

Adaptive Neuro-Fuzzy Methodology for the Information Security Risk Assessment in Transport-Logistics Centers

OLEKSII TRUNOV, MARIIA DOROSH, OLENA TRUNOVA

Department of Information Technology and Software Engineering, Chernihiv Polytechnic National University, Chernihiv, Ukraine

Corresponding author: Oleksii Trunov (e-mail: alexeytrunov1995@gmail.com).

This research was supported by the Ministry of Education and Science of Ukraine in applied research: "Development of an information-analytical system for managing logistics operations of innovative restoration of border regions to ensure national security."

ABSTRACT This paper presents an adaptive neuro-fuzzy methodology for integrated information security risk assessment in transport and logistics centers (TLCs). The proposed approach is based on a unified mathematical model for aggregating factor groups and is implemented through a comprehensive conceptual model that combines the transparency of expert knowledge with the adaptability of machine learning. The model includes six interconnected components that support a complete analytical cycle from data acquisition to managerial decision-making. A key element, the Mamdani Rule Base Generator, automates the creation of the expert rule base, reducing time costs and minimizing expert involvement. To address the computational complexity of generating large rule sets and to mitigate the "cold start" problem caused by limited historical data, the system incorporates a Rete algorithm. Adaptive Neuro-Fuzzy Inference (ANFIS) and a second-order Takagi-Sugeno-Kang (TSK) network enable nonlinear modeling and accurate approximation of expert knowledge. Experimental validation through the "Dynamic Adaptation" test confirmed the system's ability to automatically reconfigure risk assessment logic under changing external conditions. The results demonstrate robustness, scalability, and practical applicability for proactive information security management in TLCs. The methodology was validated using a real-world operational dataset across three transport and logistics centers. The neuro-fuzzy model achieved an overall classification accuracy of 95.2%, demonstrating high selectivity and stability in identifying critical information security states.

KEYWORDS Information Security; Adaptive Neuro-Fuzzy Methodology; Risk Assessment; Logistics, Management.

I. INTRODUCTION

In the face of unprecedented challenges related to Russian aggression and the urgent need for post-war recovery in Ukraine, the development and implementation of effective information technologies to ensure sustainable information security of transport and logistics centers (TLCs) is a critically important element of national security [1]. TLC are strategic arteries that play a key role in ensuring the country's defense capability, functioning of humanitarian corridors, supporting economic stability, and restoring damaged infrastructure. Given the increased risks of cyberattacks during wartime, there is an urgent need to develop not just reactive but proactive, intelligent approaches to protecting information systems [2]. Stable operation of the information systems of TLCs in the post-war period will become one of the foundations of successful reconstruction. That is why creating and implementing an adaptive intelligent decision support system

(AIDSS), which uses advanced fuzzy logic methods to effectively handle the inherent uncertainty of complex systems, is an urgent necessity.

Research on information systems in the logistics domain primarily focuses on the ISO 27001 framework as a guide to creating an information security system [3]. However, due to new threats, there is a need to develop specific risk assessment methods within this framework that consider the peculiarities of the industry and adapt general risk management methods to the field of information security.

The main obstacles affecting risk assessment include:

- It is very difficult to statistically accumulate data for modeling cybersecurity risks;
- The dynamics of the situation are constantly increasing;
- Malicious actors try to conceal possible scenarios (forecasting is almost impossible; that is their task);

- Loss assessment is complicated by the presence of unpredictable impacts on system elements, among other factors.

At the same time, a key problem in implementing intelligent protection systems is the lack of relevant historical data and the difficulty of predicting possible system states and emerging threats [4]. This complicates the use of classical machine learning methods and renders the results either useless or ineffective for supporting proactive decision-making, as they are based on already realized scenarios.

The goal of this work is to develop an adaptive methodology of the information security risk assessment in transport and logistics domain capable of functioning as an expert system at the start and automatically learning as factors and conditions affecting the information security (IS) of TLC.

Scientific Novelty. The scientific novelty of the proposed approach lies in the development of an adaptive neuro-fuzzy methodology wherein the “cold start” problem – caused by the lack of historical information security incident statistics – is resolved using an artificial (synthetic) dataset. Unlike traditional static approaches or baseline machine learning configurations, this integration enables the creation of an upper coordination level intelligent Decision Support System (DSS) capable of evolutionary self-learning.

The core architectural advancement is the transition from static expert evaluations to an active neuro-fuzzy network based on a second-order non-linear Takagi-Sugeno-Kang (TSK) polynomial. This ensures the capacity to dynamically detect non-linear interactions between risk factors and automatically retrain the system as real-world monitoring data accumulates.

II. RELATED WORKS

As noted in [5], the analysis and assessment of information security risks in automated corporate systems are often complicated by data inaccuracy and insufficient knowledge about the system under study. To address this issue, the paper proposes the use of fuzzy logic approaches. A set of fuzzy rules has been developed for testing. An approximate solution to the problem is obtained using a fuzzy inference mechanism based on these rules.

Further exploration of fuzzy models for information security risk evaluation is presented in [6], where the authors focus on maintaining the security level of ERP systems. Their contribution lies in formalizing the assessment of information value as an input parameter for the risk evaluation model.

In the logistics domain, fuzzy logic has primarily been applied to technical problem-solving. For example, [7] introduces an empirical methodology of the fuzzy analytic hierarchy process (FAHP), which integrates fuzzy logic with the analytical hierarchy process (AHP). This approach combines quantitative and systems theories within the framework of modern management theory. Similarly, [8] proposes a model for determining delivery times by incorporating expected risk factors (RF). Using fuzzy logic and expert knowledge, the study identifies key technical and operational hazards during loading and transportation, translating them into risk factors. As noted in [9], traditional mathematical methods struggle to capture such risks due to limited understanding and high uncertainty in the domain.

Fuzzy logic [10] is a valuable technique for managing complexity and uncertainty, offering a means to model systems

by mimicking human cognitive processes without relying solely on quantitative or qualitative data in computations [11]. In the context of international trade, sustainable decision-making for import and export businesses is hindered by the imprecise and multifaceted nature of the parameters involved. Researchers have therefore proposed fuzzy inference systems to measure risk, particularly in cases where sufficient data to characterize risk probability and impact are unavailable. Within the Internet of Things (IoT) environment, [12] highlights the limitations of existing risk-based models, which fail to incorporate real-time contextual information. Their proposed model leverages contextual data extracted during access requests to inform authorization decisions, while smart contracts dynamically adjust user privileges based on activity. This approach also enhances the flexibility of the methodology.

The application of adaptive neuro-fuzzy inference systems (ANFIS) to information security risk assessment has also been explored. In [13], the authors propose an ANFIS-based Security Risk Assessment (SRA) system for different stages of the Software Development Life Cycle (SDLC). Security risk factors were identified for each stage, serving as inputs to the model. However, the approach has notable limitations: correlations between SDLC stages were not considered, and the model was not validated on real-world software projects. Consequently, questions remain regarding how learning algorithms trained on historical project data could improve predictive accuracy. At the same time, a modified neuro-fuzzy Wang-Mendel architecture introduced in [14] demonstrated high efficiency for online fault classification under non-stationary information flows, halving the training time compared to classical methods while maintaining test accuracy on limited data.

A more comprehensive fuzzy information security risk assessment model was introduced in [15]. The proposed new risk assessment model has been implemented using fuzzy logic in the form of 15 fuzzy machines. In a series of experiments, the authors have scrutinized the information security risk assessment of various software products. It was also noted that the only disadvantage of these methods is the high labor intensity of experts in the evaluation.

Therefore, it is essential to develop a flexible model for information security assessment, which incorporates the application of fuzzy logic to ensure adaptability and variability in the evaluation of parameters that are otherwise rigidly predefined.

III. MATERIAL AND METHODS

For the study, methods of fuzzy logic were employed in conjunction with the Rete algorithm. The proposed methodology integrates expert knowledge (via Fuzzy AHP) with the computational capacity of machine learning (ANFIS) and algorithmic optimization (Rete). This approach establishes an adaptive environment that enables decision-makers to conduct scenario-based risk analyses and obtain mathematically substantiated forecasts of the consequences of their managerial decisions without the need to modify the system’s source code.

IV. CONCEPTUAL MODEL OF THE INFORMATION TECHNOLOGY FOR RISK ASSESSMENT IN LOGISTICS CENTERS’ INFORMATION SECURITY

The specificity of logistics center information security is characterized by incomplete input data, the vagueness of expert

evaluations, and the stochastic nature of cyberattacks. Existing risk assessment methods are predominantly static, which necessitates the development of an adaptive decision-support information technology capable of responding to changes in the threat landscape in real time. The proposed technology is constructed based on a risk-level assessment model:

$$R = f(A, P, Los, Con, F, Cul), \quad (1)$$

where R – the level of information security risk in logistics centers;

$A = \{A_1, A_2, \dots, A_j\}$ – the value level of assets;

$P = \{P_1, P_2, \dots, P_i\}$ – the probability of threat realization through identified vulnerabilities;

$Los = \{Los_1, Los_2, \dots, Los_i\}$ – the level of losses resulting from threats;

$Con = \{Con_1, Con_2, \dots, Con_n\}$ – the level of control over information resources;

$F = \{F_1, F_2, \dots, F_m\}$ – the level of expenditures for the development and operation of the information security system;

$Cul = \{Cul_1, Cul_2, \dots, Cul_k\}$ – the level of information security culture.

For mathematical modeling, unified notations are introduced for the aggregated levels of these factor groups:

- x_1 – generalized asset value level (corresponding to group A). Evaluates the hub's critical digital assets, including warehouse management system, enterprise resource planning, client databases, and specialized hardware;
- x_2 – generalized probability of threat realization (corresponding to group P). Reflects the localized probability of cyberattacks, such as distributed denial-of-service (DDoS) attacks targeting logistics web applications, phishing campaigns aimed at dispatch service personnel, and malicious interception of MQTT sensor traffic;
- x_3 – generalized loss level (corresponding to group Los). Captures the potential operational and financial impact, including disruptions to critical supply chain schedules, contractual financial penalties, and reputational damage to the terminal TLC;
- x_4 – generalized control level (corresponding to group Con). Represents internal organizational control loops and technical security defense mechanisms;
- x_5 – generalized expenditure level for information security (corresponding to group F). Defines the budget allocated for the operation, maintenance, and upgrading of security systems;
- x_6 – generalized level of information security culture (corresponding to group Cul). Assesses staff security awareness and internal constraints related to the human factor.

To implement this model in information technology, a comprehensive model of integral risk assessment has been developed, which is based on a holistic approach. This approach systematically combines the transparency of expert knowledge with the adaptability of machine learning, integrating heterogeneous mathematical methods to address specific tasks at each stage of the analysis (Fig. 1).

Conceptual Model of Integral Risk Assessment is

implemented according to a modular principle and consists of six interrelated blocks that ensure the complete cycle of information processing from raw data to decision-making (Fig. 1). Forming the operation base, knowledge base, and strategic analyses are described in [16, 17]. In this article, we will provide explanations and experiments with Rule generation and ANFIS usage to create recommendations for decision-making.

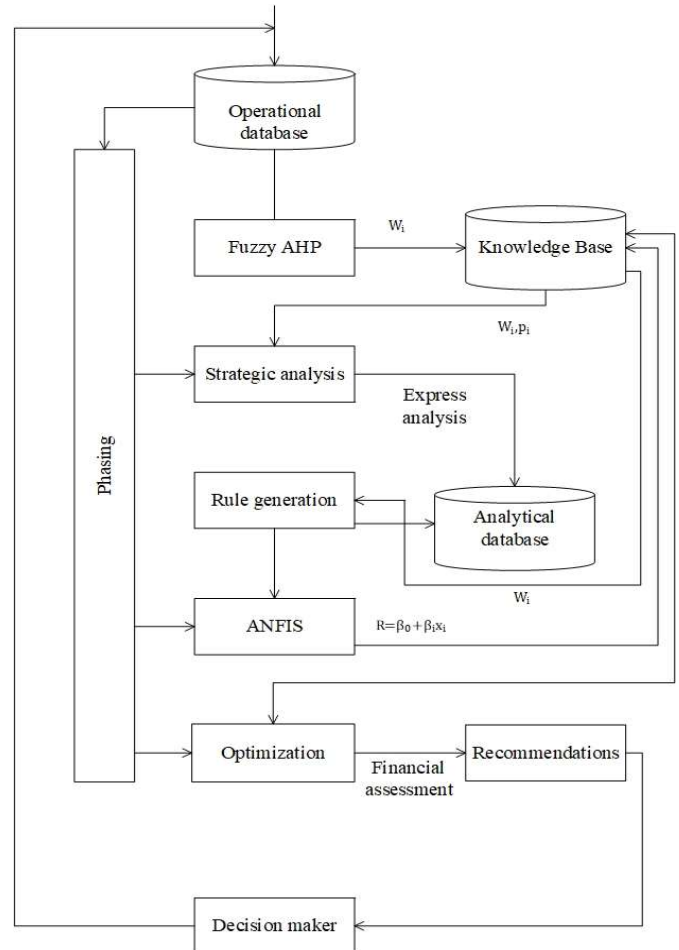


Figure 1. Conceptual Model of Integral Information Security Risk Assessment for Logistics Center.

The adaptability of the model is ensured through the automatic generation of a complete rule base [18]. This is an automated process of forming an expert knowledge base and addressing the “cold start” problem under conditions of absent historical statistics. Instead of manual rule creation, which requires direct involvement of specialists for each parameter change, the module generates a theoretically exhaustive base of Mamdani-type fuzzy rules [19].

A. GENERATION OF A COMPLETE RULE BASE

The adaptability of the model at the initialization stage is ensured by a specialized module, *MamdaniRuleBaseGenerator*. This module was developed to automate the process of forming an expert knowledge base, which usually required significant time expenditures and the direct involvement of specialists (experts) whenever parameters were modified (Fig.2).

The purpose of the module is to create a complete base of Mamdani-type fuzzy rules, serving as an initial (theoretically

exhaustive) model. In the absence of real statistical data, such a base functions as a formalized expert model (“synthetic Teacher”), which describes the full space of possible system states. This approach effectively addresses the problem of the “cold start”.

The generation process is carried out by enumerating all possible combinations of the linguistic terms of the input factors $(x_1, \dots, x_6)$ using the Cartesian product:

$$RB_{total} = T_1 \times T_2 \times \dots \times T_6 \quad (2)$$

where $T_i = \{t_{i,1}, t_{i,2}, \dots, t_{i,N_i}\}$ – Set of Linguistic Terms and Rule Count; the set of linguistic terms for the i -th factor, N_i – the number of terms.

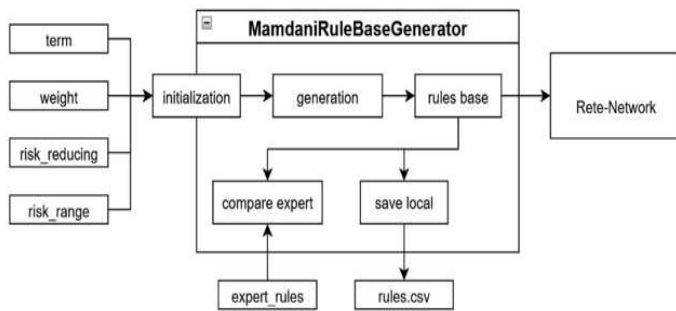


Figure 2. Workflow of the Rule Base Generation Module.

The total number of rules:

$$N_{rules} = \prod_{i=1}^6 N_i. \quad (3)$$

For each generated rule indexed by k , the reference risk index $R_{ref}^{(k)}$ is automatically computed, serving as the target value for training:

$$R_{ref}^{(k)} = \frac{\sum_{i=1}^6 w_i \cdot S_i \cdot \text{Norm}(\text{Ind}(t_i^{(k)}))}{\sum_{i=1}^6 |w_i|}, \quad (4)$$

where k – index of the current rule in the generated rule base ($k = 1, \dots, N_{rules}$); w_i – weight coefficient of the i -th factor, obtained from the Fuzzy AHP module; $S_i \in \{-1, +1\}$ – the sign indicator reflecting the direction of influence of the i -th factor on risk; $t_i^{(k)}$ – the linguistic term of the i -th factor in the antecedent of the k -th rule; $\text{Ind}(t)$ – a function that returns the ordinal number of term t within the term set of the i -th factor; $\text{Norm}(\cdot)$ – a normalization function that transforms the term index into the range $[0,1]$ or $[-1,1]$, depending on the selected modeling scale.

To overcome the computational complexity arising from the generation of a complete rule base (ranging from 729 to 3840 combinations), the system implements a Rete engine [20]. Using the Rete architecture transforms the expert knowledge base into a high-performance source of synthetic data. This solves the “cold start” problem under conditions of insufficient historical data [21]. By transforming the static set of rules into an optimized graph, the module enables instantaneous calculation of the reference risk index (R_{ref}) for each input vector, while maintaining high computational efficiency even for large knowledge bases [22]. This approach allows the complete rule base to be employed as a “Synthetic Teacher” for

tuning the ANFIS weight coefficients, thereby realizing the contemporary paradigm of neuro-symbolic artificial intelligence [23].

B. ADAPTIVE NEURO-FUZZY INFERENCE

Adaptive Neuro-Fuzzy Inference (ANFIS) implements a hybrid neuro-fuzzy reasoning model that functions as a universal approximator for reproducing and generalizing the knowledge embedded within the expert system [24]. The Conceptual Model corresponds to a second-order Takagi-Sugeno-Kang (TSK) network [25], which enables the modeling of complex nonlinear relationships between input factors and the final risk level (Fig. 3).

The key advantage of the proposed approach lies in its locally adaptive structure: the system of fuzzy rules performs a decomposition of the input factor space into distinct contexts. For each context, a separate second-order polynomial is applied, which makes it possible to account not only for the direct influence of individual factors but also for the interaction effects among them.

C. MODEL IMPLEMENTATION ALGORITHM

Step 1. Formalization of the rule structure. The system’s knowledge base is represented as a set of parametric entities. Each fuzzy rule k is defined by two components.

Antecedent (a set of linguistic conditions for the input factors that defines the feature space region in which the given rule is active):

$$IF (x_1 \text{ is } A_1^{(k)}) \text{ AND } \dots \text{ AND } (x_n \text{ is } A_n^{(k)}).$$

The parameters of the membership functions $\mu_{A_i^{(k)}}(x_i)$ are adaptive and subject to adjustment during the network training process.

Consequent (a vector of coefficients of the local polynomial that approximates the dependence of the output variable R (risk) on the input factors within the rule activation:

$$\begin{aligned} THEN \ z_k(X) = & \beta_{0,k} + \sum_{i=1}^6 \beta_{i,k} x_i + \\ & + \sum_{i=1}^6 \sum_{j=1}^6 \beta_{ij,k} x_i x_j. \end{aligned}$$

Step 2. Local Polynomial Inference. For each rule k , the output signal z_k is computed using a second-order polynomial:

$$z_k(X) = \beta_{0,k} + \sum_{i=1}^6 \beta_{i,k} x_i + \sum_{i=1}^6 \sum_{j=1}^6 \beta_{ij,k} x_i x_j. \quad (5)$$

In the non-linear part of the second-order polynomial, the mathematical conditions are specified as follows: the general constraint $j \geq i$ for the double summation eliminates parameter redundancy; the condition $i = j$ isolates the squared terms to reflect the factor’s self-interaction; and the condition $j > i$ defines the cross-terms, capturing the pure interaction between different factors without duplication.

Step 3. Initialization of Coefficients To accelerate the convergence of the training algorithm and to avoid local minima, an intelligent initialization of the parameters of the polynomial consequents is performed. The initial values of the linear coefficients $\beta_{i,k}^{(0)}$ for each i -th factor

are determined on the basis of the corresponding normalized weights w_i , obtained from the Fuzzy AHP module, with direct consideration of the nature of the factor's influence on the integral risk.

$$\beta_{i,k}^{(0)} = w_i \cdot S_i. \quad (6)$$

where w_i – the normalized weight coefficient of the i -th factor ($w_i > 0$); S_i – the sign indicator of the factor's influence

$$S_i = \begin{cases} -1, & \text{if the factor decreases the risk } (x_4, x_5, x_6); \\ +1, & \text{if the factor increases the risk } (x_1, x_2, x_3). \end{cases}$$

This mechanism accounts for the opposing effects of factors: the sign indicator S_i mathematically regulates the direction of their impact on the overall risk, enabling the accurate aggregation of conflicting data into a consistent index before model training begins.

The remaining model coefficients (the bias term $\beta_{i,k}^{(0)}$ and the coefficients associated with quadratic and cross terms $\beta_{i,k}^{(0)}$ are initialized with small random values drawn from a uniform distribution:

$$\beta_{0,k}^{(0)}, \beta_{ij,k}^{(0)} \sim U(-\varepsilon, +\varepsilon), \quad (7)$$

where ε is a small positive number.

Step 4. Reference Generation and Training
At this stage, the Rete network serves as a generator of the “teacher signal.” For each input vector from the training dataset, the engine computes the exact reference risk (R_{ref}), which acts as the target value for tuning the neural network. The parameters of all local polynomials are optimized via gradient descent using the Adam method, with minimization of the mean squared error (MSE) between the ANFIS output and the reference values provided by the previous module.

$$MSE = \frac{1}{N} \sum_{p=1}^N (R_p - R_{ref,p})^2 \rightarrow \min, \quad (8)$$

where N – number of training examples, R_p – ANFIS output for the p -th example, $R_{ref,p}$ – reference risk for the p -th example. Optimization is performed not only for the polynomial coefficients but also for the parameters of the membership functions, which is the standard practice in ANFIS.

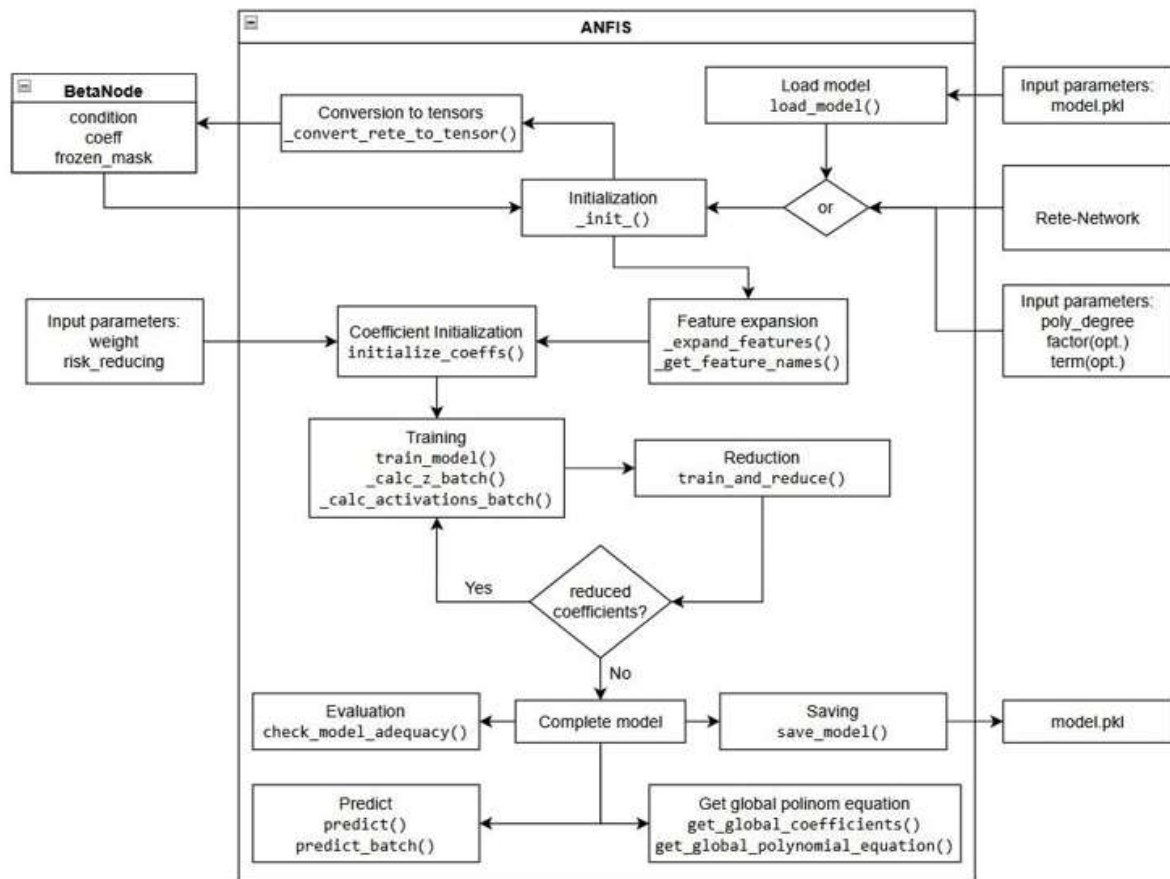


Figure 3. Architecture and Workflow of the ANFIS Module.

D. MODEL REDUCTION

After the initial training, an iterative simplification of the structure is performed to eliminate redundancy. The procedure involves identifying and discarding coefficients whose absolute values are smaller than a critical threshold δ . The justification of this threshold is based on Student's t -statistic,

which allows testing the null hypothesis regarding the insignificance of the corresponding factor's influence ($H_0: \beta = 0$) at a given confidence level [26]. To compute Student's t -statistic, the standard errors (SE) of coefficients $\beta_{i,k}$ are estimated locally within each fuzzy rule context and weighted by the rule fulfillment degrees $w_k(X)$. The t -statistic is defined as:

$$t = \frac{\beta_{i,k}}{SE(\beta_{i,k})}.$$

Parameters with $|t| < t_{crit}$ at a 95% confidence level are considered insignificant and removed. Coefficients found to be insignificant are “frozen” (excluded from the gradient optimization vector), and the training process is repeated until statistical significance is achieved for all active parameters of the model.

E. AGGREGATION AND FINAL RESULT

The degree of fulfillment of the rule $w_k(X)$ is computed as the *T-norm* (product) of the membership degrees:

$$w_k(X) = \prod_{i=1}^6 \mu_{A_i^{(k)}}(x_i) \quad (9)$$

The normalized weight of the rule:

$$\bar{w}_k(X) = \frac{w_k(X)}{\sum_{j=1}^{N_{rules}} w_j(X)}. \quad (10)$$

The final risk level $R \in [0,1]$ is computed as the weighted sum of the rule outputs, followed by normalization through the sigmoid function:

$$R(X) = \sigma\left(\sum_{k=1}^{N_{rules}} \bar{w}_k(X) \cdot z_k(X)\right), \quad (11)$$

where $\sigma(y) = \frac{1}{1+e^{-\lambda y}}$ – sigmoid activation function mapping the result into the interval $[0,1]$; λ – slope coefficient of the sigmoid; $\bar{w}_k(X)$ – normalized rule activation k , $z_k(X)$ – the local output (consequent) of the k -th rule.

The sigmoid function is applied to map the unconstrained polynomial outputs strictly into the standard probability interval $[0, 1]$. The slope parameter is set to $\lambda=1$ to ensure a stable gradient flow and prevent gradient saturation issues during neural network training.

V. ADDITIONAL CAPABILITIES

The ANFIS module supports adequacy assessment on test data using metrics such as MAE, RMSE, and correlation between predicted and actual risk values [27].

The developed methodology provides the full life cycle of the system through the implementation of three key mechanisms:

- Knowledge Persistence. Serialization of the model together with the “reduction mask” allows fixing the structure of significant connections. This eliminates the need for repeated resource-intensive rule changing during system restart or scaling.
- From Expert to Data-Driven. To overcome the “cold start” problem, the model is initialized on synthetic data. During operation, the Fine-tuning mode is activated, enabling gradual retraining of the model on accumulated real incident statistics, smoothly transforming it from expert-based to hybrid (expert + data-driven).
- Adaptive Reconfiguration. Updating the pairwise comparison matrices in the Fuzzy AHP module serves as a trigger for automatic retraining of the polynomial kernels. This ensures adaptation of the system’s sensitivity to changing strategic conditions (e.g.,

introduction of martial law) without any modifications to the program code.

VI. RESULTS AND DISCUSSION

Experimental Setup. During the computational simulation of the developed neuro-symbolic framework, the dynamic parameter tuning of the non-linear TSK consequent layer was executed using a learning rate of $\eta = 0.01$ with MSE loss control and an Early Stopping window of 5 epochs. The adaptation and validation pipelines were fully implemented in Python using PyTorch, Scikit-Fuzzy and XANFIS libraries, and executed on a workstation equipped with an 8-core CPU, 32 GB RAM, and an NVMe SSD.

The effectiveness of the developed methodology was tested in the experiment “Dynamic Adaptation”, aimed at confirming the system’s ability to automatically reconfigure the logic of risk assessment under changing external conditions (transition from “peace time” to “war time”) without any modifications to the program code.

Due to the absence of representative incident statistics for the specific conditions of martial law (“cold start”), validation was conducted on a synthetic dataset. The data were generated by the Rule Base Generation Module through exhaustive enumeration of linguistic terms (729 scenarios for the simplified configuration), ensuring coverage of the entire space of possible system states. For each scenario, the reference risk value was computed according to the current expert weighting coefficients.

Experiment Design. At State A the system was initialized with weights corresponding to the normal operating mode. At State B (Escalation of Threats) a simulated escalation scenario triggered updates of the pairwise comparison matrices in the Fuzzy AHP module.

The generalized dynamics of input priority changes are presented in Table 1, where the specific weight coefficients for both State A and State B were obtained via pairwise comparison matrices filled by TLC cybersecurity experts during structured interviews.

Table 1. Comparison of Model Parameters in Peace Time (State A) and Escalation of Threats (State B).

Factor Name	Weight W_A (State A)	Weight W_B (State B)	Dynamics of Change
Asset value level (x_1)	0.154	0.150	No significant change
Probability of threat realization (x_2)	0.225	0.200	Slight decrease
Loss level (x_3)	0.354	0.450	Significant increase (+27%)
Control level (x_4)	0.043	0.040	Slight decrease
Information security expenditure level (x_5)	0.124	0.124	No change
Information security culture level (x_6)	0.100	0.160	Increase (+60%)

As shown in Table 1, the key change was the shift of emphasis toward minimizing potential losses (x_3) and increasing the role of security culture (x_6). The change in input weights (Table 1) triggered the automatic retraining of the ANFIS neuro-fuzzy network.

Table 2 presents a comparative analysis of the polynomial

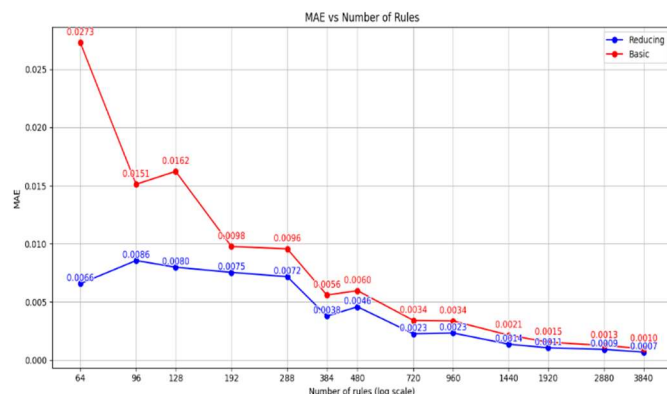
coefficients, demonstrating how the system’s “logic of reasoning” has changed.

As shown in Table 2, the system did not merely change the weights linearly but also restructured the nonlinear relationships. In particular, the increase of the coefficient for x_3 to 0.6508 confirms the main hypothesis: under wartime conditions, the acceptability of financial or reputational losses becomes critically low.

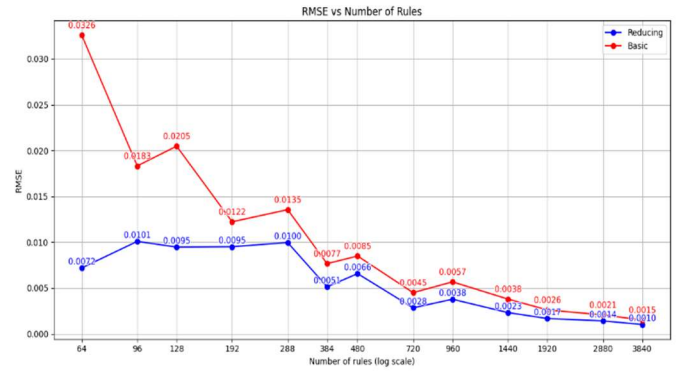
Table 2. Comparison of Risk Polynomial Coefficients

Coefficient Type	Factor Interaction	Value State A	Value State B	Interpretation of Adaptation
Linear	Loss level (x_3)	0.494	0.650	The system became significantly more sensitive to potential losses.
	Information security culture (x_6)	-0.260	-0.412	The role of personnel in risk reduction has been strengthened.
Nonlinear (reinforcement)	Asset value level / Loss level ($x_1 x_3$)	0.117	0.144	Critical assets require prioritized protection against losses.
	Threat realization probability / Loss level ($x_2 x_3$)	0.122	0.139	Increased weight of the classical risk component.
Nonlinear (mitigation)	Control level $\times$ Information security culture ($x_4 x_6$)	-0.102	-0.161	Synergistic effect – technical protection measures become 57% more effective under conditions of a high personnel security culture.

In addition to adaptability, the universality of the system with respect to computational resources was investigated. Two configurations were tested: “Light” (Reducing) – up to 729 rules, “Detailed” (Basic) – up to 3840 rules. The experimental results (Figures 4 and 5) demonstrated the following:



a)



b)

Figure 4. Dependence of Training Errors (a) MAE and b) RMSE) on the Number of Rules.

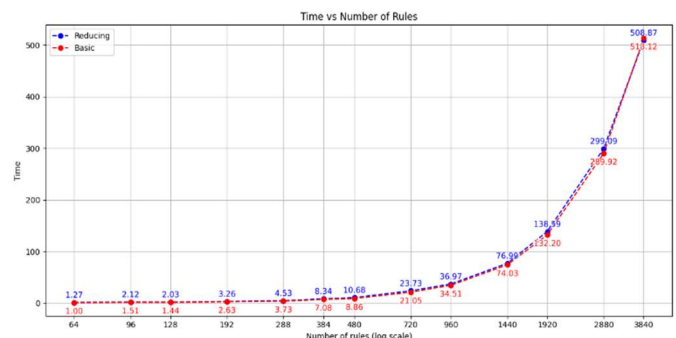


Figure 5. Dependence of Training Time on the Granularity of the Knowledge Base.

The analysis of Fig. 4 and Fig. 5 reveals that at 64 rules, the Reducing method significantly outperforms the baseline, restricting errors to MAE = 0.0066 and RMSE = 0.0072 versus MAE = 0.0273 and RMSE = 0.0326 for the Basic configuration. This four-fold precision gain requires a minimal temporal trade-off, taking 1.27 seconds compared to 1.00 second. At the 720-rule threshold, the error profiles perfectly converge (MAE = 0.0034, RMSE = 0.0045), with execution runtimes remaining close at 23.73 and 21.05 seconds respectively. At the maximum scale of 3,840 rules, accuracy is completely identical (MAE = 0.0010, RMSE = 0.0015), and the optimization overhead becomes negligible (508.87 seconds for Reducing versus 511.12 seconds for Basic). Therefore, the Reducing method is highly recommended for initial operational stages (up to 729 rules) due to its high precision, while the Basic method is advisable for large-scale knowledge bases exceeding 3,000 rules where accuracy margins fully converge.

To confirm the practical effectiveness of the proposed adaptive neuro-fuzzy methodology for the comprehensive information security risk assessment of TLCs, an adaptive retraining method was applied in accordance with the approach proposed by I. Nastac [28]. This process is based on the periodic updating of neural network parameters as new critical data arrives. Experimental testing was conducted on a real-world operational dataset comprising 3,840 records accumulated over a 22-month period, which were split into a classic 80/20 ratio for training and independent validation. Model verification was carried out in three distinct sequential stages, each corresponding to the step-by-step integration of telemetry data from a new physical facility (TLC 1, TLC 2, and TLC 3).

The evaluation of accuracy metrics confirmed that the

ANFIS neuro-fuzzy model successfully eliminates the discrepancies between a priori expert estimates and real-world monitoring data. The system automatically revealed hidden systemic biases and non-linear synergistic factor interactions, the consideration of which is typically lost in classical linear expert approaches.

Analysis of the mean squared error (MSE) curve during this evolutionary training process reveals three distinct stages of the neuro-fuzzy network's adaptation to the distributed TLC data, as graphically illustrated in Figure 6:

1. Intensive adaptation (TLC 1, epochs 1–20): The MSE decreases rapidly from 0.008104 to 0.000281. The primary accuracy gain (by epoch 5) is driven by the learning algorithm swiftly adjusting the a priori expert weights to match the empirical statistical patterns of the first facility.

2. Knowledge stabilization (TLC 2, epochs 21–30): The model exhibits monotonic convergence down to 0.000181. The absence of fluctuations confirms high generalization capability, indicating that previously acquired knowledge remains relevant to the second TLC, requiring only minor parameter fine-tuning.

3. Adaptive fine-tuning (TLC 3, epochs 31–40): Introducing data from the third facility at epoch 31 causes a local MSE spike to 0.000240, due to adaptation to specific anomalies or new boundary conditions of TLC 3. However, by epoch 40, the error drops to 0.000198, demonstrating successful integration of new knowledge without catastrophic forgetting of prior experience.

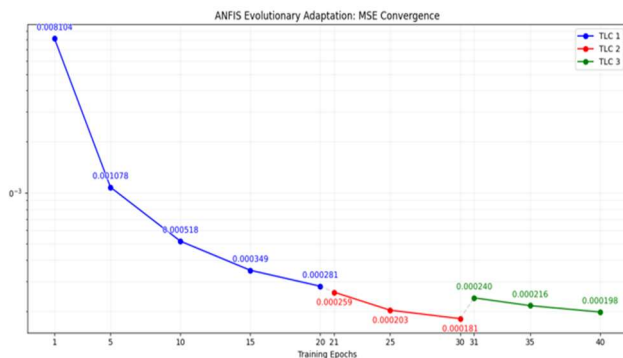


Figure 6. ANFIS Evolutionary Adaptation: MSE Convergence

A comparative analysis of the accuracy of the adapted model versus the baseline expert model across these stages is summarized in Table 3.

Table 3. Statistical Accuracy Metrics of the ANFIS Model at Different Adaptation Stages

Stage	MAE	RMSE	Correlation
Expert model	0.089383	0.109579	0.702599
Stage 1 (after TLC 1)	0.011888	0.016933	0.992841
Stage 1 (after TLC 2))	0.010866	0.015738	0.993922
Stage 1 (after TLC 3))	0.009879	0.014785	0.994522

Even after the first adaptation stage, the Root Mean Squared Error (RMSE) decreased nearly 7-fold compared to the baseline expert model. Upon completion of the final stage, the correlation coefficient stabilized at an exceptional 0.994.

The adapted model functions selectively. Instead of merely scaling the overall risk level proportionally, it restructures its

structural profile, becoming significantly more stringent regarding human factor vulnerabilities and potential operational losses, as detailed in Table 4.

Table 4. State Recognition Accuracy Metrics for TLC Information Security

Class	Precision	Recall	Support	F-mipa
L (Low)	1.00	1.00	3	1.00
M (Medium)	0.92	0.95	143	0.93
H (High)	0.97	0.95	464	0.96
VH (Very High)	0.93	0.96	158	0.94

The overall classification accuracy reached 95.2%, which is graphically illustrated by the confusion matrix in Figure 7.

An analysis of Figure 7 confirms that critical boundary states are identified by the model without error. Experimental testing based on the adaptive retraining methodology using real-world monitoring data validates the framework's capacity for dynamic self-learning and alignment with actual infrastructure behavior.

	L	M	H	VH
Actual L	3	0	0	0
Actual M	0	136	7	0
Actual H	0	12	441	11
Actual VH	0	0	7	151
	L	M	H	VH

Figure 7. Confusion matrix for system state classification.

The sequential integration of telemetry data across three distributed TLCs demonstrates that the ANFIS model effectively eliminates discrepancies between a priori expert assumptions and empirical statistics. Crucially, the model stabilizes its error rate and maintains a high generalization capability without suffering from the “catastrophic forgetting” effect of prior experiences.

VII. CONCLUSIONS

This study introduces an adaptive neuro-fuzzy methodology for the integrated risk assessment of information security in transport and logistics centers. By combining expert knowledge with machine learning and algorithmic optimization, the proposed approach effectively addresses the challenges of uncertainty, incomplete data, and the “cold start” problem. The scientific novelty of the obtained results lies in the creation of a method for automated knowledge synthesis, where the “Synthetic Teacher” component ensures the transition from a qualitative expert model to a quantitative data-based one. This allows the system to function even in the absence of historical incident statistics. Furthermore, the experimental results confirm the architectural feasibility, internal consistency, and high adaptive potential of the methodology under real-world monitoring scenarios, allowing

the framework to autonomously adapt the fuzzy rules system to support decision-making logic in critical changes of the external environment. This is achieved through the dynamic reconfiguration of functional dependencies without the need for source code modification. Experimental results confirm that the methodology is robust, scalable, and capable of functioning under various computational loads.

Future research will focus on several directions: the integration of real-time monitoring data into the adaptive framework will enhance responsiveness to emerging threats; expanding the methodology to incorporate advanced hybrid approaches will improve decision-making transparency and interpretability; and multi-center cross-domain validation in other critical infrastructure sectors, such as energy and healthcare, is required to further evaluate the generalizability of the proposed model.

References

- [1] A. O. Chernov, *Development of the Transport and Logistics System of Ukraine in the Context of European Integration*, Master's Thesis, Kyiv, 2024, 107 p. (in Ukrainian).
- [2] V. Grechaninov, "Models and technologies of intellectual protection of information systems of critical infrastructure to increase resilience. Electronic professional scientific publication," *Cybersecurity: Education, Science, Technology*, vol. 1, issue 29, pp. 877–896, 2025. <https://doi.org/10.28925/2663-4023.2025.29.948>. (in Ukrainian).
- [3] T. Malkus, S. Wawak, "Information security in logistics cooperation," *Acta Logistica: International Scientific Journal about Logistics*, vol. 2, issue 1, pp. 9-14, 2015. <https://doi.org/10.22306/al.v2i1.32>.
- [4] J. Bharadiya, "Machine learning in cybersecurity: Techniques and challenges," *European Journal of Technology*, vol. 7, issue 2, pp. 1-14, 2023. <https://doi.org/10.47672/ejt.1486>.
- [5] I.P. Khavina, "Research of the fuzzy logic mechanism for assessing information risks of an enterprise," *Proceedings of the 4th International Scientific and Practical Conference "Modern Research in Science and Education"*, Chicago, USA, December 7-9, 2023, pp. 329-335. <https://dspace.univd.edu.ua/handle/123456789/19547>. (in Ukrainian).
- [6] A.V. Mishchenko, O.V. Kurylo, O.A. Zolotukhina, "Fuzzy model for assessing information security risks and supporting the security level of ERP systems," *Telecommunications and Information Technologies*, issue 1 (66), pp. 42-51, 2020. <https://doi.org/10.31673/2412-4338.2020.011451>. (in Ukrainian).
- [7] N.S.F. Abdul Rahman, N.H. Karim, R. Md Hanafiah, S. Abdul Hamid, A. Mohammed, "Decision analysis of warehouse productivity performance indicators to enhance logistics operational efficiency," *International Journal of Productivity and Performance Management*, vol. 72, issue 4, pp. 962–985, 2023. <https://doi.org/10.1108/IJPPM-06-2021-0373>.
- [8] I. Medvediev, D. Muzylyov, J. Montewka, "A model for agribusiness supply chain risk management using fuzzy logic. Case study: Grain route from Ukraine to Poland," *Transportation Research Part E: Logistics and Transportation Review*, vol. 190, 103691, 2024. <https://doi.org/10.1016/j.tre.2024.103691>.
- [9] N. Luo, H. Yu, Z. You, Y. Li, T. Zhou, Y. Jiao, N. Han, C. Liu, Z. Jiang, S. Qiao, "Fuzzy logic and neural network-based risk assessment model for import and export enterprises: A review," *Journal of Data Science and Intelligent Systems*, vol. 1, issue 1, pp. 2-11, 2023. <https://doi.org/10.47852/bonviewJDSIS32021078>.
- [10] L.A. Zadeh, "Fuzzy sets," *Information and Control*, vol. 8, issue 3, pp. 338–353, 1965. [https://doi.org/10.1016/S0019-9958\(65\)90241-X](https://doi.org/10.1016/S0019-9958(65)90241-X).
- [11] M. Pislaru, I.V. Herghiligiu, I.B. Robu, "Corporate sustainable performance assessment based on fuzzy logic," *Journal of Cleaner Production*, vol. 223, pp. 998–1013, 2019. <https://doi.org/10.1016/j.jclepro.2019.03.130>.
- [12] H.F. Atlam, R.J. Walters, G.B. Wills et al., "Fuzzy logic with expert judgment to implement an adaptive risk-based access control model for IoT," *Mobile Networks and Applications*, vol. 26, pp. 2545–2557, 2021. <https://doi.org/10.1007/s11036-019-01214-w>.
- [13] O.O. Olusanya, R.G. Jimoh, S. Misra, J.B. Awotunde, "An integrated fuzzy-based decision support model for security risk assessment in healthcare organization," *Heliyon*, vol. 10, issue 13, e33495, 2024. <https://doi.org/10.1016/j.heliyon.2024.e33495>.
- [14] L. Dubchak, Y. Bodyanskiy, A. Sachenko, C. Wolff, N. Vivchar and N. Vasylykiv, "Modified neuro-fuzzy system for online classification of wind turbine blade defects," *IEEE Access*, vol. 13, pp. 166841-166852, 2025. <https://doi.org/10.1109/ACCESS.2025.3612267>.
- [15] S. A. Abdymanapov, M. Muratbekov, S. Altynbek, A. Barlybayev, "Fuzzy expert system of information security risk assessment on the example of analysis learning management systems," *IEEE Access*, vol. 9, pp. 156556-156565, 2021. <https://doi.org/10.1109/ACCESS.2021.3129488>.
- [16] O. Trunov, I. Skiter, M. Dorosh, E. Trunova, M. Voitsekhovska, "Modeling of the information security risk of a transport and logistics center based on fuzzy analytic hierarchy process," in: V. Kazymyr et al. (Eds.), *Mathematical Modeling and Simulation of Systems*, Lecture Notes in Networks and Systems, vol. 1091, Springer, Cham, 2024. https://doi.org/10.1007/978-3-031-67348-1_23.
- [17] O. Trunov, M. Dorosh, I. Skiter, E. Trunova, M. Voitsekhovska, "Simulation of strategies for providing information security of the transport and logistics center based on fuzzy logic methods," in: V. Kazymyr et al. (Eds.), *Mathematical Modeling and Simulation of Systems*, Lecture Notes in Networks and Systems, vol. 1391, Springer, Cham, 2025. https://doi.org/10.1007/978-3-031-90735-7_21.
- [18] D. Vitkus, Z. Steckevicius, N. Goranin, D. Kalibatiene, A. Cenys, "Automated expert system knowledge base development method for information security risk analysis," *International Journal of Computers Communications & Control*, vol. 14, issue 6, pp. 743-758, 2019. <https://doi.org/10.15837/ijccc.2019.6.3668>.
- [19] E.H. Mamdani, "Fuzzy control. A misconception of theory and application," *IEEE Expert*, vol. 9, issue 4, pp. 27-28, 1994.
- [20] O. Sova, A. Shyshatskyi, D. Malitskyi, O. Zhuk, "Development of a complex method for finding a solution for neuro-fuzzy expert systems," *Eastern-European Journal of Enterprise Technologies*, vol. 6, issue 4 (108), pp. 22-31, 2020. <https://doi.org/10.15587/1729-4061.2020.216662>.
- [21] S.I. Nikolenko, *Synthetic Data for Deep Learning*, Springer, Cham, 2021. <https://doi.org/10.1007/978-3-030-75178-4>.
- [22] Y. Li, S. Wang, X. Li, "Research on Rete algorithm improvement strategy based on Spark in big data environment," *The Journal of Supercomputing*, vol. 78, pp. 14225–14243, 2022.
- [23] P. Hitzler, M.K. Sarker (Eds.), *Neuro-Symbolic Artificial Intelligence: The State of the Art*, IOS Press, 2021. <https://doi.org/10.3233/FAIA342>.
- [24] Y. Zdorenko, A. Yanko, M. Myziura, N. Fesokha, "Development of a fuzzy risk assessment model for information security management," *Technology Audit and Production Reserves*, vol. 4, issue 2 (84), pp. 71-79, 2025. <https://doi.org/10.15587/2706-5448.2025.334954>.
- [25] D. Wu, C.-T. Lin, J. Huang, Z. Zeng, "On the functional equivalence of TSK fuzzy systems to neural networks, mixture of experts, CART, and stacking ensemble regression," *IEEE Transactions on Fuzzy Systems*, vol. 28, issue 10, 2019. <https://doi.org/10.1109/TFUZZ.2019.2941697>.
- [26] G. James, D. Witten, T. Hastie, R. Tibshirani, *An Introduction to Statistical Learning: with Applications in R*, second ed., Springer, New York, 2021. <https://doi.org/10.1007/978-1-0716-1418-1>.
- [27] V. Lavrov, A. Dudatyev, and V. Harnaha, "Neuro-fuzzy ANFIS system for assessing the risk of disinformation under information-warfare conditions," *Cybersecurity: Education, Science, Technique*, vol. 4, no. 28, pp. 321–333, 2025. <https://doi.org/10.28925/2663-4023.2025.28.805>.
- [28] I. Nastac, *An Adaptive Retraining Technique to Predict the Critical Process Variables*, TUCS Technical Report 616, Turku, Finland, 2004. http://tucs.fi/publications/view/?pub_id=tNastac04a.



PHD STUDENT OLEKSII TRUNOV graduated from the Educational-Scientific Institute of Electronic and Information Technologies of the Chernihiv Polytechnic National University. Oleksii Trunov works as a Lecturer of the Information Technology and Software Engineering Department in the Chernihiv Polytechnic National University (Ukraine). His main scientific interests

are modeling of information security risks based on fuzzy logic methods, Cyber Security, Cloud technologies of virtualization.



PROFESSOR MARIIA DOROSH is working as a Professor of the Information Technology and Software Engineering Department in the Chernihiv Polytechnic National University (Ukraine). The main scientific interests are modeling and design of intelligent systems; knowledge management; convergen-

ce of project management systems; human factors in information security systems of organizations and projects.



ASSOCIATE PROFESSOR OLENA TRUNOVA graduated from the Physics and Mathematics Faculty of the Chernihiv State Pedagogical University named after T. Shevchenko. She defended the PhD thesis in pedagogical Sciences. Olena Trunova has been working since 2015 at the Chernihiv Polytechnic National University (Ukraine) in the Information Technology and Software Engineering

Department as an Associate Professor. The main scientific interests are Mathematical modeling of systems, e-learning, and the competence approach in education.
