https://doi.org/10.33271/nvngu/2025-1/096

S. Onyshchenko,
orcid.org/0000-0002-6173-4361,
A. Hlushko,
orcid.org/0000-0002-4086-1513,
O. Laktionov[*]**,**
orcid.org/0000-0002-5230-524X,
S. Bilko,
orcid.org/0000-0003-0259-4482

National University "Yuri Kondratyuk Poltava Polytechnic",
Poltava, Ukraine
[*] Corresponding author e-mail: itm.olaktionov@nupp.edu.ua

TECHNOLOGY FOR DETERMINING WEIGHT COEFFICIENTS OF COMPONENTS OF INFORMATION SECURITY

Purpose. Development of a technology for determining weighting coefficients based on an improved methodology to ensure the accuracy of determining the level of information security, taking into account its components.

Methodology. The process of creating and conducting an experiment on the technology for determining weight coefficients of components of information security at the macro level is studied. The proposed technology utilizes two comprehensive assessments that consolidate information into a single score. One comprehensive indicator is based on considering the human factor, while the other excludes the human factor through the use of artificial intelligence. Arrays of resulting assessments are used to determine the level of information security, which allows improving the efficiency of the information security diagnostic process.

Findings. The proposed technology, by utilizing a comprehensive indicator, demonstrates more effective diagnostic results, as determined by the standard deviation criterion. The integrated indicator that considers the human factor demonstrates a standard deviation value of 0.0195, while the comprehensive indicator without considering the human factor shows a value of 0.0047.

Originality. The proposed technology differs from the existing ones by employing a comprehensive indicator that takes into account a six-digit interaction of integrated indicators, with weight coefficients determined using artificial intelligence tools.

Practical value. The developed approach provides a more accurate result of integral assessment of the level of information security. This will allow the development of effective state instruments to enhance the level of information security, considering its current value, and to justify strategic directions for strengthening the state's information security.

Keywords: *linear model, integrated indicator, artificial intelligence, information security*

Introduction. In recent decades, the issue of ensuring the security of information, information flows, and the information environment as a whole has become a priority at both national and international levels. The virtualization of the global economy, the shift to a digital format, and the increasing volume of data circulating in cyberspace have given rise to new challenges and threats. Cybercrime, hacking attacks, data theft, and misinformation have become serious issues that can significantly impact the security of nations, companies, and individuals, disrupt government administration and economic systems, and cause other dangers [1]. Therefore, information security is an integral part of national security, as it aims to protect national interests from potential and real threats in the information space. This includes minimizing risks associated with the spread of false and incomplete information, unauthorized access to data, and their unauthorized use. Effective information security management is key to ensuring the integrity, confidentiality, and availability of information resources, which is essential for maintaining national stability and protecting against information threats.

The heightened impact of internal and external destabilizing factors on national security due to the military aggression of the Russian Federation has underscored the need to ensure Ukraine's information security [2, 3]. Given the instability and aggressive nature of the information space, there is a need to develop effective regulatory measures and tools to strengthen the country's information security. In particular, it is crucial to create economic and mathematical models that enable comprehensive assessment, analysis, and forecasting of the level of information security. This task requires the development of scientifically grounded approaches and methods capable of effectively addressing the outlined problems in the context of the modern information environment.

Due to the diversity of approaches, the complexity and dynamism of the information environment, and the varying nature of threats to the information security of economic entities, a unified methodology for evaluating information security does not currently exist. Each methodology has its advantages and disadvantages, and their effectiveness can vary depending on specific conditions and evaluation objectives. A common feature of most approaches is that they are based on an integral evaluation method. However, the issue of determining the weights of the indicators introduced into the model (coefficients) remains a topic of debate.

On the one hand, weighting coefficients are determined by expert methods. On the other, to avoid the influence of the human factor, approaches based on the imbalance or difference between expert assessments and regulatory assessments are used [4]. However, these solutions are not universal and require time to configure the relevant models, where time is used as a criterion of accuracy. Consequently, there is a need to improve the process of determining the weighting coefficients for the components of information security.

Literature review. According to previous research by the authors, the developed methodology for integrated assessment of information security at the macro level is based on a set of indices that include indicators reflecting various aspects of information security, namely the E-Government Development Index (EGDI), Global Cybersecurity Index (GCI), Global Innovation Index (GII), National Cyber Security Index (NCSI), Social Progress Index (SPI), Press Freedom Index (PFI), and World Digital Competitiveness Rankings (WDCR) [5, 6]. These indices allow for a comprehensive assessment of a country's information security status, taking into account a wide range of factors influencing its level.

According to the general scientific concept of stability, to enhance the reliability and accuracy of results obtained, different methods should be used to process identical data. Utilizing multiple approaches allows consideration of various aspects of analysis, contributing to a deeper understanding of the phenomena under study and minimizing the risk of errors due to the specificities of individual methods. There is every reason to believe that these conclusions reflect reality. However, conclusions may vary depending on the data processing method, subject to the researcher's subjective influence in selecting the initial data analysis method. Various methods are employed to aggregate partial indicators into an integrated one: the taxonomic method, calculation of the multidimensional mean, and fuzzy set theory. In economic research, the taxonomic method is most commonly used. Its main advantage lies in its ability to handle multidimensional economic objects characterized by a sufficiently wide range of indicators [7]. This method involves the use of weighting coefficients, which are determined in various ways.

Determining the significance of indicators in economic models essentially serves as a prototype for artificial intelligence models, where the ultimate goal is to forecast a numerical value. Currently, several approaches are known for developing new tactics for determining weighting coefficients, which are fundamental to creating a model and, based on it, a corresponding technology. For instance, in study [8], a partially linear functional-coefficient model is used, allowing for adjustments to the impact of environmental regulation depending on economic development. The practical outcome of using the model is a 40 % reduction in city pollution without affecting economic indicators. While the results are impressive, the issue of optimal determination of weighting coefficients was not explored within the study, limiting the solution. The search for weighting coefficients was investigated in study [9], which addresses the problem of assessing economic activities in organized industrial zones. The primary tool used in this research is aggregation operators, which involve the use of weighting coefficients, although it remains unclear whether these coefficients are used to address the problem of developing information security diagnostics tools.

The use of weighting coefficients forms the basis of existing research methods, particularly the principal component method, studied as an aggregate indicator in study [10]. As noted by the authors [10], weighting coefficients enable an examination of each factor's influence on the variable. In study [11], the ideas from [10] were expanded, proposing a method of dynamic weighting coefficient adjustment based on fuzzy control. The value of this approach lies in adjusting the coefficient depending on the conditions of the object under study. This coefficient affects the elasticity of the object, as demonstrated in study [12].

In addition to the approaches discussed in studies [11, 12], other methods for investigating weighting coefficients exist. For example, in the work presented in [13], an exponential curve function measurement method is proposed. The authors describe this as an innovative solution. However, these studies addressed entirely different tasks and did not consider the development of a corresponding technology or a method for determining the reliability of weighting coefficients.

The reliability of determining weighting coefficients is established as the deviation of the obtained weighting coefficients from the estimated comparative priorities of criteria [14]. The reliability indicator of weighting coefficients can also be assessed using statistical methods. Additionally, existing artificial intelligence methods operate based on weighting coefficients selected according to input data. In essence, the updating of weighting coefficients is a core principle of artificial intelligence [15]. This concept was also explored in [16], where weighting coefficients were used as one of the components of a heuristic algorithm for determining medians using the Hamming metric.

The fuzzy neural network method, formed by combining fuzzy comprehensive evaluation with neural network technology [17], also involved the use of weighting coefficients that did not require determining their influence on parameter interaction.

The ideas from [17] are further developed in [18], where a risk assessment method is proposed that includes weighting coefficients, with the final assessment presented as a fuzzy evaluation. The determination of weighting coefficients is carried out using artificial intelligence. Another known method for determining weighting coefficients is based on factor analysis parameters [19].

Particular emphasis on determining weighting coefficients is highlighted in reinforcement methods [20]. These methods represent optimization tasks where the objective function includes a mechanism for rapid sample re-weighting. This allows for the optimal selection of weighting coefficients that impact the final result of the function.

In [21], weighting coefficients are determined to solve Hardy-Hilbert type inequality problems. The study text provides an in-depth look at the procedure for creating a mathematical model and the results obtained. The proposed solutions can be practically used for creating artificial intelligence models.

In addition to determining weighting coefficients, [22] addresses the normalization of variables depending on the values of the input data. However, the model's adequacy was tested on data outside the information security field, specifically in logistics. Thus, [23] expands on the ideas in [22], studying a partially linear model with high-dimensional variable coefficients. The advantages of this solution include the simultaneous use of non-parametric and parametric models combined with regularization techniques, allowing for the creation of a hybrid model whose study is currently promising.

The limitations of the models include the inability to represent all types of project activities, which is addressed in [24]. The proposed solution can be practically used for enterprise activity planning, with partial examination of its application in the security domain.

An increasing number of studies focus on improving or creating new linear models. Unlike [23, 25] proposes a model where variables are selected with a penalty for various effects. The model's advantages include scaling different evaluation metrics. However, the use of these models to study economic security has not been thoroughly explored.

Modern developments are increasingly using algorithm-based research technologies, while [26] offers theoretical research results on improving the Fisher criterion using neural networks. The uniqueness of [26] lies in the heteroscedasticity of conditional class distributions to differentiate one class from another. Similar advancements in refining regression models were studied in [27].

In [28], attention is focused on interpreting the research results using regression analysis tools, particularly multiple regression. The authors highlight the importance of following the model creation algorithm, including the use of cross-validation methods that impact the weighting coefficients. Unlike [28], the authors of [29] combine tools of supervised and unsupervised learning and regularization when creating the model. Regularization enables more efficient research solutions. Using regularization tools allows for an influence on the outcome of the studied model. It is essential to choose the optimal regularization method, as done in [29].

Unsolved aspects of the problem. The work of authors [8–29] shares one common fact: no one has fully explored the issue of developing technology based on an improved methodology for determining the weighting coefficients of information security components. This is the main drawback of existing approaches, where solutions were pre-programmed rather than learning from their own errors through artificial intelligence tools.

Purpose. The aim of this work is to develop a technology based on an improved methodology for determining the weighting coefficients of information security components.

Achieving this goal requires addressing the following tasks.

1. To develop a technology based on an improved methodology for determining the weighting coefficients of information security components.

2. To implement the software and conduct experimental verification of the proposed technology.

3. To provide practical recommendations for creating relevant technologies.

Description of the research methodology for determining the weighting coefficients of information security components. The foundation for studying information security is Ukraine's position in international rankings, which are consolidated into an integral assessment. It is important to note that when forming the integral indicator, a matrix of observations is utilized, created based on the values of the corresponding indicators reflecting various components of information security. During the formation of the feature space (set of indicators), it is crucial to ensure the information alignment of the indicators. To achieve this, the indicators are divided into stimulators and destimulators. It should be emphasized that the relationship between the integral coefficient and the stimulating indicators is direct, while the relationship between the integral coefficient and the destimulating indicators is inverse, as defined by the technique. In fact, the characteristics of the underlying database are one of the prerequisites for creating an integrated indicator. The experimental sample of weight coefficients is determined through expert evaluation, which involved a group of experts (10 candidates of sciences and 10 doctors of sciences) and artificial intelligence methods.

The process of creating the integrated indicator involved determining the scale and levels for diagnosing the respective research objects. Trapezoidal membership functions are commonly used functions in fuzzy set theory. The analytical representation of these functions provides simplicity and convenience when performing operations on fuzzy sets. In describing the subsets of values for the linguistic variable "level of indicator," a system of five trapezoidal-shaped membership functions is employed, known as the standard five-level 01-classifier. Using these concepts, differentiation of economic indicators was conducted.

In assessing the level of information security, fuzzy set theory is employed. Fuzzy descriptions are used when it is challenging to clearly define the concepts of "high" or "maximum" levels of indicators, or when it is necessary to distinguish between "medium" and "low" levels. In such situations, a membership function is utilized to determine the degree of membership of these indicators in specific categories. Since the studied variables have different scales, normalization of the scales is applied. The standardization (normalization) process of the initial data involves adjusting their statistical characteristics, particularly aligning variances so that all variances become equal to 1. Additionally, normalization of the feature values is carried out, which entails bringing the mean value of the features to zero. The essence of the normalization method for input indicators lies in bringing them to a unified measurement scale, where the best value of the indicator equals one and the worst equals zero. This approach ensures comparability and adequacy in evaluating indicators within a specified scale.

In the first stage of the research, regression analysis tools were used, where the model's weight coefficients were determined through expert evaluation. Tools for calculating the concordance coefficient were also employed. By calculating the concordance coefficient, the hypothesis of agreement among specialists and the reliability of the results from the expert group survey is confirmed. The value of the concordance coefficient ranges from [0, 1]. When the coefficient equals 0, it indicates a lack of consensus among the experts. Conversely, if the coefficient equals 1, it signifies the highest level of agreement in the experts' evaluations.

The second stage of the research involved the development of artificial intelligence tools for determining the magnitude of weight coefficients. Constraints included that the sum of the weight coefficients must equal 1.0, and negative values were not permissible. The subtasks of the second stage of the research were:

1. To create a model that combines a set of integrated assessments into a single comprehensive evaluation, taking into account the principles of interaction and emergence.

2. To select a neural network architecture for finding weight coefficients, where n integrated indicator values are input, and the output is the predicted value of the weight coefficient. The architecture of the neural network consists of input and output layers, with no hidden layer; it is therefore a single-layer network with one input neuron. The mean squared error was used as the loss function for the neural network, along with the Adam optimizer, and the training was conducted over 200 epochs. The software implementation of the proposed solutions was carried out using the Python programming language and the TensorFlow library.

The development of the model for combining integrated indicators was conducted with consideration of the principles of interaction and emergence, where the optimal model was selected based on the condition of minimizing the standard deviation. For this purpose, combinatorial tools were employed, specifically the combination method, defined by the well-known formula

$$C = n!/k!(n-k)!,$$

where n is the total number of elements (for the specified study, 7); k – the number of elements in the combination (for the specified study, 6).

For the comparative analysis of composite indicators, standard deviation was used.

Presentation of the main material and the scientific results obtained. The taxonomy method is applied for integrating data from several heterogeneous parameters that characterize the level of information security over various time intervals. This method allows for the integration of these data into a single indicator that reflects the overall level of information security. The calculation of the integral indicator is performed by generalizing and normalizing individual indicators, enabling a comprehensive assessment of the level of information security (Fig. 1).

The specified scheme is used to determine the integral indicator of information security at the macro level and constitutes one of the blocks of the corresponding technology, specifically Block 1 to Block 10.

Block 1. The method for determining the integral indicator of information security is selected, taking into account the human factor or excluding it. If an integral indicator that considers the human factor is chosen, the process proceeds to Block 2.

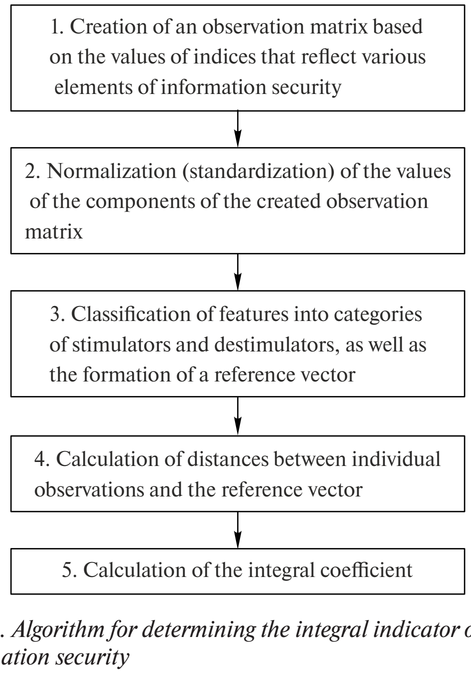
1. Creation of an observation matrix based on the values of indices that reflect various elements of information security
2. Normalization (standardization) of the values of the components of the created observation matrix
3. Classification of features into categories of stimulators and destimulators, as well as the formation of a reference vector
4. Calculation of distances between individual observations and the reference vector
5. Calculation of the integral coefficient

Fig. 1. Algorithm for determining the integral indicator of information security

Block 2. Qualitative indicators are transformed into quantitative ones. In economic research, normalization refers to the transition from absolute values of indicators to normalized (standardized) values, which range from 0 to 1.

Block 3. The weighting coefficients are determined using expert assessment methods.

Subblock 3.1. The sum of assessments is calculated for each row ($\sum S_i$ – the sum of each expert's assessments) and for each column ($\sum S_j$ – the sum of the experts' assessments for each indicator). In this case $\sum S_i = \sum S_j$.

Subblock 3.2. The significance of each indicator (weight coefficient) will be determined according to the formula

$$b_i = \overline{S_i} \Big/ \sum \overline{S_i},$$

where $\overline{S_i}$ is the average value of the assessment for the i^{th} indicator; $\sum \overline{S_i}$ – the sum of the average ratings from the engaged experts for the indicators.

These normalized values reflect the degree of proximity to the optimal value and can be interpreted as percentages: 0 corresponds to 0 %, and 1 corresponds to 100 %. This allows for the comparison of different indicators on a common scale and assesses their performance in the context of achieving optimal values.

Subblock 3.3. To determine the overall weight of each indicator, the arithmetic mean of the scores obtained for each factor should be calculated. This calculation is carried out according to the formula

$$\overline{S} = \sum S_i \big/ j,$$

where *j* is the number of experts involved.

Subblock 3.4. The calculation of the deviations from the mean $S_i - \overline{S}$ and their squares $(S_i - \overline{S})^2$ is carried out.

Subblock 3.5. To assess the degree of agreement among the evaluations provided by the experts, the concordance coefficient is calculated using the following formula

$$W = 12\sum (S_i - \overline{S})^2 \Big/ j^2 (i^3 - i),$$

where *i* is the number of indicators entered into the model.

Block 4. The calculation of the integral coefficient of information security is performed using the weighted sum method according to the established formula

$$I = \sum b_i \cdot i_{mn(nom)},$$

where b_i is weight coefficients of the components of information security; $i_{mn(nom)}$ – normalized indicators of the components of information security.

In this case $0 \le b_i \le 1$, a sum b_i is equal to 1. The integrated indicators and the comprehensive indicator determined based on them were recorded in Table 1.

Block 5. A classification of the level of information security is carried out, which falls within one of five intervals (Fig. 2).

Block 6. If the results of the integral coefficient of information security calculation do not satisfy the decision-maker, a transition to Block 3 is initiated; otherwise, a transition to Block 7 occurs. If the integral indicator is selected without considering the human factor, the transition to Block 7 is made.

Table 1

The initial integrated indicators used for combining into a single assessment

The studied indicator	Year 1	…	Year *n*
The studied indicator 1	x_{11}	…	x_{1n}
…	…	…	…
The studied indicator *n*	x_{m1}	…	x_{mn}
Complex indicator	I_1	…	I_n
Standard deviation of complex indicators			

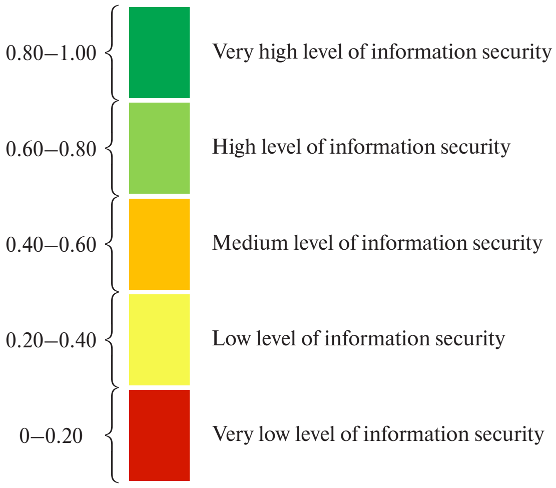
0.80–1.00
Very high level of information security
0.60–0.80
High level of information security
0.40–0.60
Medium level of information security
0.20–0.40
Low level of information security
0–0.20
Very low level of information security

Fig. 2. Typical scale for assessing the level of information security

The development of a model that integrates the array of integrated assessments into a single composite assessment, considering the principles of interaction and emergence, involved the use of a set of evaluations belonging to the range $[x_1, x_7]$, where combinations of evaluations across six elements are defined. The identified combinations of assessments are presented as a set of six elements $\{x_1, x_2, x_3, x_4, x_5, x_6\}$, $\{x_1, x_2, x_3, x_4, x_5, x_7\}$, $\{x_1, x_2, x_3, x_4, x_6, x_7\}$, $\{x_1, x_2, x_3, x_5, x_6, x_7\}$, $\{x_1, x_2, x_4, x_5, x_6, x_7\}$, $\{x_1, x_3, x_4, x_5, x_6, x_7\}$, $\{x_2, x_3, x_4, x_5, x_6, x_7\}$.

Block 7. The determination of weight coefficients is carried out using artificial intelligence methods according to the research methodology.

Block 8. The comprehensive indicator is calculated using the formula

$$CP = \sum_{i=1}^{7} (k_i \cdot \prod\nolimits_{j \neq i} x_j),$$

where k_i is the weight coefficient; $P_{j \neq i}$ – the product of all values of *j*, except for *i*.

Block 9. If the results of the comprehensive indicator evaluation do not satisfy the decision-maker, a transition is made to Block 7; otherwise, a transition is made to Block 10.

Block 10. The final decision is made regarding the results of the determined integrated information security coefficients.

Let us consider the pseudocode for determining the proposed comprehensive indicator.

```
# Initialization of variables
factors = [x1, x2, x3, x4, x5, x6, x7]
   weight_coefficients = [weight_coefficient_1,
   weight_coefficient_2, weight_coefficient_3,
   weight_coefficient_4, weight_coefficient_5,
   weight_coefficient_6, weight_coefficient_7]
# Index combinations for each component
index_combinations = [
          [0, 1, 2, 3, 4, 5],
          [0, 1, 2, 3, 4, 6],
          [0, 1, 2, 3, 5, 6],
          [0, 1, 2, 4, 5, 6],
          [0, 1, 3, 4, 5, 6],
          [0, 2, 3, 4, 5, 6],
          [1, 2, 3, 4, 5, 6]
]
# Calculation of the complex indicator
complex_indicator = 0
# Cycle for calculating components
for i from 0 to length weight_coefficients:
component= 1
for index in index_combination [i]:
```

```
component = component * factors [індекс]
component = component * weights_factors [i]
complex_indicator = complex_indicator + component
# Outputting the result
output complex_index
```

According to the results of expert assessments, the weight coefficients for the components of information security included in the model were distributed as follows. The highest weight coefficients (0.20) were assigned to the National Cyber Security Index (NCSI) and the Global Cybersecurity Index (GCI), indicating their critical importance for evaluating information security. The NCSI reflects the level of national cybersecurity, taking into account the legal, technical, and organizational aspects of countering cyber threats, while the GCI assesses cybersecurity at the global level, considering international standards. The World Digital Competitiveness Rankings (WDCR) and the E-Government Development Index (EGDI) were assigned a weight coefficient of 0.15, emphasizing their role in determining a country's ability to utilize digital technologies for economic development and the effectiveness of e-government implementation, which also impacts the overall level of information security. The Global Innovation Index (GII), Social Progress Index (SPI), and Press Freedom Index (PFI) received a weight coefficient of 0.10. Although their influence on the overall assessment of information security is smaller, they remain significant for evaluating innovative development, social progress, and the level of press freedom, which are essential aspects of a comprehensive assessment of information security. This distribution of weight coefficients allows for the consideration of various aspects of information security, creating a multifactorial model that reflects the complexity and multidimensionality of this phenomenon.

Taking into account the weight coefficients of the information security components, the calculation of the integrated indicator has been conducted. The results are presented in Fig. 3.

As can be seen, the integrated indicator has been determined based on data from the years 2013 to 2023. Until 2023, the integrated indicator ranged from 0.53 to 0.60, indicating a moderate level of information security in Ukraine (Fig. 2). In 2023, the integrated information security indicator increased to 0.62, attributed to positive trends in Ukraine's standings in the Press Freedom Index and the National Cyber Security Index. This growth is linked to significant advancements in Ukraine's cybersecurity domain, particularly in military cybersecurity and the fight against cybercrime. Improvements in these areas include enhancements in information system protection technologies, strengthening national cybersecurity measures, and actively combating cybercrime. Ukraine has expanded its cooperation with EU countries, NATO, and private companies specializing in cybersecurity, allowing for the adoption of advanced technologies to enhance its cyber defense capabilities. The implementation of modern monitoring and detection systems for cyber threats based on artificial intelligence and machine learning has improved the security of information systems. Conducting joint operations with international partners, such as Interpol and Europol, has enabled the identification and neutralization of cybercriminal groups operating within and beyond Ukraine's borders. These achievements have positively influenced the overall level of information security in the country.

The density of the integrated indicators on the coordinate plane is characterized by a standard deviation of 0.0195. For a comparative analysis of the obtained result with another comprehensive indicator, its calculation has been performed.

According to the research methodology, a neural network has been constructed, where 11 assessments of integrated indicators were inputted, and a single value of weight coefficients was produced at the output, representing 0.0096; 0.0134; 0.0073; 0.0131; 0.0099; 0.0156; 0.0101; 0.0155; 0.0229; 0.00000015467; 0.00000021. The objectivity of the obtained result is confirmed by the learning curve (Fig. 4).

As seen from the learning curves (mean squared error of training), the MSE decreases from 1.0 to 0.3 as the number of epochs increases from 1 to 75. From epochs 75 to 200, the MSE drops to less than 0.01, which meets the expectations of the study.

When using a smaller number of epochs, specifically 150 or 100, the desired accuracy results based on the MSE criterion and others are not achieved. This result confirms the adequacy of the developed model, which can be used for determining the coefficients.

The results of the defined integral indicators of information security based on the proposed approach are presented in Table 2.

The difference in standard deviation, as shown in Table 2, indicates the superiority of the proposed approach over the one represented in Fig. 3. Thus, based on the standard deviation criterion, the proposed approach prevails, with a standard deviation of 0.0047 compared to 0.0195 for the existing method. This result suggests a more accurate generalization of assessments into a single indicator. From a practical standpoint, this points to a more precise outcome in determining the integral assessment of information security.

According to the diagnostics of the level of information security using the first approach, we observe an average level of information security; however, employing the second approach yields a very low level. Consequently, decision-makers have the opportunity to analyze increases or decreases in the level of information security. Ensuring the accuracy of the information security level through the use of a new mathematical framework and method for determining weight coefficients, representing the relevant technology, serves as a foundation for developing effective state policy in the field of information security.

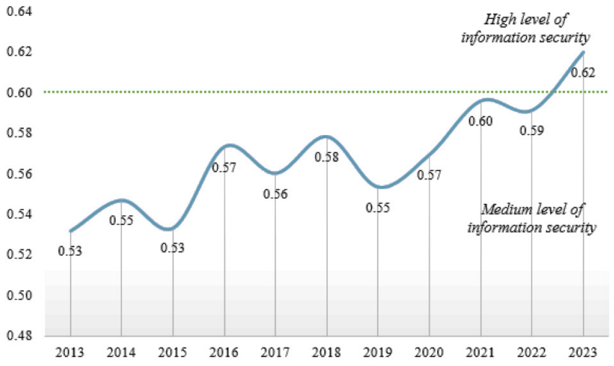

Fig. 3. The dynamics of the integrated information security indicator, taking into account the weighting coefficients determined by the expert evaluation method

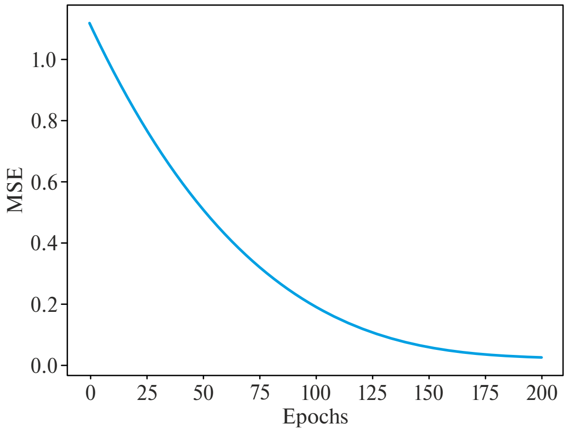

Fig. 4. The mean squared error of training, which determines the values of the weight coefficients

Table 2

The results of determining the integral indicator of information security based on the proposed approach are as follows

The studied indicator	2013	2014	2015	...	2020	2021	2022	2023
Press Freedom Index	0.3000	0.2944	0.2833	...	0.4667	0.4611	0.0411	0.0561
Social Progress Index	0.6196	0.6196	0.6196	...	0.6135	0.7055	0.0681	0.0638
E-Government Development Index	0.5492	0.5492	0.6140	...	0.6425	0.6425	0.1142	0.1142
Global Innovation Index	0.4621	0.5227	0.5152	...	0.6591	0.6288	0.0568	0.0583
World Digital Competitiveness Rankings	0.1429	0.2063	0.0635	...	0.0794	0.1429	0.0214	0.0214
Global Cybersecurity Index	0.6000	0.6000	0.6000	...	0.5928	0.5979	0.1196	0.1196
National Cyber Security Index	0.8500	0.8500	0.8500	...	0.8438	0.8500	0.17	0.1863
Integral indicator of information security of the national economy	0.0096	0.0134	0.0073	...	0.0155	0.0229	0.00000015	0.00000021
The standard deviation of the complex indicators 0.0047								

No unexpected results were recorded in the study of the components of national economic information security; however, several ineffective approaches were identified. These approaches are explained by the technology used to determine the composite indicator, where the method for finding weight coefficients is more precise when utilizing artificial intelligence.

It is noteworthy that a wide range of methods for determining weight coefficients using artificial intelligence is currently available. This can be further expanded and improved in the proposed technology in the future.

We affirm that the research methods employed for diagnosing the level of information security were adequate, as confirmed by corresponding mathematical calculations. Limitations of the proposed approach include insufficient consideration of variable regularization ideas. This mathematical operation would also impact the study's results, although it is unclear whether positively or negatively. Future research should explore the issue of variable regularization and other ways to improve models and technology overall.

Another insufficiently studied aspect of developing models for diagnosing information security levels and the effectiveness of regulatory measures in this context is the consideration of parametric and non-parametric approaches to model construction. This could also be integrated with regularization into a unified ensemble model.

From another perspective, given a sufficient volume of data, a promising addition to the research toolkit may be artificial intelligence, particularly clustering, classification, and regression. Constructing these models will enhance the process of analyzing information security levels. Additionally, a robust enhancement to the created technology could be the use of models that operate online. This would allow for real-time diagnostics of the information security level but would also require hardware, specifically single-board computers.

Thus, the proposed technology involves selecting a method for determining the weight coefficients of the components of information security and, at the same time, a method for aggregating assessments into a single indicator. As observed, the primary diagnostic method demonstrated the superiority of the components of the National Cyber Security Index and the Global Cybersecurity Index, each scoring 0.2. Other components, specifically the World Digital Competitiveness Rankings and the E-Government Development Index, received a score of 0.15, while the Global Innovation Index, the Social Progress Index, and the Press Freedom Index reached scores of 0.1, respectively.

With the use of artificial intelligence, the priorities of the weight coefficients have shifted. The most significant components of information security, according to the obtained results, are the National Cyber Security Index (0.196) and the Global Innovation Index (0.1917). The weight coefficients for components such as the Global Cybersecurity Index, the E-Government Development Index, and the Press Freedom Index were 0.1787, 0.144, and 0.1416, respectively. Components with less significant impact introduced into the model include the Social Progress Index (with a weight coefficient of 0.1185) and the World Digital Competitiveness Rankings (with a weight coefficient of 0.0296). This distribution has affected the final practical outcome.

Accordingly, based on the obtained results, it can be asserted that strengthening cybersecurity and developing innovative technologies are of paramount importance for supporting national security and the economic development of Ukraine, especially in the context of contemporary challenges.

We will formulate recommendations for creating similar technologies. The foundation for building technologies for diagnosing information security can be based on the following actions that should be considered.

1. Utilize various methods for determining assessments.

2. Employ different approaches for calculating weight coefficients, with a preference for artificial intelligence techniques.

3. Create variables considering not only six-factor interactions but also two-factor, three-factor, and higher interactions, depending on the number of input variables.

4. Develop linear and nonlinear models, or linear models with nonlinear parameters. The adequacy of these models can be assessed by maintaining the condition of normal distribution, among other criteria. Alternatively, different distribution laws may apply depending on the research conditions.

5. In the absence of experimental assessments, it is recommended to use artificially generated evaluations through various methods, including bootstrap sampling, where adjustments are made for noise/signal considerations.

6. Validate the obtained results using two or more experimental datasets.

7. Implement and enhance the proposed technology in accordance with technical requirements. It is worth noting that the accumulation of assessments for the indicated indicators each year forms a time series, where it is possible to utilize alternative tools for analyzing the assessments and weight coefficients of the components of information security.

Thus, the proposed technology for assessing the level of information security has improved the methodology by increasing the accuracy of the weight coefficients integrated into the model.

Conclusions.

1. The task of developing technology based on an improved methodology for determining the weighting coefficients of information security components is addressed by refining the mathematical operations of the linear model, specifically through a six-factor interaction of parameters and a method for determining weighting coefficients. These coefficients are defined using artificial intelligence tools.

2. Experimental verification of the proposed technology indicates its advantage by comparing the standard deviation of the existing and proposed comprehensive information security indicators. The integrated indicator, which takes the human factor into account, shows a standard deviation of 0.0195, while the comprehensive indicator without the human factor is 0.0047.

From a practical perspective, the proposed approach provides more accurate diagnostics of information security. This, in turn, will enable the development of effective state tools to enhance information security levels, taking its current status into account.

3. The task of providing recommendations for developing similar technologies is addressed by offering clear steps for implementing the core tools of the technology. Practically, this serves as a methodological foundation for improving or creating new technology to determine the weighting coefficients of information security components. The proposed technology can be used alongside existing ones to expand their capabilities.

References.

1. Onyshchenko, S., Yanko, A., Hlushko, A., & Maslii, O. (2023). Economic cybersecurity of business in Ukraine: strategic directions and implementation mechanism. *Economic and cyber security*. Kharkiv: PC TECHNOLOGY CENTER, (pp. 30-58). https://doi.org/10.15587/978-617-7319-98-5.ch2.

2. Onyshchenko, S., Yanko, A., & Hlushko, A. (2023). Improving the efficiency of diagnosing errors in computer devices for processing economic data functioning in the class of residuals. *Eastern-European Journal of Enterprise Technologies*, *5*(4(125)), 63-73. https://doi.org/10.15587/1729-4061.2023.289185.

3. Krasnobayev, V., Yanko, A., & Hlushko, A. (2023). Information Security of the National Economy Based on an Effective Data Control Method. *Journal of International Commerce, Economics and Policy*, article no. 2350021. https://doi.org/10.1142/S1793993323500217.

4. Laktionov, A. (2019). Application of index estimates for improving accuracy during selection of machine operators. *Eastern-European Journal of Enterprise Technologies*, *3*(1(99)), 18-26. https://doi.org/10.15587/1729-4061.2019.165884.

5. Kuzior, A., Yarovenko, H., Brożek, P., Sidelnyk, N., Boyko, A., & Vasilyeva, T. (2023). Company Cybersecurity System: Assessment, Risks and Expectations. *Production Engineering Archives*, *29*(4), 379-392. https://doi.org/10.30657/pea.2023.29.43.

6. Onyshchenko, S., Zhyvylo, Y., Cherviak, A., & Bilko, S. (2023). Determination of the peculiarities peculiarities of using information security systems in financial institutions in order to increase the financial security level. *Eastern-European Journal of Enterprise Technologies*, *5*(13(125)), 65-76. https://doi.org/10.15587/1729-4061.2023.288175.

7. Onyshchenko, S., Yanko, A., Hlushko, A., Maslii, O., & Cherviak, A. (2023). Cybersecurity And Improvement Of The Information Security System. *Journal of the Balkan Tribological Association*, *29*(5), 818-835.

8. Wang, A., Hu, S., & Li, J. (2021). Does economic development help achieve the goals of environmental regulation? Evidence from partially linear functional-coefficient model. *Energy Economics*, *103*, 105618. https://doi.org/10.1016/j.eneco.2021.105618.

9. Kara, K., Yalçın, G.C., Simic, V., Polat, M., & Pamucar, D. (2024). An integrated neutrosophic Schweizer-Sklar-based model for evaluating economic activities in organized industrial zones. *Engineering Applications of Artificial Intelligence*, *130*, 107722. https://doi.org/10.1016/j.engappai.2023.107722.

10. Atchadé, M.N., Mahoudjro, C., & De-Dravo, H.H. (2024). A new index to assess economic diplomacy in emerging countries. *Research in Globalization*, *8*, 100205. https://doi.org/10.1016/j.resglo.2024.100205.

11. Sun, J., Li, Z., Li, J., Wu, G., & Xia, Y. (2023). Hybrid power system with adaptive adjustment of weight coefficients multi-objective model predictive control. *International Journal of Electrical Power & Energy Systems*, *153*, 109296. https://doi.org/10.1016/j.ijepes.2023.109296.

12. Carmen, R.-C., Lasarte-Navamuel, E., & Geoffrey, J.D.H. (2023). Some considerations on assessing the importance of a coefficient. *Socio-Economic Planning Sciences*, 101765. https://doi.org/10.1016/j.seps.2023.101765.

13. Altintaş, F. F. (2024). A novel method for assessing the weight coefficients of criteria within the framework of multi-criteria decision-making: Measurement relying on the impacts of an exponential curve function (MIEXCF). *Gazi University Journal of Science Part A: Engineering and Innovation*. https://doi.org/10.54287/gujsa.1419551.

14. Pamučar, D., Stević, Ž., & Sremac, S. (2018). A New Model for Determining Weight Coefficients of Criteria in MCDM Models: Full Consistency Method (FUCOM). *Symmetry*, *10*(9), 393. https://doi.org/10.3390/sym10090393.

15. Yuan, Q., Pi, Y., Kou, L., Zhang, F., & Ye, B. (2022). Quantitative Method for Security Situation of the Power Information Network Based on the Evolutionary Neural Network. *Frontiers in Energy Research*, *10*. https://doi.org/10.3389/fenrg.2022.885351.

16. Hryhorii Hnatiienko, Nikolay Kiktev, Tatiana Babenko, Alona Desiatko, & Larysa Myrutenko (2021). Prioritizing Cybersecurity Measures with Decision Support Methods Using Incomplete Data. *XXI International Scientific and Practical Conference "Information Technologies and Security" (ITS-2021)*, (pp. 169-180).

17. Zhu, G., & Wang, Y. (2019). Research on Risk Assessment of Information System Based on Fuzzy Neural Network. *Proceedings of the International Academic Conference on Frontiers in Social Sciences and Management Innovation (IAFSM 2018)*. Atlantis Press. https://doi.org/10.2991/iafsm-18.2019.8.

18. Yang, M. (2022). Information Security Risk Management Model for Big Data. *Advances in Multimedia*, *2022*, 1-10. https://doi.org/10.1155/2022/3383251.

19. Randjelovic, D., Stanković, J., Jankovic-Mmilic, V., & Stankovic, J. (2013). Weight coefficients determination based on parameters in factor analysis. *Metalurgia international*, *18*, 128-131.

20. Zhang, Z., & Pfister, T. (2021). Learning fast sample re-weighting without reward data. *2021 IEEE/CVF International Conference on Computer Vision (ICCV)*. https://doi.org/10.1109/iccv48922.2021.00076.

21. Huang, X., Wu, S., & Yang, B. (2022). A Hardy-Hilbert-type inequality involving modified weight coefficients and partial sums. *AIMS Mathematics*, *7*(4), 6294-6310. https://doi.org/10.3934/math.2022350.

22. Nitsenko, V., Kotenko, S., Hanzhurenko, I., & Ingram, K. L. (2020). Determination of Weight Coefficients for Stochastic and Fuzzy Risks for Multimodal Transportation. *Journal of Physics: Conference Series*, *1529*, 032007. https://doi.org/10.1088/1742-6596/1529/3/032007.

23. Zhao, M., Feng, A., Zhou, J., Jin, Z., & Fan, J. (2024). Optimization study of high-dimensional varying coefficient partially linear model based on elastic network. *Engineering Science and Technology, an International Journal*, *55*, 101731. https://doi.org/10.1016/j.jestch.2024.101731.

24. Altanany, M. Y., Badawy, M., Ebrahim, G. A., & Ehab, A. (2024). Modeling and optimizing linear projects using LSM and Non-dominated Sorting Genetic Algorithm (NSGA-II). *Automation in Construction*, *165*, 105567. https://doi.org/10.1016/j.autcon.2024.105567.

25. Yang, Y., Luo, C., & Yang, W. (2024). Double penalized variable selection for high-dimensional partial linear mixed effects models. *Journal of Multivariate Analysis/Journal of Multivariate Analysis*, 105345. https://doi.org/10.1016/j.jmva.2024.105345.

26. Alsolami, I., & Fukai, T. (2022). *An Extension of Fisher's Criterion: Theoretical Results with a Neural Network Realization*. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2212.09225.

27. Thaden, H., & Kneib, T. (2018b). Structural equation models for dealing with spatial confounding. *The American Statistician*, *72*(3), 239-252. https://doi.org/10.1080/00031305.2017.1305290.

28. Maindonald, J. H., Braun, W.J., & Andrews, J. L. (2024). Multiple Linear Regression. *A Practical Guide to Data Analysis Using R: An Example-Based Approach*, (pp. 144-207). Chapter, Cambridge: Cambridge University Press.

29. Jagielski, M., Oprea, A., Biggio, B., Liu, C., Nita-Rotaru, C., & Li, B. (2018). *Manipulating Machine Learning: Poisoning attacks and Countermeasures for regression learning*. https://doi.org/10.1109/sp.2018.00057.

30. Svistun, L., Glushko, A., & Shtepenko, K. (2018). Organizational Aspects of Development Projects Implementation at the Real Estate Market in Ukraine. *International Journal of Engineering & Technology*, *7*(3.2), 447-452. https://doi.org/10.14419/ijet.v7i3.2.14569.

31. Bashynska, I. O. (2015). Using the method of expert evaluation in economic calculations. *Aktual'ni problemy ekonomiky*, *7*, 408-412.

Технологія визначення вагових коефіцієнтів складових інформаційної безпеки

С. В. Онищенко, А. Д. Глушко, О. І. Лактіонов, С. С. Білько*

Національний університет «Полтавська політехніка імені Юрія Кондратюка», м. Полтава, Україна

* Автор-кореспондент e-mail: itm.olaktionov@nupp.edu.ua

Мета. Розроблення технології визначення вагових коефіцієнтів на основі удосконаленої методики для забезпечення точності визначення рівня інформаційної безпеки з урахуванням її складових.

Методика. Досліджено процес створення й проведення експерименту технології визначення вагових коефіцієнтів складових інформаційної безпеки на макрорівні. Особливістю запропонованої технології є використання двох комплексних оцінок, котрі узагальнюють інформацію в одну оцінку. Один комплексний показник, побудований на основі врахування людського фактору, інший – з виключенням людського фактору за рахунок використання штучного інтелекту. Масиви результуючих оцінок використовуються для визначення рівня інформаційної безпеки. Це дозволяє поліпшити ефективність процесу діагностики інформаційної безпеки.

Результати. Запропонована технологія за рахунок використання комплексного показника демонструє ефективніші результати діагностики, що визначено за ознакою стандартного відхилення. Інтегрований показник, що враховує людський фактор, демонструє значення стандартного відхилення 0,0195, а комплексний показник без урахування людського фактору – 0,0047.

Наукова новизна. Запропонована технологія відрізняється від існуючих використанням комплексного показника, котрий ураховує шестизначну взаємодію інтегрованих показників і вагові коефіцієнти, визначені засобами штучного інтелекту.

Практична значимість. Створена технологія забезпечує точніший результат інтегрального оцінювання рівня інформаційної безпеки. Це дозволить розробити ефективні державні інструменти для підвищення рівня інформаційної безпеки з урахуванням його поточного значення та обґрунтувати стратегічні напрями зміцнення інформаційної безпеки країни.

Ключові слова: *лінійна модель, інтегральний показник, штучний інтелект, інформаційна безпека*

The manuscript was submitted 08.04.24.