consists in the use of fuzzy logical equations obtained on the basis of linguistic rules tables and allowing to calculate the values of the membership functions of various solutions for fixed values of input variables, considering them known [12]:

– set of solutions $y = d_z$, $z = \overline{1,m}$;

– set of input variables $X^* = (x_1^*, x_2^*, ..., x_n^*)$ – ranges of variation of each input variable $x_i \in [\underline{x_i}, \overline{x_i}]$, $i = \overline{1,n}$;

– membership functions representing input variables, $\tilde{C}(\alpha) = \{\mu_{\tilde{C}(\alpha)}(x)/x\}$, $x \in X$, and output variable $\tilde{C}(d) = \{\mu_{\tilde{C}(d)}(y)/y\}$, in $y \in Y$ form of fuzzy sets;

– knowledge base presented in the form of logical statements (2).

Using operations $\cap$ and $\cup$, tables of linguistic rules are presented in the form:

$$\bigcup_{h=1}^{k_z} \left[\bigcap_{i=1}^{n} \left(x_i = \alpha_i^{(ih)} \right) \right] \rightarrow y = d_z, \quad z = \overline{1,m}.$$

Knowing the initial data, it is required to develop a decision-making algorithm that allows a fixed vector of input variables $X^* = (x_1^*, x_2^*, ..., x_n^*)$, $x_i^* \in [\underline{x_i}, \overline{x_i}]$ match the solution $y \in D = (d_1, d_2, ..., d_z)$, $z = \overline{1,m}$.

Obtaining fuzzy logical equations is as follows. Let's consider fuzzy variables $\alpha_i^{(jh)}$, $i = \overline{1,n}$, $j = \overline{1,m}$, $h = \overline{1,k_z}$ of linguistic variables x_i, $i = \overline{1,n}$, included in logical statements about decisions d_z, $z = \overline{1,m}$ (2). Let $\mu_{\tilde{C}(\alpha_i^{(jh)})}(x_i)$ – parameter membership function $x_i \in [\underline{x_i}, \overline{x_i}]$ of fuzzy variable α_i^{jh}, $i = \overline{1,n}$, $j = \overline{1,m}$, $h = \overline{1,k_z}$; $\mu_{\tilde{C}(d_z)}(x_i, x_2, ..., x_n)$ – membership function of the vector of input variables $X^* = (x_1^*, x_2^*, ..., x_n^*)$ to the value of the output variable $y = d_z$, $z = \overline{1,m}$. The relationship between these functions is determined by (2) and can be represented in the form of the following equations

$$\begin{aligned}
&\mu_{\tilde{C}(\alpha_{d_1})}(x_1, x_2, ..., x_n) = \\
&= \mu_{\tilde{C}(\alpha_1^{11})}(x_1) \wedge \mu_{\tilde{C}(\alpha_2^{11})}(x_2) \wedge ... \wedge \mu_{\tilde{C}(\alpha_n^{11})}(x_n) \vee \\
&\mu_{\tilde{C}(\alpha_1^{12})}(x_1) \wedge \mu_{\tilde{C}(\alpha_2^{12})}(x_2) \wedge ... \wedge \mu_{\tilde{C}(\alpha_2^{12})}(x_n) \vee ... \\
&... \vee \mu_{\tilde{C}(\alpha_1^{1k_1})}(x_1) \wedge \mu_{\tilde{C}(\alpha_2^{1k_1})}(x_2) \wedge ... \wedge \mu_{\tilde{C}(\alpha_n^{1k_1})}(x_n),
\end{aligned}$$

$$\begin{aligned}
&\mu_{\tilde{C}(\alpha_{d_2})}(x_1, x_2, ..., x_n) = \\
&= \mu_{\tilde{C}(\alpha_1^{21})}(x_1) \wedge \mu_{\tilde{C}(\alpha_2^{21})}(x_2) \wedge ... \wedge \mu_{\tilde{C}(\alpha_n^{21})}(x_n) \vee \\
&\mu_{\tilde{C}(\alpha_1^{22})}(x_1) \wedge \mu_{\tilde{C}(\alpha_2^{22})}(x_2) \wedge ... \wedge \mu_{\tilde{C}(\alpha_n^{22})}(x_n) \vee ... \\
&... \vee \mu_{\tilde{C}(\alpha_1^{2k_2})}(x_1) \wedge \mu_{\tilde{C}(\alpha_2^{2k_2})}(x_2) \wedge ... \wedge \mu_{\tilde{C}(\alpha_n^{2k_2})}(x_n), \qquad (8)
\end{aligned}$$

$$\begin{aligned}
&\mu_{\tilde{C}(\alpha_{d_m})}(x_1, x_2, ..., x_n) = \\
&= \mu_{\tilde{C}(\alpha_1^{m1})}(x_1) \wedge \mu_{\tilde{C}(\alpha_2^{m1})}(x_2) \wedge ... \wedge \mu_{\tilde{C}(\alpha_n^{m1})}(x_n) \vee \\
&\mu_{\tilde{C}(\alpha_1^{m2})}(x_1) \wedge \mu_{\tilde{C}(\alpha_2^{m2})}(x_2) \wedge ... \wedge \mu_{\tilde{C}(\alpha_n^{m2})}(x_n) \vee ... \\
&... \vee \mu_{\tilde{C}(\alpha_1^{mk_m})}(x_1) \wedge \mu_{\tilde{C}(\alpha_2^{mk_m})}(x_2) \wedge ... \wedge \mu_{\tilde{C}(\alpha_n^{mk_m})}(x_n).
\end{aligned}$$

So, making a recommendation d_z, $z=\overline{1,m}$, which corresponds to a vector of fixed values of input variables $X^*=\left(x_1^*,x_2^*,...,x_n^*\right)$, $x_i^*\in\left[\underline{x_i},\ \overline{x_i}\right]$, carried out in the following sequence [6]:

1. Parameters that influence the determination of parameters for the planned identification of an information leakage channel based on predicted values are determined and analyzed.

2. The vector of values of input variables is fixed $X^*=\left(x_1^*,x_2^*,...,x_n^*\right)$ and the values $\mu_{\tilde{C}(\alpha)}(x)$ are determined for the input variables x_i^*, $i=\overline{1,n}$.

3. Using logical equations (8), multidimensional membership functions $\mu_{\tilde{C}(\alpha_{d_z})}\left(x_1^*,x_2^*,...,x_n^*\right)$ of X^* vector are determined for all values d_z, $z=\overline{1,m}$ of output variable y.

Thus, according to the fuzzy identification method, for a given vector of fixed states of input variables $X^*=\left(x_1^*,x_2^*,...,x_n^*\right)$ and the knowledge base it is possible to find discrete values (d_1, d_2, ..., d_m). By applying fuzzy logical inference to the resulting set of production rules, let's obtain a recommendation on the use of appropriate information security parameters.

Methods for formalizing and processing knowledge in DSS provide:

– presentation and processing of ambiguous, incomplete, contradictory data and knowledge;

– processing of a production rules set for determining appropriate strategies for the planned information security process, formed as a result of solving a multicriteria optimization problem in a fuzzy formulation;

– determining the sequence of production rules that most fully influence the process of determining an appropriate strategy for the planned information security process;

– determining the membership function of fuzzy variables for a linguistic variable for which it is inappropriate to use the algebraic approximation procedure in order to reduce the number of its production rules to be determined;

– adaptability of recommendations to changes in the information situation and industrial espionage activities.

To test the functionality of the synthesized model of an automated decision-making system when managing information security channels, according to Tab. 1 and formula (8), the dependence of the gain in time when searching for and eliminating information leakage channels was calculated (Fig. 4) for different numbers of information channels *N*.

The average time to search for information leakage channels was determined according to the formula:

$$t_{\Pi}=\sum_{i=1}^{N}P_i\times\overline{t_{1_i}},$$

where P_i – probability of information leakage in the i-th information channel; $\overline{t_{1_i}}$ – average time to search for information leaks on the i-th information channel.

The time gain when searching for and eliminating information leakage channels was calculated as follows:

$$\mu=\frac{\overline{t_p}}{\overline{t_0}},$$

where $\overline{t_0}$ – average search time taking into account preliminary data on information channels and the enemy's interest in obtaining information; $\overline{t_p}$ – average search time for the real (existing) structure of an information leak detection system.

The calculation of the synthesized model of an automated decision-making system for managing information security channels according to the introduced fuzzy linguistic variables was carried out. Analysis of the resulting diagram (Fig. 4) shows that the time gain in searching and eliminating information leakage channels when using the proposed automated system can be from 10 % to 45 %. The amount of gain varies depending on the number of information channels.

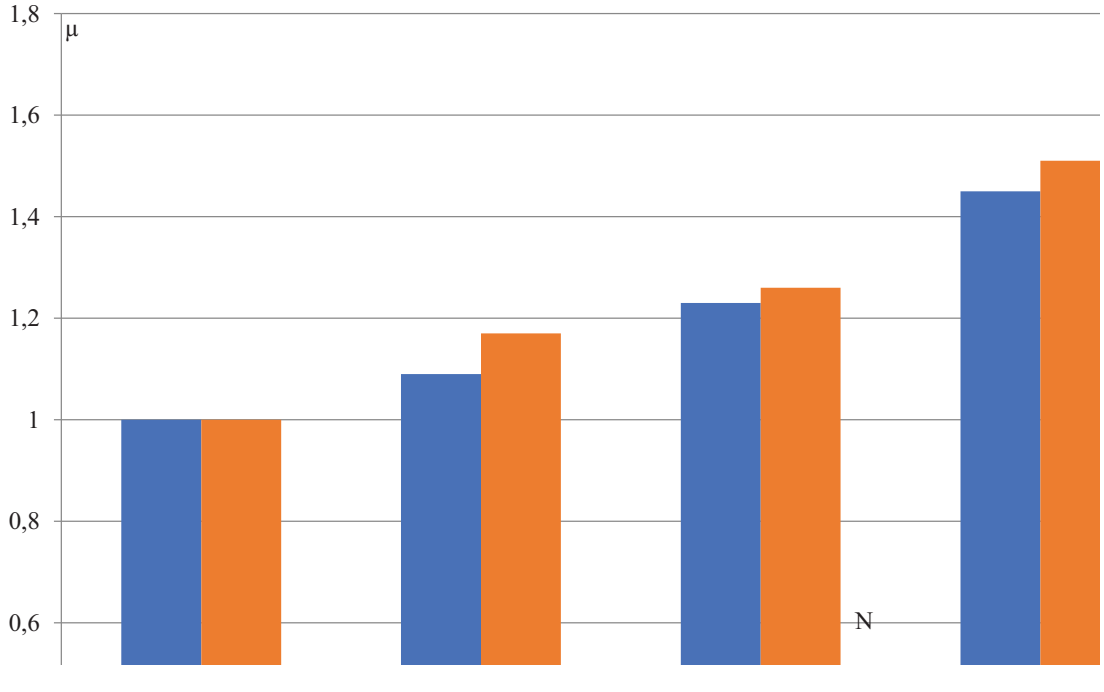

Fig. 4. Dependence of time gain on searching and eliminating information leakage channels

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

The advantage of this study is the development of a unified approach to describing the properties of the considered area of information protection from unauthorized access based on the use of procedures for the logical and analytical activities of decision makers when managing information security channels.

The developed logical-linguistic hierarchical production model for determining information security parameters (Fig. 3) made it possible to obtain connection equations for fuzzy logical equations. At the same time, the linguistic rules of a weakly formalized decision-making process when managing information security channels were also defined (Table 1). To evaluate the developed method, the dependence of the gain over time when searching for and eliminating information leakage channels (Fig. 4) was calculated for a different number of information channels *N*. This dependence is based on the data in Tab. 1 and generalizing formula (8).

The obtained results of applying the developed method make it possible to increase the efficiency of searching and eliminating information leakage channels when using the proposed automated system in comparison with the known ones, for example, [2]. So, in Fig. 4 diagrams of time indicators for searching for information leakage channels for known systems (orange) were obtained based on modeling the security systems of critical infrastructure facilities [2].

The proposed method can be used in further research in the field of information security, for example in the continuation of [13]. The study [13] proposed a scheme for intelligent operational authentication of information leakage channels, which requires knowledge of reliable (legitimate) nodes of information channels. The proposed method allows to obtain such preliminary data, which will further reduce the time for identifying possible channels of information leakage.

The study developed a structural diagram of information exchange when managing information security channels. This scheme made it possible to substantiate that the area of possible information attacks is a difficult logical and analytical problem to solve. Therefore, a logical-linguistic hierarchical production model for determining information security parameters has been proposed. For a hierarchically organized structure based on classification characteristics, a hierarchy tree is proposed. This tree displays the relationships between partially ordered sets. The proposed logical-linguistic model makes it possible to determine the influences for blocking information leakage channels in an automated mode (control).

A developed method for formalizing knowledge to determine appropriate strategies for the planned information security process. The proposed method suggests considering not subsets of variables involved in specific rules, but the set of all variables, both in the premise and in the conclusion of the rule. Then the mapping of possible actions is represented as corresponding linguistic rules.

The proposed results in the field of information security make it possible to avoid the assumptions made in classical decision-making theory about the process as a choice of one of many alternatives. The presented method of formalizing knowledge to determine appropriate strategies for the planned information protection process allows to establish the most preferable data protection parameters. These parameters influence the determination of appropriate strategies for the planned information security process. Elements of the resulting set of knowledge are ordered by levels of non-dominance from the point of view of the greatest influence on conclusions about channels of possible information leakage in the information field.

The limitations of the study can be considered the calculation of the probability of an information leak in the *i*-th information channel when calculating the average time to search for information leak channels (for constructing the dependence, Fig. 4). In the study, values for this probability were calculated according to the algorithm presented in [8].

When conducting research, the parameters of the synthesized system are presented in the form of a set of mappings of fuzzy linguistic variables. The disadvantage of the work is the presentation of the main parameters of the universal decision-making system when managing information security channels. In the practical development of a decision-making system when managing information security channels for a specific enterprise (organization), it is necessary to take into account additional parameters. At the same time, in addition to the main parameters proposed in the study, it is necessary to justify specific (additional) ones that are characteristic only of the specific decision-making system being synthesized.

The development of this research consists in substantiating a multicriteria optimization problem in a fuzzy formulation when managing information security channels. Solving this problem will make it possible to determine a rational strategy for the planned information security process using an automated decision-making system.

7. Conclusions

1. A structural diagram of information exchange in managing information security channels has been developed. This block diagram allows to schematically represent the order of tasks to be solved in a synthesized automated decision-making system when managing information security channels to formalize decision-making tasks. A feature of the proposed structural diagram is that it takes into account both intellectual and technical results of decision-making when managing information security channels. The implementation of the proposed scheme allows to take into account the influence of the decision maker (a priori data) and the characteristics of technical means of monitoring information transmission channels (a posteriori data).

2. A comparative assessment of strategies for the planned information security process involves solving a multicriteria optimization problem. The logical-linguistic production hierarchical model is justified as a mathematical model for determining protection parameters. The main form of recording in it is interconnected tables of linguistic rules, which are a display connecting the previous, current and future states of the described process.

3. The process of determining information security parameters directly in the logical-linguistic hierarchical production model is difficult to trace. Therefore, this process is described using an algebraic model that is closest to a linguistic description. If it is inappropriate to synthesize products in order to reduce the number of production rules, it is proposed to use the fuzzy identification method. The

method of formalizing knowledge to determine appropriate strategies for the planned information security process has been improved. It differs from the known ones in the formation of a set of production rules taking into account parameters that, when developing recommendations under conditions of non-stochastic uncertainty, describe a fuzzy environment. The method of processing knowledge to determine appropriate strategies for the planned information security process has also been improved. It differs from the known ones in the processing of knowledge based on the developed procedure for their algebraic approximation and fuzzy identification.

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 affect 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. Petrunia, Yu. Ye., Litovchenko, B. V., Pasichnyk, T. O. et al.; Petrunia, Yu. Ye. (Ed.) (2020). Pryiniattia upravlinskykh rishen. Dnipro: Universytet mytnoi spravy ta finansiv, 276. Available at: http://biblio.umsf.dp.ua/jspui/bitstream/123456789/4070/1/Прийняття%20упр%20рішень%202020.pdf
2. 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. doi: https://doi.org/10.15587/978-617-7319-57-2
3. Butko, M. P., Butko, I. M., Mashchenko, V. P. et al.; Butko, M. P. (Ed.) (2015). Teoriya pryiniattia rishen. Kyiv: «Tsentr uchbovoi literatury», 360. Available at: https://duikt.edu.ua/uploads/l_101_88535923.pdf
4. Sokolov, A. Y. (1999). Algebraic approach on fuzzy control. IFAC Proceedings Volumes, 32 (2), 5386–5391. doi: https://doi.org/10.1016/s1474-6670(17)56917-7
5. Yevseiev, S., Herasymov, S., Kuznietsov, O., Opirskyy, I., Volkov, A., Peleshok, Y. et al. (2023). Method of assessment of frequency resolution for aircraft. Eastern-European Journal of Enterprise Technologies, 2 (9 (122)), 34–45. doi: https://doi.org/10.15587/1729-4061.2023.277898
6. Bidiuk, P. I., Tymoshchuk, O. L., Kovalenko, A. Ye., Korshevniuk, L. O. (2022). Systemy i metody pidtrymky pryiniattia rishen. Kyiv: KPI, 610. Available at: https://ela.kpi.ua/bitstream/123456789/48418/1/Systemy_i_metody_pidtrymky_pryiniattia_rishen.pdf
7. 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. doi: https://doi.org/10.15587/1729-4061.2021.229221
8. 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. doi: https://doi.org/10.15587/978-617-7319-31-2
9. Komeylian, S., Paolini, C., Sarkar, M. (2023). Beamforming Technique for Improving Physical Layer Security in an MIMO-OFDM Wireless Channel. Advances in Distributed Computing and Machine Learning, 127–134. doi: https://doi.org/10.1007/978-981-99-1203-2_11
10. Li, Z., Lin, Q., Wu, Y.-C., Ng, D. W. K., Nallanathan, A. (2023). Enhancing Physical Layer Security with RIS under Multi-Antenna Eavesdroppers and Spatially Correlated Channel Uncertainties. IEEE Transactions on Communications, 1–1. doi: https://doi.org/10.1109/tcomm.2023.3333919
11. Qu, K., Wang, Z., Li, Z., Li, Z. (2023). Vectorial Manipulating Encryption for Multi Channel Capacity and Security Enhancement. Laser & Photonics Reviews, 17 (10). doi: https://doi.org/10.1002/lpor.202300105
12. Mizuno, T., Nishikawa, H., Kong, X., Tomiyama, H. (2023). Empirical analysis of power side-channel leakage of high-level synthesis designed AES circuits. International Journal of Reconfigurable and Embedded Systems (IJRES), 12 (3), 305. doi: https://doi.org/10.11591/ijres.v12.i3.pp305-319
13. Qiu, X., Yu, J., Zhuang, W., Li, G., Sun, X. (2023). Channel Prediction-Based Security Authentication for Artificial Intelligence of Things. Sensors, 23 (15), 6711. doi: https://doi.org/10.3390/s23156711
14. Culbreth, S., Graham, S. (2023). Demonstrating Redundancy Advantages of a Three-Channel Communication Protocol. International Conference on Cyber Warfare and Security, 18 (1), 513–522. doi: https://doi.org/10.34190/iccws.18.1.964
15. 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. doi: https://doi.org/10.1007/s11036-023-02149-z

16. Masure, L., Cassiers, G., Hendrickx, J., Standaert, F.-X. (2023). Information Bounds and Convergence Rates for Side-Channel Security Evaluators. IACR Transactions on Cryptographic Hardware and Embedded Systems, 522–569. doi: https://doi.org/10.46586/tches.v2023.i3.522-569
17. Masure, L., Standaert, F.-X. (2023). Prouff and Rivain's Formal Security Proof of Masking, Revisited. Lecture Notes in Computer Science, 343–376. doi: https://doi.org/10.1007/978-3-031-38548-3_12
18. Díaz, Á., Kaschel, H. (2023). Scalable Electronic Health Record Management System Using a Dual-Channel Blockchain Hyperledger Fabric. Systems, 11 (7), 346. doi: https://doi.org/10.3390/systems11070346
19. Wichelmann, J., Peredy, C., Sieck, F., P tschke, A., Eisenbarth, T. (2023). MAMBO–V: Dynamic Side-Channel Leakage Analysis on RISC–V. Lecture Notes in Computer Science, 3–23. doi: https://doi.org/10.1007/978-3-031-35504-2_1
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. doi: 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. doi: https://doi.org/10.1111/poms.14015
22. Grant, D. G., Behrends, J., Basl, J. (2023). What we owe to decision-subjects: beyond transparency and explanation in automated decision-making. Philosophical Studies. doi: https://doi.org/10.1007/s11098-023-02013-6