Vol-4271
urn:nbn:de:0074-4271-x

Copyright © 2026 for the individual papers by the papers' authors. Copyright © 2025 for the volume as a collection by its editors. This volume and its papers are published under the Creative Commons License Attribution 4.0 International (CC BY 4.0).



CPITS 2026

Cybersecurity Providing in Information and Telecommunication Systems 2026

Proceedings of the Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2026)

Virtual Event, Kyiv, Ukraine, February 28, 2026.

Edited by

Volodymyr Sokolov [1]
Vasyl Ustimenko [2]
Tamara Radivilova [3]
Mariia Nazarkevych [4]

[1] Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
[2] Royal Holloway, University of London, London, UK
[3] Kharkiv National University of Radio Electronics, Kharkiv, Ukraine
[4] Lviv Polytechnic National University, Lviv, Ukraine

Table of Contents

- Preface
  Summary: There were 71 papers submitted for peer-review to this workshop. Out of these, 24 papers were accepted for this volume.

- On quadratic equations of q-regular tree and their applications to symmetric cryptography 1-10
  Vasyl Ustimenko, *Oleksandr Pustovit*, *Tymofii Svyrydenko*

- Architecture design of ML-based spoofing detection solution 11-20
  Serhii Bulba, *Danylo Yefimov*, *Larysa Kriuchkova*, *Roman Kyrychok*, *Sergiy Obushnyi*

- Verification of video content authenticity and integrity using artificial intelligence
  Pavlo Skladannyi, *Yuliia Kostiuk*, *Dmytro Hnatchenko*, *Igor Goncharenko*, 21-45
  Artem Platonenko

- An integrated AI-supported model for developing digital competence in lifelong learning 46-64
  Svitlana Popereshnyak, *Oleh Kulynich*

- Risk-aware proactive hardening of IoT and cyber-physical networks 65-79
  Tetiana Babenko, *Kateryna Kolesnikova*, *Larysa Myrutenko*, *Oleksandr Kruchinin*

- S3 and S4: Novel hybrid activation functions for deep neural networks 80-97
  Sergii Kavun

- Computational data-processing methods for sustainable enterprise development under energy- and resource-saving constraints 98-108
  Zarina Poberezhna, *Maksym Zaliskyi*, *Khadija Slimani*, *Dmytro Shvets*, *Nataliia Demchenko*

- Developing students' cognitive resistance to information manipulation through critical thinking: Practical aspects 109-121
  Liudmyla Ilich, *Olena Akilina*, *Svitlana Shevchenko*, *Yuliia Zhdanova*

- Well-posedness of boundary-value problems in information security of cyber-physical systems for the bioeconomy 122-135
  Dmytro Levkin, *Ruslana Levkina*, *Yana Kotko*, *Artur Levkin*, *Andriy Dudnik*

- A fuzzy-logic and machine-learning multicriteria model for cybersecurity risk management 136-162
  Yuliia Kostiuk, *Pavlo Skladannyi*, *Dmytro Hnatchenko*, *Nadiia Dovzhenko*, *Halyna Kuchakovska*

- Autonomous intelligent navigation in unknown environments 163-186
  Bohdan Zhurakovskiy, *Sergii Otrokh*, *Anatoliy Makarenko*, *Oleksandr Pliushch*, *Serhij Mamchenko*

- An ISO/IEC 25010-based quality assessment model for distributed ledger technology platforms 187-199
  Serhii Zhebka, *Viktoriia Zhebka*, *Kateryna Nesterenko*, *Ganna Grynkevych*, *Oleksii Cherevyk*

- A method for detecting unauthorized interference in network communications using intelligent traffic analysis 200-215
  Vladyslav Bilous, *Dmytro Bodnenko*, *Oleksandra Lokaziuk*, *Valerii Kozachok*, *Zoreslava Brzhevska*

- A method for implementing security-as-code in relational databases 216-230
  Yaroslava Momryk, *Yuriy Yashchuk*, *Roman Tuchapskyy*, *Ivan Opirskyy*

- Artificial intelligence in higher education: Balancing innovation against ethical risk 231-240
  Tamara Mykheieva, *Nataliia Zaiets*, *Oleksii Holubnychyi*, *Olena Datsun*, *Mariia Patrul*

- Connection context verification as a basis for network access control in zero-trust architectures 241-255
  Roman Syrotynskyi, *Ivan Tyshyk*, *Bohdan Zhurakovskiy*

- Protecting machine-learning datasets with digital watermarking based on modified QR decomposition 256-277
  Oles Hospodarskyy, *Natalia Kukharska*, *Orest Polotai*, *Oleh Harasymchuk*, *Ivan Tyshyk*

- Evaluating speaker verification robustness to neural voice cloning attacks 278-289
  Nazarii Dzhaliuk, *Khrystyna Ruda*, *Dmytro Sabodashko*, *Volodymyr Khoma*

- Development of intelligent intrusion detection systems based on intelligent data analysis methods 290-305
  Serhii Toliupa, *Serhii Buchyk*, *Yurii Shcheblanin*, *Anastasiia Shabanova*, *Andrii Kulko*

- Classical machine learning baselines for synthetic speech detection across modern voice cloning systems 306-317
  Khrystyna Ruda, *Dmytro Sabodashko*, *Volodymyr Povoroznyk*, *Yuriy Khoma*

- Integrating the compartmentalization method into information protection against OSINT reconnaissance (short paper) 318-325
  Valeriia Ivkova, *Ivan Opirskyy*

- Language and conflict: verbal aggression and strategies for mitigation and resolution in online discourse (short paper) 326-334
  Alla Golovnia, *Liana Budanova*, *Yuliia Petrova*

- Accounting for the information threat level in the route-segment cost metric for UAVs in emergency situations (short paper) 335-343
  Viktor Shevchenko, *Yevhen Derevianko*, *Olena Derhylova*, *Volodymyr Shevchenko*, *Yulii Kondratenko*

- A software-defined-radio replay attack on Bluetooth Low Energy devices (short paper) 344-352
  Oleksandr Romaniuk, *Volodymyr Sokolov*, *Andrii Anosov*, *Hennadii Hulak*, *Nataliia Korshun*

2026-09-05: submitted by Volodymyr Sokolov, metadata incl. bibliographic data published under Creative Commons CC0
2026-09-24: published on CEUR Workshop Proceedings (CEUR-WS.org, ISSN 1613-0073) |valid HTML5|

A fuzzy-logic and machine-learning multicriteria model for cybersecurity risk management*

Yuliia Kostiuk[1,*,†], Pavlo Skladannyi[1,†], Dmytro Hnatchenko[2,†], Nadiia Dovzhenko[1,†], and Halyna Kuchakovska[1,†]

[1] *Borys Grinchenko Kyiv Metropolitan University, 18/2 Bulvarno-Kudriavska str., 04053 Kyiv, Ukraine*
[2] *Kyiv State University of Trade and Economics, 19 Kyoto str., 02156 Kyiv, Ukraine*

Abstract

This article presents an intelligent multi-criteria model for managing cybersecurity risks in intelligent information and communication systems. The proposed approach combines fuzzy logic and machine learning methods for decision-making under conditions of incomplete information, linguistic assessments, and a rapidly changing threat environment. The model formalizes the task of selecting an effective set of protective measures, accounting for multiple criteria such as security level, cost, response time, scalability, and others. Fuzzy sets and Mamdani-type inference mechanisms are used to process uncertain data. The machine learning component is based on Extreme Gradient Boosting algorithms and neural networks for building predictive risk models. The model simulates threat scenarios using attack graphs. Algorithms for optimal resource allocation to minimize residual risk have also been developed. The practical implementation of the model was carried out using the Python programming language, the Scikit-learn and TensorFlow libraries, the Flask platform, and integration with Security Information and Event Management (SIEM) systems. The results can be applied in critical infrastructure, cloud environments, and Zero Trust architectures.

Keywords

multi-criteria decision making, cybersecurity risk management, fuzzy logic, machine learning, adaptive security policy, intelligent protection system, information and communication systems.

1. Introduction

The growing complexity and dynamism of cyber threats in the context of the intellectualization of information and communication systems (ICS) necessitate urgent improvements to cybersecurity risk management [1, 4, 8]. Traditional methods based on static risk indicators — such as the product of the probability of an incident and its impact — are unable to adequately reflect modern attack scenarios, contextual factors, and the behavioral dynamics of attackers [1-3, 6]. Lacking flexibility and adaptability, such models fail to ensure effective real-time response, especially in complex and distributed systems.

The key problem lies in the absence of an integrated model that combines cyber threat forecasting, fuzzy information processing, and multi-criteria decision-making to formulate sound defense strategies [5, 7-9]. In today's environment, aspects such as decision explainability, optimal resource utilization, and consideration of interdependencies among system elements are also becoming critically important.

At the same time, an analysis of current approaches reveals a clear scientific gap. First, most existing cyber risk management models treat forecasting, fuzzy evaluation, and the selection of protective measures as isolated tasks, without a unified formalized multi-criteria decision space. Second, the adaptability of such models often boils down to local updates of individual parameters and does not ensure coordinated optimization across multiple criteria (risk, resources, response time, scalability). Third, the interpretability of decisions and their integration into Zero Trust and SIEM frameworks are largely lacking a formal model-level description, which complicates the verifiability and reproducibility of results.

* *CPITS 2026: Cybersecurity Providing in Information and Telecommunication Systems, February 28, 2026, Kyiv, Ukraine*
* Corresponding author.
† These authors contributed equally.
y.kostiuk@kubg.edu.ua (Y. Kostiuk); p.skladannyi@kubg.edu.ua (P. Skladannyi); hnatchenko@knute.edu.ua (D. Hnatchenko); n.dovzhenko@kubg.edu.ua (N. Dovzhenko); h.kuchakovska@kubg.edu.ua (H. Kuchakovska)
0000-0001-5423-0985 (Y. Kostiuk); 0000-0002-7775-6039 (P. Skladannyi); 0000-0002-6584-4525 (D. Hnatchenko); 0000-0003-4164-0066 (N. Dovzhenko); 0000-0002-4555-896X (H. Kuchakovska)
© 2026 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073
published 2026-09-24

CEUR-WS.org/Vol-4271/paper10.pdf

Despite the widespread use of RBAC (Role-Based Access Control) and ABAC (Attribute-Based Access Control) models, they remain insufficiently effective in a dynamic cyber environment [1, 3, 6]. In particular, these approaches do not account for multi-criteria decision-making and cannot adapt to changes in the risk profile in real time.

Most existing risk management models are based on static metrics (e.g., CVSS or DREAD), which do not account for access context, the temporal dynamics of incidents, or the level of trust in the subject [4]. As a result, such systems exhibit low flexibility, a high number of false positives, and an inability to respond to complex, combined attacks [7, 10, 12]. Furthermore, the lack of support for adaptive security rule update policies and insufficient integration of explainability mechanisms (e.g., XAI) in traditional approaches limit their applicability in intelligent information and communication systems.

The research poses the following scientific question: Is it possible to construct a unified multi-criteria cybersecurity risk management model that simultaneously enables the prediction of threat scenarios, the fuzzy evaluation of uncertain/linguistic factors, and the well-founded selection of protective measures, while accounting for limited resources and real-time adaptability requirements? The working hypothesis is that integrating gradient boosting, fuzzy inference, and attack graphs within a joint optimization framework reduces residual risk and improves decision stability compared to static metrics and isolated intelligent models.

The aim of the study is to develop a multi-criteria cybersecurity risk management model that combines fuzzy logic methods, machine learning algorithms, and threat scenario modeling to support adaptive decision-making in intelligent ICS [6, 11, 13, 16]. The model should minimize residual risk, be flexible in responding to environmental changes, and allocate resources efficiently under conditions of uncertainty.

The scientific novelty of this work lies in the formalization of the risk management task as a multi-criteria optimization problem with fuzzy constraints, the construction of a hybrid risk assessment model based on the gradient boosting algorithm and fuzzy inference [3, 6], the application of fuzzy hierarchy analysis for the selection of protective measures [12], as well as in the use of attack graphs for dynamic forecasting of threat behavior [18].

The practical significance of the research lies in the potential to implement the developed model within information security management systems, Zero Trust architecture platforms, cloud environments, SIEM solutions, and corporate ICS [19, 21, 23, 27]. The use of the proposed approach will help increase cyber resilience, reduce protection costs, and shorten incident response times.

The main scientific contributions of this work are as follows:

- a formalized multi-criteria risk management model with fuzzy constraints is proposed;
- a hybrid approach to risk assessment based on a combination of gradient boosting and fuzzy logic inference has been developed;
- attack graphs have been integrated for dynamic forecasting of threat scenarios;
- a mechanism for the adaptive selection of protective measures, taking into account limited resources, has been proposed;
- ensured the explainability of decisions made and the possibility of integration with SIEM and Zero Trust architectures.

2. Literature review

The increasing complexity and dynamics of cyber threats in the context of the intellectualization of information and communication systems necessitate modern approaches to risk management using multi-criteria analysis, fuzzy logic, and machine learning. Currently, there is active development of adaptive risk assessment models focused on accounting for context, uncertainty, and the interdependence of information infrastructure components.

Atlam et al. [1] conducted a systematic review of risk-based access control models, emphasizing the need to use contextual attributes and dynamically update security policies. In turn, Jazairy et al. [2] proposed a concept for the multi-level integration of risk management strategies across supply chains, emphasizing the importance of adaptive interactions among system agents. The study by Barlybayev et al. [3] presents a flexible risk management model that combines an ontological approach with machine learning and logical-linguistic analysis.

A significant portion of the scientific literature is devoted to the use of fuzzy logic in conditions of non-statistical uncertainty. In particular, Bakhtavar et al. [4] generalized the application of fuzzy

cognitive maps for systematic risk analysis, demonstrating their effectiveness in identifying interdependencies between risk events. Kerimkhulle et al. [5] adapted fuzzy logic methods to risk assessment in industrial Internet of Things systems, which is particularly relevant for critical ICS.

Modern approaches to risk modeling actively integrate machine learning. Hamid and Rahman [6] summarized the capabilities of artificial intelligence, particularly deep learning, in cyber risk management, with an emphasis on dynamic incident classification. Zadeh et al. [7] proposed a framework for quantitative probabilistic analysis to support decision-making in the risk minimization process.

The literature has paid particular attention to the explainability of machine learning models in cybersecurity tasks. For example, Islam et al. [8] developed a dynamic intelligent risk management system that combines predictive models with interpretation mechanisms (SHAP, LIME), enabling informed real-time decision-making. The work by Katnapally et al. [9] presents an implementation of a neural network-based risk assessment model for ERP systems with large volumes of data, which reduces incident response time. Additionally, Kozhukhivskyi and Kozhukhivska [10] proposed a fuzzy risk assessment model for enterprise resource planning systems that accounts for fuzziness in both input data and decision-making criteria.

Despite significant achievements, most existing solutions either focus on individual aspects of the problem, such as threat classification or the selection of protective measures [7, 24], or fail to integrate forecasting, fuzzy assessment, and multi-criteria decision-making within a single context-adaptive environment [3, 5, 8, 12]. Furthermore, the problem of the optimal allocation of limited resources in the case of multiple and conflicting objectives — minimizing residual risk, the cost of implementing measures, and response time — has not been sufficiently studied [6, 11, 13, 29-30, 33]. Thus, the results of the literature review allow us to identify a research niche for developing a comprehensive cybersecurity risk management model that combines fuzzy logic methods, machine learning algorithms, and dynamic threat modeling in the context of intelligent information and communication systems.

3. Research Methods

Within the scope of this study, a multi-criteria cybersecurity risk management model was developed that combines fuzzy logic and machine learning for effective decision-making under uncertainty [3, 5-6]. To process fuzzy, linguistic, and partially defined input data, mechanisms of fuzzy set theory and Mamdani fuzzy inference were applied [4, 5, 12]. The predictive risk model was constructed using a gradient boosting algorithm, which enables the modeling of complex nonlinear relationships between security parameters and risk assessment [6, 30, 32]. For decision-making under multiple criteria, including residual risk level, cost, response time, and scalability, a fuzzy-logic-based hierarchical analysis was used [4-5, 12]. Threat modeling is implemented using attack graphs, which allow the logic of malicious action scenarios and their probabilistic characteristics to be taken into account [11, 29]. The optimal selection of protective measures is formalized as a multi-criteria fuzzy mathematical programming problem that accounts for the acceptable risk level and limited resources [3, 13]. The system architecture is described using structural and flow modeling techniques, including data flow diagrams and functional blocks [33]. The prototype was implemented in Python using the Scikit-learn, TensorFlow, FuzzyLogic, and Flask libraries, which ensures integration with the information system [6, 21] and risk assessment scenarios in a dynamic environment.

To demonstrate the advantages of the proposed multi-criteria cybersecurity risk management model, a comparative analysis was conducted with existing approaches, including classical (DREAD, CVSS) [2, 28], context-oriented ones (RAdAC), as well as intelligent models based exclusively on machine learning or fuzzy logic [3, 6-8, 34]. The comparison considered key characteristics such as assessment accuracy, adaptability to environmental changes, scalability, decision-making time, and compliance with the Zero Trust concept.

As shown in Table 1, the proposed model demonstrates a better balance between accuracy, adaptability, and alignment with modern security concepts. Unlike static models, it enables flexible decision-making based on a set of criteria formalized in both quantitative and fuzzy forms, a capability that is particularly important for intelligent information and communication systems.

Table 1.
Comparative analysis of cybersecurity risk assessment models

Model	Accuracy	Adaptability	Scalability	Decision Time	Zero Trust Compliance
Proposed Hybrid Model	High	High	High	Moderate	Full
DREAD	Low	Low	Low	Fast	Partial
CVSS	Medium	Low	Medium	Fast	No
RAdAC	Medium	Medium	Medium	Slow	Partial
ML-based only (XGBoost)	High	Medium	High	Fast	Depends
Fuzzy-only model	Medium	High	Medium	Moderate	Partial

It should be noted that the proposed model is oriented toward intelligent ICSs in which telemetric data and incident history are available, sufficient for training the predictive component. The quality of risk assessment depends on the completeness and representativeness of the training samples, as well as on the correctness of the initial construction of fuzzy rules and membership functions during the initialization stage. Further research should focus on the automated adaptation of fuzzy rules, reducing sensitivity to class imbalance in incidents, and scaling the model for very large, distributed environments.

4. Presentation of the Main Material

Within the scope of this study, the task of cybersecurity risk management is considered as a multi-criteria decision-making problem under conditions of uncertainty and dynamic changes in threats. The input data consists of a set of contextual features, asset characteristics, environmental parameters, and threat scenarios obtained from the telemetry of the information and communication system. The controlled variables are the selection and configuration of protective measures. The goal of management is to minimize residual risk while simultaneously accounting for implementation costs, response time, and limited system resources.

The risk management process is formalized as a multi-criteria optimization problem that simultaneously accounts for the level of residual risk, the costs of implementing protective measures, response time characteristics, and scalability requirements. Under conditions of fuzzy uncertainty in the input parameters, the objective function is defined as a weighted composition of criteria, where the weighting coefficients are determined using fuzzy hierarchy analysis methods and adapted according to the current threat context.

The current state of cybersecurity risk management systems in intelligent information and communication systems demonstrates the inadequacy of single-criterion models focused exclusively on minimizing costs or risk [1-2, 7-8]. The urgency of improving cybersecurity effectiveness requires the development of multi-criteria models that take into account not only the level of residual risk but also such important aspects as response time, scalability, costs, impact on system performance, technical compatibility, and threat context.

Based on an analysis of modern approaches to risk management, it can be argued that it is critically important to develop models and algorithms capable of operating under conditions of incompleteness, uncertainty, rapidly changing attack scenarios, and complex dependencies among system agents [24, 29-30]. Particular attention should be paid to systems designed to maintain a guaranteed level of residual risk throughout the ICS's operational life, with dynamic adjustment of risk targets depending on context.

The diagram in Figure 1 illustrates the architecture of an intelligent cybersecurity risk management system and the interaction logic of its key modules: the input data collection subsystem, the machine learning module (XGBoost, LSTM), the fuzzy decision-making module based on Fuzzy AHP, the residual risk assessment mechanism, as well as the feedback loop with SIEM and the adaptive real-time updating of security policies.

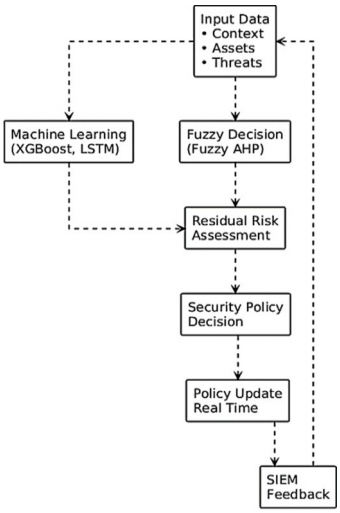


Figure 1: Architecture of an intelligent multi-criteria cybersecurity risk management system integrating machine learning, fuzzy logic, and SIEM feedback

The primary risk management tool is to reduce medium- and high-risk levels to an acceptable threshold at which their consequences can be controlled or mitigated [6]. This approach is implemented by selecting a set of protective measures that optimally balances numerous conflicting criteria [3-4]. Single-criterion mathematical models, formulated as optimization problems, typically do not account for the multiplicity of requirements for modern cryptographic and software protection systems (CSPs), nor for the fuzzy nature of the input information [5, 10]. The risk management model is formulated as a multi-criteria optimization problem [6-8, 11]:

$$Q(X)=\{q_1(X),q_2(X),\ldots,q_m(X)\} \rightarrow ext_{X\in D}, G(X)\leq 0, \quad (1)$$

where $X \in D$ is the solution vector describing the selected set of measures and parameters of the protection system, $D \subset R^n$ is the set of feasible solutions satisfying all technical, financial, and risk-oriented constraints, $q_1(X), i=1,\ldots,m$ are private criteria for evaluating protection quality (e.g., residual risk level, cost, response time, scalability, implementation complexity, etc.), $Q(X)$ is objective vector (vector of performance functions), *ext* is an extremum operator (min or max, depending on the type of criterion), $G(X)\leq 0$ — system of constraints, in particular: $g_1(X)\leq R_{res}^{max}$ is constraint on the permissible level of residual risk, $g_2(X)\leq C_{max}$ is constraint on total costs, $g_3(X)\leq T_{max}$ is constraint on system response time.

In cases where some of the criteria are informal or represented as linguistic variables, it is advisable to use fuzzy membership functions [4, 5, 12]. For each criterion $q_i(X)$, a corresponding fuzzy evaluation function is introduced:

$$\mu_{(q_i)}(X)=\frac{(q_i(X)-q_i^{min})}{(q_i^{max}-q_i^{min})}, \mu_{q_i}(X)\in[0,1] \quad (2)$$

where $\mu_{q_i}(X)$ is the degree of criterion satisfaction q_i (membership function), which allows formalizing fuzzy expert information, for example: “low risk,” “high efficiency,” “sufficient compatibility” [5, 13], q_i^{min}, q_i^{max} are the minimum and maximum permissible values of the criterion, respectively, $q_i(X)$ is the criterion evaluation for a given set of solutions X. This approach allows for the formalization of fuzzy expert information, such as: “low risk,” “high efficiency,” “sufficient compatibility.”

Given the growing complexity of cyber threats and the interdependence of information in intelligent information and communication systems, there is a need to develop adaptive cybersecurity risk management models [14]. Based on the concept of multi-criteria decision-making (MCDM), this paper proposes a dynamic model for assessing and managing cybersecurity risks using fuzzy logic, the pairwise comparison method, machine learning, and situational analysis [3-4, 6, 8, 19-20]. The objective function takes the form of a multidimensional vector criterion:

$$Q(X)=\begin{cases} q_1(X)=R_{res}(X)-\textit{residual risk (to be minimized)} \\ q_2(X)=C_{total}(X)-\textit{total cost (to be minimized)} \\ q_3(X)=T_{resp}(X)-\textit{response time (to be minimized)}, \\ q_4(X)=\eta(X)-\textit{security level coefficient (to be maximized)} \\ q_5(X)=\mu_{comp}(X)-\textit{compatibility level (to be maximized)} \end{cases} \quad (3)$$

where X is the vector of input parameters for the ICS (assets, threats, vulnerabilities, protection resources), R_{res} is the residual risk after implementing measures, C_{total} is the total cost of implementation and maintenance, T_{resp} is the expected average response time, $\eta(X)$ is the integrated security assessment, μ_{comp} is the degree of technical compatibility.

In the event of environmental changes, such as the emergence of new attack vectors or a decrease in the effectiveness of existing measures, the model must re-optimize under modified constraints [8, 24-27, 30]. This approach meets the requirements of adaptive cyber defense and enables reactive updates to security policies based on real-time risk assessment.

Residual risk model [6, 13]:

$$R_{res}=R_{init}\cdot(1-E) \quad (4)$$

where R_{init} is the initial risk without protective measures, $E\in[0,1]$ is the effectiveness of the implemented protective mechanisms,R_{res} is the residual risk (to be minimized). The model determines the amount of risk remaining after the implementation of the protection system. It serves as a fundamental element in decision-making regarding the need for additional measures.

Multi-criteria optimization objective function [4, 28]:

$$Q(X)=[R_{res}(X),C_{total}(X),T_{resp}(X),\eta(X),\mu_{comp}(X)] \quad (5)$$

where $R_{res}(X)$ is residual risk (to be minimized), $C_{total}(X)$ is total costs of implementing the ISMS (to be minimized), $T_{resp}(X)$ is average incident response time (to be minimized), $\eta(X)$ is security coefficient (to be maximized), $\mu_{comp}(X)$ is compatibility with existing infrastructure (to be maximized). A vector function is used to find a Pareto-optimal solution, i.e., one where it is impossible to improve one criterion without worsening another.

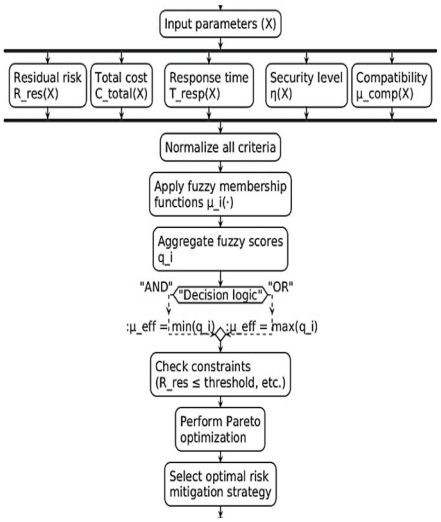


Figure 2: Diagram of the construction of a multi-criteria risk management model

The flowchart in Figure 2 illustrates the sequence of steps in developing a multi-criteria cybersecurity risk management model, including the assessment of key criteria (residual risk, cost, response time, security level, compatibility), the processing of fuzzy assessments, and the search for a Pareto-optimal solution.

Fuzzy risk membership function:

$$\mu_R(r)=\begin{cases} 0. & r\le R_{min} \\ \dfrac{r-R_{min}}{R_{max}-R_{min}}, & R_{min}<r<R_{max}, \\ 1, & r\ge R_{max} \end{cases} \tag{6}$$

where $\mu_R(r)$ is the degree of membership of the value$r$ in the "high risk" set, r is the current risk value, R_{min}, R_{max} are the boundaries of the fuzzy risk region. The formula allows for handling fuzziness and uncertainty in risk assessment, for example, from expert sources.

The selected set of criteria$\{q_1(X), q_2(X), \ldots, q_n(X)\}$ is the result of an analytical review of cybersecurity system requirements and is based on the principles of completeness and independence [6, 11, 13]. Completeness means that every important aspect of the system's effectiveness is represented by at least one criterion, ranging from technical security to the soundness of decision-making. The independence of the criteria is confirmed by the absence of linear or functional dependencies between them, which precludes duplication or bias in the results [7]. For the mathematical representation of the model, we use a generalized metric space of performance Q, in which each alternative X is projected as an image vector:

$$Q(X)=[q_1(X), q_2(X), \ldots, q_n(X)]. \tag{7}$$

This is a vector of criteria for a specific alternative X, which shows its position in the n-dimensional efficiency space Q. Each component of the vector is the value of the alternative according to the corresponding criterion, where each $q_i(X)$ is a function that evaluates the alternative X according to a specific criterion. In the context of cybersecurity, such criteria may include: $q_1(X)$ — level of technical security, $q_2(X)$ — scalability, $q_3(X)$ — implementation cost, $q_4(X)$ response speed, $q_n(X)$ — level of decision validity (confidence).

Each criterion $q_i(X)$ is mapped to a fuzzy set via a membership function $\mu_{q_i}(X)\in[0,1]$, which indicates the extent to which an alternative X meets the desired level of that criterion: $\mu_{q_i}(X)=1$ full compliance,$\mu_{q_i}(X)=0$ full non-compliance, and intermediate values partial compliance. This is particularly important for qualitative or linguistic assessments, such as "high security," "low cost," etc. [4-5]. The aggregate performance function is defined as $\mu_{eff}=\min\limits_i \mu_{q_i}(X)$ for AND logic, where the alternative X is evaluated based on the worst criterion, which is appropriate when all requirements are met simultaneously (strict approach), or as $\mu_{eff}=\max\limits_i \mu_{q_i}(X)$ for OR logic, where the best criterion is considered, corresponding to a flexible approach in cases of partial compliance. In this space, the criterion functions are defined either as fuzzy sets (for qualitative indicators) or as metrics (for quantitative indicators). This allows the use of fuzzy logic mechanisms to construct an aggregated performance function:

$$\mu_{eff}=min_i\ \mu_{q_i}(X)(for\ AND\ logic)\ OR\ \mu_{eff}=max_i\ \mu_{q_i}(X)(for\ OR\ logic) \tag{8}$$

The given formulas allow formalizing the decision-making process in situations of uncertainty and multi-criteria decision-making. Instead of a simple average or weighted sum, fuzzy logic is used, which better reflects real-world situations in the context of cyber risk [3, 7, 28]. Thus, the proposed system of criteria forms a formally defined decision-making space suitable for fuzzy multi-criteria optimization.

Formal verification of the model is based on the consistency property of the aggregated performance function in the fuzzy space Q. In particular, when using AND logic, the model guarantees convergence to the worst-case criterion, which is consistent with the principle of conservative decision-making [19-20, 25-27]. Additionally, the accuracy of the decisions made was verified using XAI analysis (SHAP), which confirmed the stability of the influence of key features with an average confidence score exceeding 0.85.

In addition, an analysis of the monotonicity of the aggregated function was conducted, which showed that as the level of threats or losses increases, the value of the integral risk does not

decrease, which satisfies the formal requirements for the model's validity. The stability of the results was confirmed by athrougheries of scenario experiments in,which the weighting coefficients and fuzzy inference parameters were varied without a sisignificantlyecting the final decisions. The results obtained demonstrate the model's robustness to input data noise and partial contextual uncertainty. Thus, the proposed approach can be regarded as a formally consistent and interpretable decision support mechanism for cybersecurity risk management tasks.

The graph in Figure 3 illustrates three triangular membership functions: Low, Medium, and High, which are widely used in fuzzy logic for the linear mapping of fuzzy variables. They are defined by simple conditions on the input value and allow for the effective modeling of fuzzy sets in a multi-criteria environment.

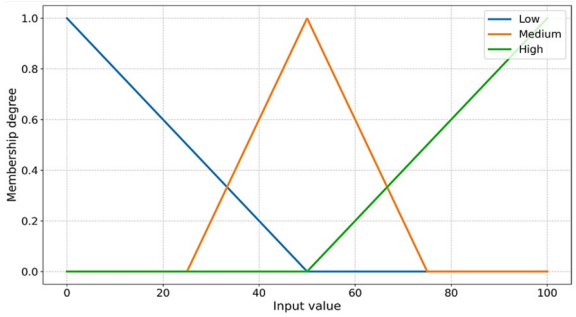


Figure 3: Triangular membership functions

For comparison with linear triangular functions, it is advisable to consider alternative forms of defining fuzzy sets. In particular, in practical risk management tasks, the smoothness of transitions between linguistic levels and the reduction of abrupt changes in membership degree play an important role. That is why the next step in the analysis is the use of Gaussian functions, which better reflect the continuous nature of many real-world processes. This allows us to assess the impact of the choice of membership function form on the sensitivity and stability of fuzzy inference.

The graph in Figure 4 shows three Gaussian membership functions with smooth, symmetric shapes. They provide a continuous, smoothed representation of the degree of membership in fuzzy sets, which is useful for fuzzy models that are highly sensitive to changes in input data.

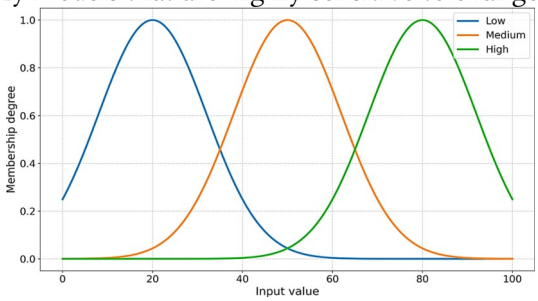


Figure 4: Gaussian membership functions

Reactive policy update function:

$$\Delta P = a \cdot \left(R_{res}^{curr} - R_{res}^{thresh} \right), \tag{9}$$

where ΔP is the security policy update threshold, a is the system sensitivity coefficient, R_{res}^{thresh} is the threshold value for acceptable risk, R_{res}^{curr} is the current residual risk. The function determines the need to update policies following a threat assessment; that is, when the risk exceeds the acceptable level, the system automatically initiates a policy update.

This approach ensures a proportional system response to rising threat levels without abrupt or excessive changes to the security configuration. The sensitivity coefficient aaa allows you to adjust the response intensity based on asset criticality and system resilience requirements. For values of, policy updates are not performed, which prevents unnecessary intervention and reduces operational costs. Thus, the reactive function serves as a formalized mechanism for the dynamic adaptation of security policies in a changing risk environment.

The values obtained using Gaussian membership functions allow for the formation of a smoothed estimate of residual risk without sharp jumps when input parameters change. Such a continuous interpretation of risk is critical for the correct activation of adaptive response mechanisms in the security system. Based on this, a reactive policy update function is introduced, which formalizes the relationship between the risk level and the intensity of management actions.

The graph in Figure 5 illustrates the dependence of the scale of policy updates on the extent to which the current residual risk exceeds the permissible threshold. The linear relationship shows that the greater the risk exceeds the threshold, the more extensive the update should be.

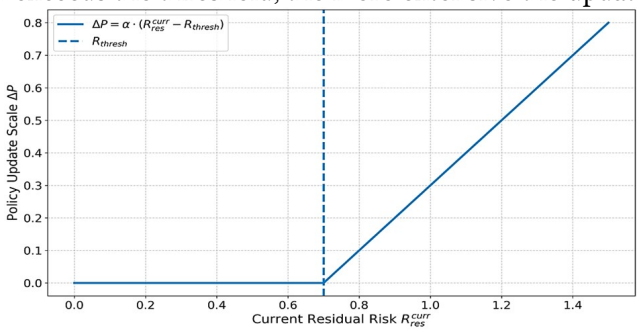


Figure 5: Reactive function for updating security policies

Loss model for incorrect response:

$$L = \lambda_1 \cdot FP + \lambda_2 \cdot FN \tag{10}$$

where FP is the number of false positives (a legitimate action is considered an attack), FN is the number of false negatives (the attack was not detected), λ_1, λ_2 are the loss weighting coefficients for each type of error. The model helps minimize the cost of errors and select the optimal threshold values for incident detection.

The proposed loss model allows for a quantitative assessment of the trade-off between different types of errors in an incident detection system. The selection of weight coefficients λ_1, λ_2 reflects security priorities and the acceptable level of risk for a specific information and communication system.

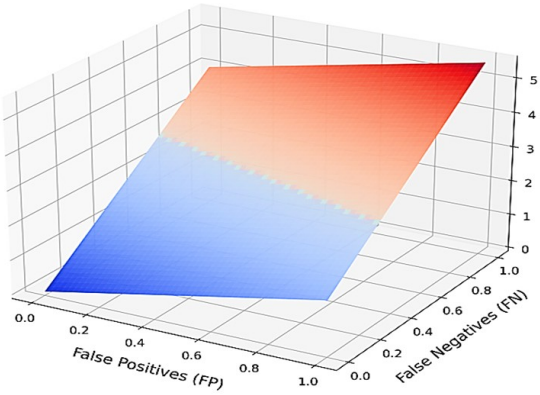


Figure 6: Loss function surface for false responses

The three-dimensional surface (Figure 6) depicts the total loss LLL as a function of the number of false positives and false negatives. The higher the FN, the steeper the increase in loss, illustrating the importance of reducing missed attacks.

Model for assessing the relevance of the threat context:

$$C_{rel} = \sum_{i}^{nw} \cdot f_i(x) \tag{11}$$

where $f_i(x)$ is a function of i^{th} contextual feature (time, IP, attack type, user, etc.), w_i are the weights of the contextual parameters, C_{rel} is the generalized threat importance/relevance index. The model allows for prioritizing a threat or request depending on the context.

The diagram (Figure 7) shows contextual features (time, user role, IP, etc.), their individual scores, and weights. The dotted line represents the calculated generalized relevance index, which determines the threat priority.

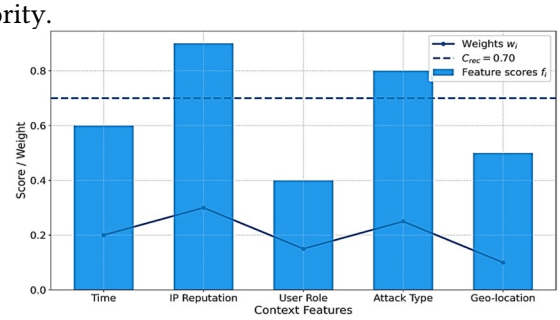


Figure 7: Assessment of threat context relevance

Bayesian event confidence model:

$$T(E)=\frac{(P(E|safe)\cdot P(safe))}{(P(E))} \tag{12}$$

where $T(E)$ is the event confidence score E, $P(E|safe)$ is the probability of the event occurring if it is safe, $P(safe)$ is the prior probability of a safe state, $P(E)$ is the overall probability of the event [19, 20]. The model allows calculating how likely it is that a request is safe, based on prior data. This Bayesian approach provides a formalized combination of prior knowledge and current observations in the process of confidence assessment. The value of `$T(E)$` can be dynamically updated as the volume of data grows, which increases the model's adaptability to changes in user behavior or the environment. This allows the confidence score to be used as an input parameter for subsequent decision-making regarding authorization, incident response, or security policy adjustments.

Risk prediction based on fuzzy regression:

$$\hat{R_{t+1}}=a\cdot\hat{R}_t+b\cdot\Delta Threat(t)+c. \tag{13}$$

where $\hat{R}_t$ is the predicted risk at time t, $\Delta Threat(t)$ is the change in threat level, a, b, c are the model parameters that are tuned, and $\hat{R}_{t+1}$ is the risk prediction for the next time step [19, 25]. The formula allows predicting the future risk level for proactive response. This approach combines the inertial properties of risk with the dynamic impact of changing threats in the environment. The parameter a reflects the degree of dependence of future risk on the previous state, while the coefficient b characterizes the model's sensitivity to the escalation of threats. An additional shift ccc allows for the consideration of the background risk level caused by the characteristics of the ICS. Thus, the fuzzy regression model provides a basis for proactive security management through the timely adjustment of policies and protective measures.

Assessment of the overall effectiveness of the IS [10, 13]:

$$E_{sys}=\frac{(\eta(X))}{(C_{total}(X))}\cdot\mu_{comp}(X), \tag{14}$$

where $\eta(X)$ security, $\mu_{comp}(X)$ compatibility with ICS, $C_{total}(X)$ implementation costs. This is an aggregated metric that allows one to assess the feasibility of implementing a particular solution from an efficiency standpoint.

Adaptive access function (decision rule):

$$Access_{Granted}=\begin{cases}1, if\ R_{res}<\tau \wedge T(E)>\delta\\ 0, \quad otherwise\end{cases} \tag{15}$$

where R_{res} is the residual risk,τ is the dynamic risk threshold, $T(E)$ is the confidence metric for the environment or context,δ — is the minimum acceptable confidence level [19, 20, 25]. A decision to allow or block a request is made based on the risk and confidence in the event.

When developing an intelligent adaptive cyber defense system, it is important to consider the temporal dynamics of attacks, risk forecasting, learning from experience in interacting with threats, and trust-based context assessment [19]. To this end, the integration of several mathematical models covering various aspects of decision-making in an unstable environment is proposed [11, 12, 26]. The system's behavior under conditions of varying security levels is described by a model based on a first-order discrete Markov chain:

$$P_{ij}(t)=P[S_{(t+1)}=j \mid S_t=i] \tag{16}$$

where $S_t \in \{S, C, R\}$ is the system state (secure, compromised, recovering) at time t: Secure (S) the system is functioning securely, Compromised (C) a breach has been detected, Recovering (R) recovery is in progress, $P_{ij}(t)$ is the probability of transition from state i to j at time t. This approach allows us to analyze how defensive or offensive actions affect changes in the system's state over time [16-17, 27]. Matrix form:

$$P(t)=\begin{bmatrix} p_{SS} & p_{SC} & p_{SR} \\ p_{CS} & p_{CC} & p_{CR} \\ p_{RS} & p_{RC} & p_{RR} \end{bmatrix}, \tag{17}$$

where each element p_{ij} represents the probability of transitioning from state i to state j at time step t: p_{SS} represents the probability of remaining in a secure state, p_{SC} represents the probability that the system will be compromised from a secure state, p_{SR} represents the probability of transitioning from a secure state to a recovery state (e.g., due to a scheduled update), p_{CS} represents the probability of recovering after an attack, p_{CC} represents the probability of remaining in a compromised state (e.g., if no measures are taken), p_{CR} is the probability of transitioning from an attack to recovery, p_{RS} is the probability of full system recovery,p_{RC} is the probability of re-compromise during recovery (e.g., due to a repeat attack),p_{RR} is the probability of remaining in the recovery state for another cycle [16, 17, 29]. The model allows for assessing the dynamics of changes in the system's cybersecurity status, predicting recovery or threatening transitions, and adjusting security policies accordingly.

The diagram in Figure 8 illustrates a Markov model of transitions between the security states of an information system: Secure (S) is a normal operation, Compromised (C) is a security breach, Recovering (R) is a recovery. The transition directions are labeled with probabilities that characterize state changes resulting from attacks or response measures.

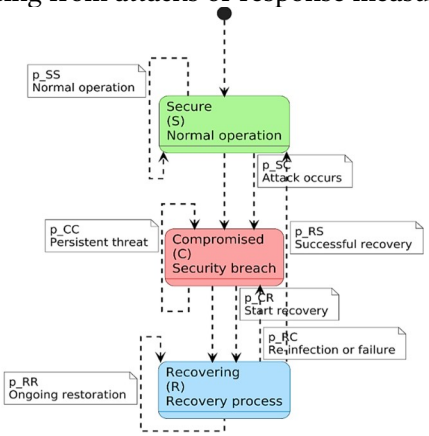


Figure 8: Security transition diagram (S ⟶ C ⟶ R)

Each row of the matrix describes the probability distribution of transitions from one state to another, thus:

$$\sum_j p_{ij}=1,\ \forall i \in \{S, C, R\}. \tag{18}$$

The matrix allows us to analyze the dynamics of security state changes and calculate the probability of reaching the desired state (e.g., returning to a secure state) in a few steps:

$$P^n(t)=P(t)^n \tag{19}$$

where n is the number of steps (cycles), P^n is the transition matrix through n states. The model is ideally suited for describing the behavior of ICS under conditions of periodic attacks, recovery, and adaptive policy updates [16, 29]. It can be extended to a semi-autoregressive model if it is important to account for the influence of history on subsequent transitions.

To predict the likely development of risks based on historical data, it is advisable to use a recurrent neural network with long-term short-term memory:

$$\hat{R_{t+1}}=f_{LSTM}(R_t, R_{t-1}, \ldots, R_{t-k}) \tag{20}$$

where $\hat{R}_{t+1}$ is the predicted risk level at the next time step, $R_t, \ldots, R_{t-k}$ are the observed values for the previous time steps, and f_{LSTM} is the LSTM-based prediction function [20, 25]. This enables the system to proactively respond to rising risk trends. This enables the system to proactively respond to rising risk trends (Figure 9).

Figure 9 illustrates the dynamics of cyber risk level forecasting over time using the LSTM model. Observed risk values are denoted by a solid line, and predicted values by a dashed line. The model allows for the assessment of future risk behavior based on historical data, which serves as the foundation for proactive response in intelligent cyber defense systems.

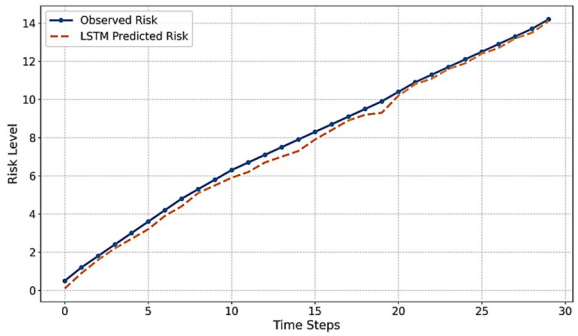


Figure 9: Risk forecasting trend based on the LSTM model

An adaptive system must be able to learn from its interactions with the environment. In this context, reinforcement learning is applied, specifically the "Q" method:

$$Q(s,a) \leftarrow Q(s,a)+a[r+\gamma\, max_{\acute{a}} Q(\acute{s},\acute{a})-Q(s,a)], \tag{21}$$

where $Q(s,a)$ is the utility function for action a in state s, $a \in (0,1)$ is the learning rate, r is the instantaneous reward for action a, $\gamma \in (0,1)$ is the discount factor for future benefits, and $\acute{s}$ is the new system state after executing the action [26]. The model allows the system to learn over time to make the best decisions in terms of risk reduction and resource optimization, even in cases where the threat context is dynamic and unpredictable.

A statistical model is used to assess trust in a source, user, or scenario:

$$T(E)=\frac{a_E}{(a_E+\beta_E)} \tag{22}$$

where a_E is the number of positive interactions, β_E is the number of negative interactions, $T(E)$ is the confidence value. The model is used in adaptive access policies and in the formation of response scenarios [27-28, 31, 34]. The combined use of Markov processes, LSTM, Q-learning, and

the beta distribution forms a flexible and self-learning system capable of responding to environmental changes in real time, adapting security policies, and prioritizing well-founded decisions even in situations of uncertainty [24-27]. This approach meets modern requirements for Zero Trust, dynamic risk assessment, and active countermeasures against cyber threats.

The diagram (Figure 10) illustrates the interaction between system components during the access decision-making process. The user's request is processed by the risk assessment module, which calculates the residual risk R_{res}. The result is sent to the XAI module to generate an explanation, after which the Policy Engine makes a decision, taking into account the risk level and the task's criticality $T(E)$. The final decision (approval or denial) is sent to the user.

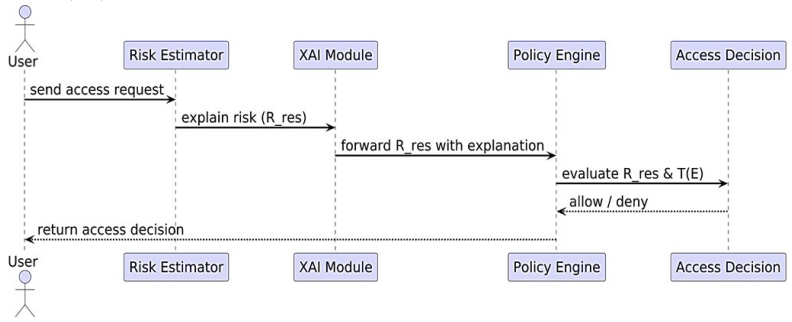


Figure 10: Access decision-making sequence

The proposed mathematical model formalizes the process of multi-criteria decision-making in cybersecurity, accounting for not only technical indicators but also qualitative aspects, including the threat context, the interpretation of expert assessments, and system flexibility [12, 30]. It provides a foundation for implementing intelligent protection systems capable of adapting to environmental changes and making informed decisions even under conditions of uncertainty [19, 34].

The risk of a cyber incident is modeled as a function [13, 28, 35]:

$$y(t)=f(x_1(t),x_2(t),x_3(t)) \tag{23}$$

where $x_1(t)$ is the probability of a threat materializing at a given time t, $x_2(t)$ is the system's vulnerability level, $x_3(t)$ is the potential damage, $y(t)$ is the risk level (or control influence) that must be minimized. This functional formulation allows for the integration of key risk components into a single formalized model. The time dependence of the arguments t ensures that the dynamics of threats, changes in the state of vulnerabilities, and variations in potential losses are taken into account. This creates a foundation for building adaptive risk management algorithms to minimize $y(t)$ in real time.

All input and output parameters are treated as linguistic variables, which are formalized using membership functions [12]. For example, fuzzy rules take the form: If the probability of a threat is high AND the loss is large, THEN the risk is high; If the probability is high AND the loss is large, THEN the risk is significantly reduced. The assessment model is constructed as a system of fuzzy logic rules of the type:

$$IF\ x_1\ high\ \text{AND}\ x_3\ large\ ,THEN\ y\ is\ high \tag{24}$$

which provides decision-making logic based on expert knowledge and adaptation to the current state of the system. This rule-based approach enables the formalization of expert knowledge in a comprehensible, interpretable form. Furthermore, the use of linguistic variables ensures flexible adaptation of the model to uncertainty and incompleteness of input data during the risk assessment process.

The fuzzy inference rule map in Figure 11 depicts a generalized Mamdani-type logical inference system for determining the risk level based on two input factors: threat level and potential damage. Each cell of the matrix corresponds to a rule of the form: IF Threat is X AND Damage is Y THEN Risk is Z, where X, Y, Z are fuzzy linguistic variables (Low, Medium, High). This enables the easy interpretation and formalization of expert knowledge about the impact of various scenarios on risk levels.

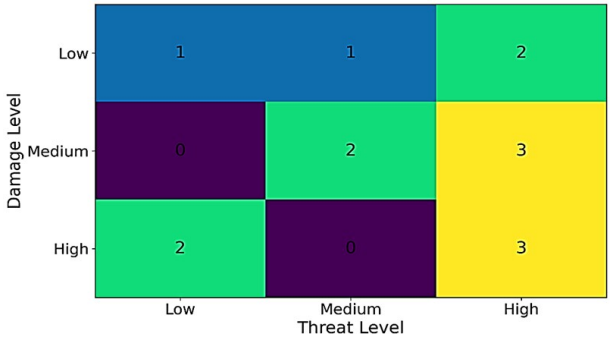


Figure 11: Fuzzy inference rule map for risk assessment

Figure 12 shows a three-dimensional fuzzy inference surface that illustrates how the risk level depends on two linguistic input variables: threat level and potential damage. The surface is constructed based on a Mamdani-type rule base and aggregates the results of applying fuzzy rules of the form IF Threat is X AND Damage is Y THEN Risk is Z. This form of representation allows for a visual analysis of the nonlinear nature of risk changes and the influence of combinations of input factors in a multi-criteria evaluation model.

For a more in-depth analysis of the fuzzy inference system's operation, it is advisable to transition from a discrete representation of rules to their continuous interpretation. This transition allows one to trace how individual fuzzy rules interact with each other after aggregation and defuzzification. That is why the next step is to visualize the rule base's results as a three-dimensional surface. This provides an intuitive understanding of the impact of combinations of input factors on the risk level, as demonstrated in Figure 12.

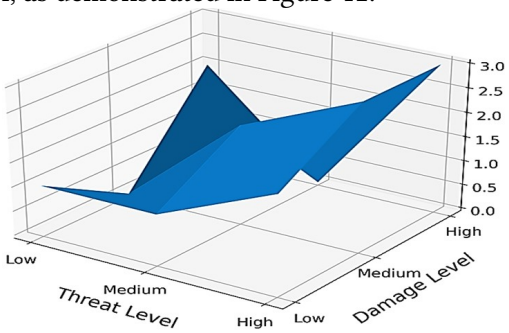


Figure 12: Three-dimensional surface of fuzzy inference for risk assessment

The generalized fuzzy logic inference system is described by the equation:

$$y(t)=F(x_1(t),x_2(t);W,B_1,C_1,B_2,C_2) \tag{25}$$

where W is the vector of weights of fuzzy rules, B_i, C_i are the parameters of the centers and widths of the membership functions, F is a Mamdani- or Sugeno-type fuzzy inference operator.

To train the model, a sample is formed from M historical cyber incident events:

$$x_1(t), x_2(t), y(t), t=1,\ldots,M, \tag{26}$$

which serves as the basis for optimizing parameters and adjusting the model to accommodate changes in the environment.

Model parameter tuning is performed by minimizing the loss function:

$$X=min_X \sum_{(t=1)}^{M} p(t)\cdot(y_{model}(t)-y_{actual}(t))^2 \tag{27}$$

where $p(t)$ is the weight coefficient of event significance, $X=\{W,B_1,C_1,B_2,C_2\}$ is the vector of parameters to be optimized [30-32]. To minimize criterion (27), a heuristic search algorithm (e.g., gradient descent or a genetic algorithm) adapted to the multidimensional parameter space of the fuzzy model is used.

The diagram in Figure 13 illustrates the sequential interaction between the main components of the risk assessment system: from the receipt of user input data through the fuzzyfier module, the activation of rules in the Rule Engine block, the calculation of the estimate in the Inference Engine module, defuzzification in the Defuzzifier module, to the generation of the final risk value in the Risk Output module. This process ensures the integration of fuzzy logic into automated decision-making regarding the risk of cyber incidents.

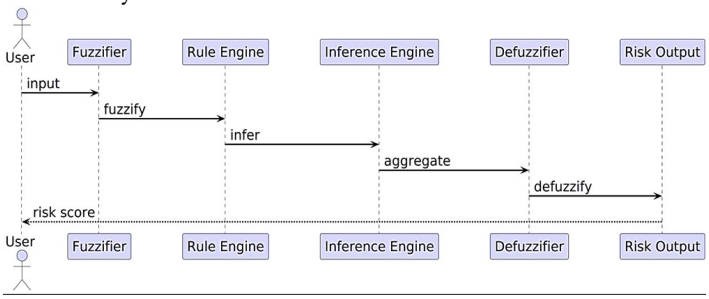


Figure 13: Sequence diagram of the interaction between risk assessment modules in a fuzzy inference system

The membership function for the variable u with respect to the term j is defined as:

$$\mu_j(u)=\frac{1}{1+\left|\frac{u-b_j}{c_j}\right|^{2p}}, \tag{28}$$

where b_j is the center of the membership function of the term j, c_j is the width (concentration), p is the degree of fuzziness (usually $p=2$).

The least squares method is used to adjust the parameters of the fuzzy model:

$$J(W)=\sum_{t=1}^{M} p(t)\cdot[y(t)-\hat{y}(t,W)]^2 \to min, \tag{29}$$

where W is the vector of weights for fuzzy rules, $p(t)$ is the weighting function that accounts for the importance of each case.

The modified hierarchical model (Fuzzy AHP) uses a priority aggregation function [34-35]:

$$\lambda_i=\frac{\prod_{j=1}^{n} a_{ij}^{1/n}}{\sum_{k=1}^{n}\prod_{j=1}^{n} a_{kj}^{1/n}}, \tag{30}$$

where a_{ij} is the comparison score between the i^{th} criterion and the j^{th} criterion, λ_i is the normalized weight of the criterion.

Since risk assessment is dynamic and depends on the ICS operational context, a situational approach is proposed [24, 30]. The sequence of events is analyzed as a sequence of fuzzy situations [4, 12, 29]:

$$st_i=\{\Lambda_1,\Lambda_2,\ldots,\Lambda_m\} \tag{31}$$

where Λ_i are linguistic variables describing the current situation (e.g., “high risk,” “unclear context,” “critical vulnerability”), each Λ_i is defined by a triplet (Ω_i, T_i, X_i), where Ω_i is the variable name, T_i is the term set (e.g., {low, medium, high}), X_i is the domain of definition.

The three-dimensional graph (Figure 14) shows the dependence of residual risk on the level of investment in preventive and reactive cybersecurity measures. It can be seen that as costs increase, residual risk decreases exponentially but eventually reaches a plateau, meaning that further increases in costs yield diminishing returns. This illustrates the saturation effect in the risk management model.

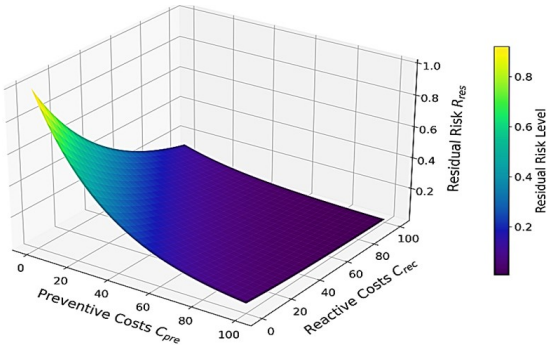


Figure 14: Surface of the residual risk function as a function of preventive and reactive expenditures

To enhance the clarity of the analysis, it is advisable to supplement the three-dimensional representation of risk with its projection onto a two-dimensional space. Such visualization allows for faster identification of areas of minimum and maximum residual risk without losing meaningful information about the impact of expenditures. The transition to a heat map simplifies the interpretation of trade-offs between preventive and reactive investments.

Figure 15 shows a heat map of the relationship between residual risk and the level of spending on preventive and reactive safety measures. The model demonstrates that risk decreases exponentially as any cost component increases, but the decrease has a saturation limit. The graph illustrates the trade-off between investments in protection and residual risk for the system.

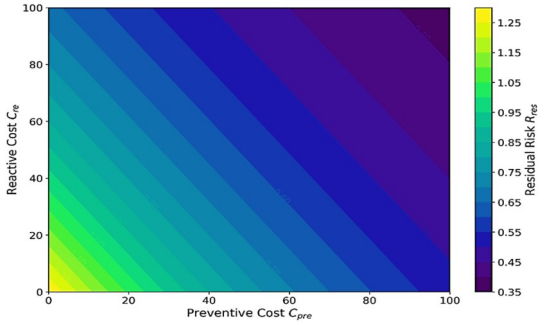


Figure 15: Relationship between residual risk and preventive and reactive costs

The degree to which the current situation belongs to one of the reference scenarios is estimated using the membership function:

$$v(st_0, st_j) = max_i \; min\left(\mu_{\Lambda_i^{(0)}}\right)(x), \mu_{\left(\Lambda_i^{(j)}(x)\right)}, \tag{32}$$

where st_0 is the current fuzzy situation, st_j is the reference situation from the knowledge base, $v \in [0,1]$ is the degree of similarity. If no situation fully matches the current one, a partial comparison is performed based on the most relevant features [12, 29]. The most similar situation is used to select the appropriate control action stored in the decision table. This approach increases the risk management system's flexibility, adaptability, and resilience to changes in environmental conditions, supporting reactive and predictive decision-making in real time.

To adapt decisions in real time, a metric for incorporating the current situation S_0 into the prototype S_i is introduced:

$$v(S_0, S_i) = min_j \left[\sup_{u \in X_j} \left(min\left(\mu_{\left(S_0^j\right)}(u), \mu_{\left(S_i^j\right)}(u)\right)\right)\right] \tag{33}$$

where $\mu_{S^j}(u)$ membership functions for the j^{th} situational variable, S_0 current situation (threat context, system technical parameters, etc.), S_i is prototype situation from the knowledge base (historically observed or classified), X_j universe of values of the j^{th} variable (e.g., load level, query frequency, risk level), $\mu_{S_0^j}(u), \mu_{S_i^j}(u)$ membership functions of fuzzy sets for the j^{th} variable of situations S_0 and S_i, sup is upper bound (supremum) over all values of u, min is intersection

operator of fuzzy sets. The minimum operation is used to model the intersection of membership functions, after which the smallest among the maxima over all variables is taken to calculate the worst-case correspondence scenario. The minimum operation is used to model the intersection of membership functions, after which the smallest among the maxima over all variables — is taken to calculate the worst-case correspondence scenario.

Based on the similarity of situations, a control action is selected [24, 30]:

$$u(t)=\arg\max_i v(S_0(t)S_i), \tag{34}$$

where $v(S_0,S_i)$ — is the value of the metric measuring the similarity between the current and prototype situations, $u(t)$ — is the control action (e.g., activation of countermeasures, policy changes, access reconfiguration). The formula allows selecting the best control action $u(t)$ at a given time$t$ that best matches the current situation $S_0(t)$ from all known situations S_i. The system selects the action that best matches the situation for adaptive real-time response. This implements knowledge-based intelligent risk management.

Residual risk update:

$$R_{res}(t+1)=R_{res}(t)-\Delta R(t) \tag{35}$$

where R_{res} is residual risk at time$t$ (risk remaining after applying measures), $\Delta R(t)$ is risk reduction due to the application of a control action $u(t)$,$R_{res}(t+1)$ is an updated value of residual risk. The formula describes the dynamics of residual risk reduction following the implementation of the selected control action. The system dynamically updates the risk depending on the effectiveness of the response. This enables an adaptive approach to risk management, ensuring continuous improvement of the security system. This sequence not only enables responding to incidents but also formalizes the process of fuzzy intelligent decision-making, which is critically important for ensuring the sustainable and flexible operation of the cyber defense system under conditions of uncertainty.

Let us denote the set of criteria defining the objective function as:

$$Q(X)=q_1(X),q_2(X),\ldots,q_m(X)\in R^m \tag{36}$$

where $q_i(X)$ is a normalized criterion (e.g., residual risk, cost, response time, compatibility, security level, etc.). The set $Q(X)$ forms a vector of criterion values that determine the effectiveness of decisions.

The performance space $Q\,space$ [30, 34]:

$$Q-space=\{Q(X)\,|\,X\in D\subseteq R^n\}, \tag{37}$$

where D is the set of feasible solutions. Let us denote the metric between two solutions $X_1,X_2\in D$ as:

$$d(Q(X_1),Q(X_2))=\sqrt{(\sum_{i=1}^m w_i\cdot q_i(X_1)-q_i(X_2)^2)}, \tag{38}$$

where $w_i\in[0,1]$ are the weights of the criteria, reflecting their relative importance. The metric d satisfies the conditions of a metric: symmetry, non-negativity, identity of indistinguishable solutions, and triangle inequality.

The criteria q_i are considered linearly independent if there is no nonzero set of coefficients $a_1,\ldots,a_m$ for which:

$$\sum_{i=1}^m a_i q_i(X)=0,\ \forall\ X\in D \tag{39}$$

where a_i are the coefficients. This ensures that each criterion is independent and significant in the model [6, 34]. $q_1=R_{res}(X)$ is residual risk after implementing measures, $q_{2.}=C_{total}(X)$ is total

cost of implementation and maintenance, $q_3 = T_{resp}(X)$ is expected average response time, $q_4 = \eta(X)$ integrated security assessment, $q_5 = \mu_{comp}(X)$ is degree of technical compatibility. These criteria describe different dimensions of effectiveness (risk, resource efficiency, productivity, security, integration), and therefore form a minimal, sufficient, and independent set. None of them is a linear combination of the others.

A solution X^* is Pareto-optimal if there is no such $X \in D$ that:

$$q_i(X) \le q_i(X^*)\ \forall i, \text{and for at least one } i: q_i(X) < q_i(X^*), \tag{40}$$

Let us denote the set of Pareto-optimal solutions as [28, 34]:

$$P = \{ X \in D \mid \nexists X' \in D : Q(X') \prec Q(X) ¿, \tag{41}$$

This approach allows us to preserve multi-criteria analysis without the need to reduce it to a single integrated indicator.

The graph (Figure 16) visualizes the three-dimensional set of Pareto-efficient risk management options, where no solution can be improved on one criterion without worsening another. The X-axis represents the cost of implementing security measures; the Y-axis represents the residual risk after their implementation; the Z-axis represents the integral assessment of system security.

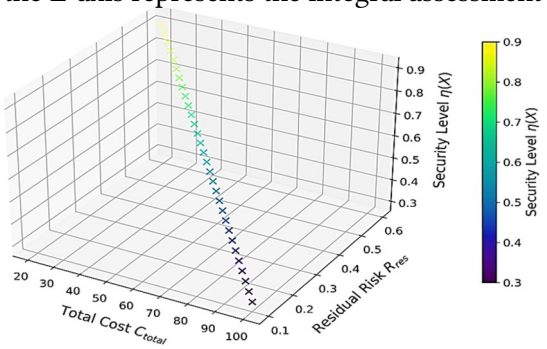


Figure 16: Set of Pareto-optimal solutions in Q-space

Weighted aggregation (for deterministic criteria):

$$F_{agg}(X) = \sum_{i=1}^{m} w_i \cdot \mu_{(q_i)}(X), \tag{42}$$

where $\mu_{q_i}(X) \in [0,1]$ is the normalized criterion value, and w_i are the weights (summing to 1).

To determine the effectiveness of security policy implementation, an aggregation function based on fuzzy logic is used [12, 28, 29]:

$$\mu_{eff}(X) = min_i\ \mu_{(q_i)}(X) (for\ \text{AND}\ logic), \text{or}\ \mu_{eff}(X) = max_i\ \mu_{(q_i)}(X) (for\ \text{OR}\ logic) \tag{43}$$

An interval model, where each criterion $q_i(X)$ is represented as an interval:

$$q_i(X) \in [q_i^{min}, q_i^{max}], \tag{44}$$

Instead of a single value, the worst-case scenario or expected value is analyzed:

$$E[q_i(X)] = \frac{(q_i^{min} + q_i^{max})}{2} \tag{45}$$

The probability of risk occurrence is represented by the posterior probability:

$$P(r \mid data) = \frac{(P(r \mid data) \cdot P(r))}{(P(data))}$$

Expected value of risk [28]:

$$E[R_{res}(X)]=\int_0^1 r\cdot P(r\,|\,data)\,dr, \tag{46}$$

This approach allows for the creation of a risk distribution with "tails," which is important when accounting for low-probability/high-impact threats.

As part of the development of a multi-criteria model for cybersecurity risk management in intelligent information and communication systems, it is proposed to use fuzzy logic production rules of the form:

$$d_{(t)}: IF\ x_1=\mu_{(1)} \wedge x_2=\mu_{(2)} \wedge \cdots \wedge x_p=\mu_p, THEN\ S=B_t \tag{47}$$

where x_j are the criteria for evaluating alternatives (e.g., cost, protection level, response time, scalability, etc.), μ_i are the corresponding fuzzy evaluations for these criteria, B_t is the result or decision made based on the fulfillment of the conditions.

To combine (convolve) criteria in such rules, the minimum operation is traditionally used; however, this reduces the problem to a single-criterion one, which can significantly lower the quality of decision-making under conditions of multifactorial uncertainty. To address this shortcoming, a new operation, a generalized projection (GP) of fuzzy sets is proposed.

The operation GP allows establishing a correspondence between the fuzzy sets A and$B$ according to the formula [4, 12]:

$$GP(A,B)=\{\,y : \mu_{A\to B}(y)=\sup min_x\ \mu_A(x), \mu_B f(x) \tag{48}$$

where μ_A are the membership functions of elements in the sets A and B, respectively, and $f(x)$ is the projection function that transforms the space of one criterion into the space of another. Thus, this operation allows one to determine the correspondence between sets of evaluations of different criteria, even when these evaluations are fuzzy or linguistic in nature (e.g., "high," "low," "medium").

A distinctive feature of the modern approach to selecting protective measures is the consideration of the variability of correspondences and permissible deviations from the ideal values of the criteria. For this purpose, a vector of permissible deviations is introduced:

$$E=\{\,e_j\in[0,1], j=1,\ldots,J\}, \tag{49}$$

where e_j is the limit of the permissible deviation of the estimate for the j^{th} criterion. Such a vector allows flexible consideration of trade-offs between criteria without rigidly rejecting alternatives that do not fully align with optimal values. This enhances the adaptability of the protective equipment selection model and enables more realistic decision-making under limited-resource and uncertain conditions.

Based on this, we introduce the aggregated metrics of an alternative's rir_iri compliance with the set of criteria, taking into account permissible deviations:

$$Pos(e,r_i)=\frac{1}{J}\sum_{j=1}^{J} Pos(e_j,r_{ij}), Nes(e,r_i)=\frac{1}{J}\sum_{j=1}^{J} Nes(e_j,r_{ij}), \tag{50}$$

where Pos is the degree of possible compliance, Nes is the required compliance, and the subjective confidence in the decision is also determined:

$$\Delta(e,r_i)=\frac{1}{J}\sum_{j=1}^{J}\mu_{(e_i)}(r_{ij}) \tag{51}$$

where $\mu_{e_i}(r_{ij})$ is the function mapping the actual criterion evaluation to an acceptable deviation. The resulting metrics allow for a quantitative assessment of both the optimistic (Pos) and conservative (Nes) scenarios of an alternative's compliance with the specified safety requirements. The indicator $\Delta(e,r_i)$ additionally reflects the decision-maker's level of confidence in the correctness of the choice, taking into account permissible deviations across all criteria. Collectively, this ensures more informed and robust decision-making in multi-criteria risk management tasks.

The solution is the alternative to the information security measure (ISM) for which the following conditions hold:

$$l\uparrow, Pos\uparrow, \Delta\uparrow, Nes\downarrow \tag{52}$$

That is, the desirable characteristics (possibility of satisfaction, decision confidence) are maximized, and the constraints (necessary satisfaction) are minimized.

To select the best option for the information security system, the objective function is optimized:

$$Q=\frac{(\Delta R_j)}{(C_j R_s)}\cdot 100\,\% \tag{53}$$

where ΔR_j is the risk reduction resulting from the implementation of the j^{th} measure, C_j is the cost of this measure, and R_s is the initial integral risk. Maximizing Q allows selecting the option with the best cost-effectiveness ratio.

To rank alternatives within a multi-criteria risk management model, a modified Saati hierarchy analysis method adapted to the context of fuzzy sets was applied. Each of the criteria q_j, which characterizes the parameters for evaluating the effectiveness of options (e.g., residual risk, cost, response delay), is presented as a fuzzy set with a corresponding membership function $\mu(q_j)$, which determines the degree of acceptability of the criterion's value for each alternative. The ranking procedure begins with a survey of experts regarding pairwise comparisons of decision alternatives. Based on the results, generalized (aggregated) membership functions for each alternative with respect to each individual criterion are derived. This allows for both expert opinion and the level of uncertainty in the assessments to be taken into account. The final ranking of alternatives is performed using the principle of the intersection of fuzzy sets, which ensures the selection of the most balanced solution. For each alternative x_i, the integral membership function is calculated [10, 11]:

$$\mu_{alt}=min\,(\mu(q_1,\mu(q_2),\ldots,\mu(q_m))), \tag{54}$$

which corresponds to the minimum value among all membership functions for the criteria. The best alternative is considered to be the one for which μ_{alt} is maximized, ensuring the highest consistency with all criteria simultaneously. This approach ensures a conservative decision-making process that focuses on minimizing the worst-case scenario across the criteria. The use of the minimum operation corresponds to the logic of fuzzy AND and is consistent with the principles of robust risk management. As a result of the ranking, an ordered set of alternatives is formed, allowing for a well-founded selection of the optimal solution under conditions of multi-criteria and uncertainty.

At the stage of rational resource allocation, an integral utility function is constructed:

$$Q(X,w)=\sum_{i=1}^{n} w_i\cdot x_i, \tag{55}$$

where x_i is the share of resources allocated to the i^{th} CIP, and w_i is the priority weighting coefficient calculated using the pairwise comparison method. The values of the weighting coefficients w_i reflect the relative importance of each protection service, taking into account the current level of risk and the criticality of assets. Optimizing the function $Q(X,w)$ allows us to find a resource allocation that achieves the maximum overall protection effect within a limited budget. Thus, the integral utility function serves as a formal decision-support tool during the planning stage of cybersecurity measures.

To solve the multi-criteria optimization problem, a solution space $X\in D$ was generated by creating quasi-random points using the Sobolev-Statnikov method, which ensures uniform coverage of the multidimensional region of feasible parameters. During the optimization process, one of the criteria, specifically the residual risk q_1, was selected as the primary criterion. The goal

is to minimize it, while the other criteria $q_2, q_3, \ldots, q_m$ are treated as pseudo-criteria that reflect secondary aspects of decision quality (e.g., costs, response time, performance, etc.).

For each pseudo-criterion, a corresponding membership function $\mu(q_k)$ is constructed, describing the degree of acceptability of the criterion value, taking into account the permissible deviation from the optimal level Δq_1. The overall compliance of decisions with all non-primary criteria is determined using the intersection of fuzzy sets, i.e., as:

$$U(q_{nonmain}) = min\ (\mu(q_2, \mu(q_3), \ldots, \mu(q_m))), \tag{56}$$

which allows us to evaluate the component with the worst acceptability. The final decision is selected according to the maximum-minimum rule:

$$M(q) = max\, min\ (\mu(q_1, \mu(q_2), \ldots, \mu(q_m))) \tag{57}$$

which guarantees the selection of the option that achieves the highest level of balanced compliance with both the primary and all secondary criteria simultaneously.

To enhance the model's flexibility and adaptability in the face of dynamic cyber threats, we propose integrating machine learning models (XGBoost, Random Forest, LSTM) at the following stages: refinement of weight coefficients w_i, modeling dependencies between criteria and risks, forecasting the effectiveness of ICS options, and automatic real-time policy updates. This combination enables the construction of an effective adaptive risk management model focused on reducing residual risk, optimizing costs, and enhancing the cyber resilience of intelligent ICS.

The formal verification of the model is based on the consistency property of the aggregated performance function. Specifically, when using AND logic to aggregate criteria, the system guarantees convergence to the smallest of the estimates, which is consistent with the principle of conservative decision-making. This means that none of the decisions made contradicts any critical constraints. Additionally, within the framework of modified fuzzy analytic hierarchy process (Fuzzy AHP), the consistency coefficient of the pairwise comparison matrices was CR < 0.1, confirming the acceptable coherence of the priority system.

The proposed multi-criteria model operates as a sequential algorithmic loop. In the first stage, a security context is formed based on telemetry data and asset characteristics. Next, using machine learning algorithms, the probability of threat scenarios occurring is predicted. The resulting quantitative estimates are transformed into linguistic variables and processed by fuzzy inference mechanisms. In the final stage, a multi-criteria selection of a set of protective measures is performed, taking into account resource constraints and the acceptable level of risk.

5. Practical implementation and test results

The proposed multi-criteria model for cybersecurity risk management in intelligent information and communication systems was implemented using a comprehensive architecture that integrates components of fuzzy logic, machine learning, situational analysis, and reactive security policy management. The system prototype was implemented using the Python programming language, the Scikit-learn, TensorFlow, and FuzzyLogic libraries, as well as Flask for building a REST API [21, 30]. The selected libraries ensure reliability, scalability, and compatibility with real-time tasks in the context of cybersecurity risk analysis. The proposed system supports integration with modern cybersecurity standards and architectures, including Zero Trust Architecture (NIST SP 800-207) and ISO/IEC 27005 [13, 24, 34]. A REST API interface has been implemented for data exchange with external platforms, enabling real-time interaction with incident detection and response systems, including Splunk SIEM.

Figure 17 shows a UML deployment diagram of an intelligent cybersecurity risk management system within an information and communication system. The architecture is built on a modular principle and includes five main layers: the user interface (Web Dashboard), the application layer (Flask API Server), the machine learning layer (XGBoost, LSTM, SHAP), the data layer (PostgreSQL, user profiles, risk logs), and the security monitoring module (Splunk SIEM). Dotted arrows indicate the interaction logic between modules, including the exchange of REST requests, the transmission of risk assessments, the formation of access policies, and the activation of incident

response. External data sources (CICIDS-2017, UNSW-NB15) and compliance with ISO/NIST standards are also considered.

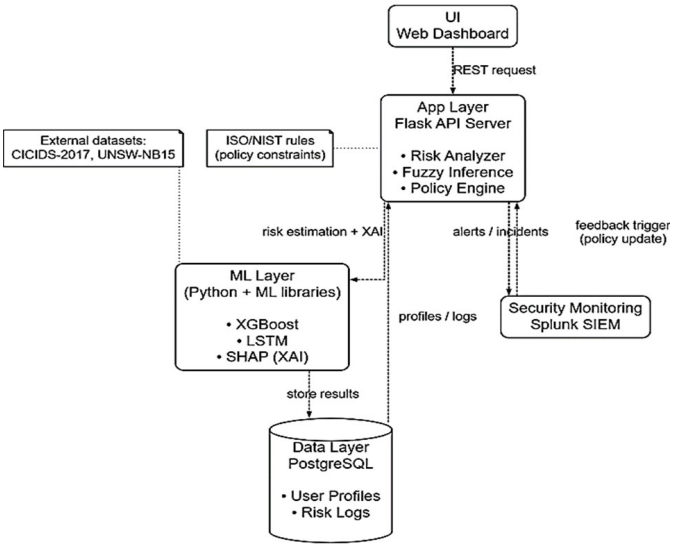


Figure 17: Deployment of the multi-criteria ICS risk management system architecture

A key component is a Mamdani-type fuzzy inference module that evaluates the residual risk level based on linguistic rules of the form "IF x_1 = low AND x_2 = high THEN y = medium". The input parameters (threat, vulnerability, potential losses, user context) are formalized as linguistic variables with corresponding membership functions [12]. The risk assessment takes into account both quantitative and qualitative factors, including the context ntext and behavioral patterns.

To build the predictive risk model, the Extreme Gradient Boosting (XGBoost) algorithm was used, which achieved a classification accuracy of 92%, a precision of 91%, and an F1 Score of 0.90. The XGBoost algorithm was used to build the predictive model with the following hyperparameters: tree depth (max_depth) 4, learning rate (learning_rate) 0.1, number of trees (n_estimators) 150, subsample ratio (subsample) 0.8, feature ratio per tree (colsample_bytree) 0.7, loss function binary: logistic. Hyperparameter optimization was performed using a grid search method with 5-fold cross-validation.

The algorithm was trained on a synthetic dataset containing over 100,000 records with historical incident data, attack parameters, and response outcomes [21]. Additionally, a recurrent neural network (LSTM) was used, which was trained to predict risk dynamics in time series while accounting for changes in attack activity [16, 18]. The prediction results showed a root-mean-square error (RMSE) of ≈ 0.031, indicating a high level of agreement between the model and the actual data. During the training of the LSTM model on time series with risk dynamics, a gradual decrease in the root-mean-square error (RMSE) was observed, from 0.094 in the first epoch to 0.031 in the twentieth [16, 19]. This indicates the model's stable convergence and ability to adequately generalize attack patterns.

To evaluate the effectiveness of the proposed XGBoost model with SHAP analysis, a comparison was conducted with the classic Snort intrusion detection system on the same dataset (CICIDS-2017). The comparison was based on key classification accuracy metrics, as shown in Table 2.

Table 2.
Comparison of performance metrics for XGBoost and Snort

Metric	XGBoost (with SHAP)	Snort IDS
Precision	0.94	0.88
Recall	0.91	0.86
F1-score	0.925	0.87
Accuracy	0.93	0.89
Average response time	~1.2 sec	~4.8 sec
False positives	6%	10%

As shown in Table 2, the XGBoost model achieves significantly higher attack-detection accuracy and response speed than the traditional Snort IDS. This underscores the effectiveness of combining machine learning methods with XAI to create an adaptive access-control and threat-detection system.

Figure 18 shows the risk forecast generated by the LSTM model compared to actual values. A consistent trend is observed, confirming the neural network's ability to identify patterns over time and predict potential spikes in risk within the intelligent ICS.

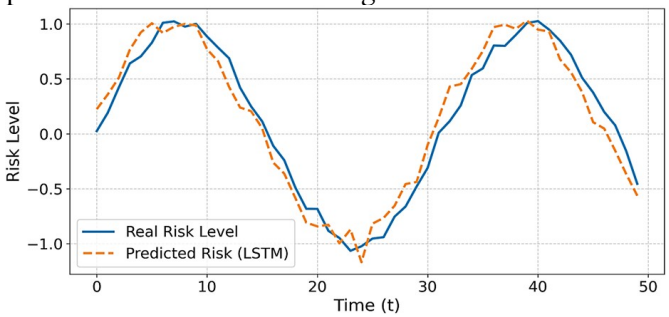


Figure 18: Risk level forecast graph using LSTM

The selection of the optimal set of security measures (SM) was performed using a modified fuzzy AHP (Fuzzy Analytic Hierarchy Process) method [10, 12]. A group of experts in the field of information security was involved in the formation of the pairwise comparison matrix of criteria (residual risk, cost, scalability, response time, compatibility with ICS) [15]. Weight coefficients were determined to ensure a consistency ratio (CR) < 0.1, confirming the reliability and consistency of the resulting priority structure.

To support reactive updates to security policies, an integration mechanism with the Splunk platform has been implemented that provides triggers for changes in threat and risk status [8, 13]. If the residual risk threshold is exceeded or the context confidence index decreases, the system automatically initiates a change in access policies and a recalculation of the resource allocation strategy for protection [27, 30]. Testing on realistic incident scenarios showed a 38% reduction in mean time to resolution (MTTR) compared to the baseline policy.

The summarized results of the prototype's effectiveness are presented in a table that shows the relationship among each component's functional objectives, the achieved accuracy or effectiveness, and the implementation tools [17, 21, 34]. This modular architecture ensures both integration flexibility and system scalability within critical and corporate ICS environments.

The implemented system enables context-aware risk assessment, supports adaptive access policies, and ensures optimal allocation of security resources in accordance with the current threat landscape, attack scenarios, and residual risk. In addition, the use of explainable machine learning methods (SHAP, LIME) ensures the interpretability of predictive models, significantly increasing trust in automated decisions. The model's correctness was assessed through an interpretable analysis of SHAP influences, yielding a stable distribution of priority features. This confirms the model's internal consistency in decision-making.

Thus, the practical implementation results confirm the feasibility of applying the proposed model in a dynamic, uncertain cyber environment [24, 34]. The implemented solution meets the modern requirements of Zero Trust architectures, supports the ISO/IEC 27005 and NIST SP 800-30 standards, and can be recommended for use in cybersecurity systems for critical information infrastructure, government platforms, and corporate environments.

The effectiveness of the proposed model was evaluated using quantitative indicators of risk prediction accuracy, decision stability, and residual risk reduction relative to baseline approaches. The experimental results confirmed that integrating machine learning with fuzzy multi-criteria analysis yields more consistent and robust risk management in the face of dynamically changing threats.

6. Discussion

The results obtained demonstrate the effectiveness of the proposed multi-criteria cybersecurity risk management model, which integrates methods of fuzzy logic, machine learning, and adaptive real-

time situation assessment. Practical implementation has confirmed that the use of combined risk assessment models ensures both forecasting accuracy and decision-making flexibility in conditions of uncertainty and dynamic changes in cyber threats.

Unlike classical risk assessment models such as CVSS, DREAD, and RAdAC, the proposed approach provides a holistic combination of forecasting, fuzzy evaluation, and decision optimization within a single context-adaptive environment. Compared to models based exclusively on machine learning or fuzzy logic, the developed model demonstrates greater decision stability and better interpretability in complex threat scenarios.

Compared to classical risk management models that rely on rigidly formalized metrics (e.g., the product of probability and impact), the proposed system demonstrates greater sensitivity to contextual cues, as well as the ability to adaptively adjust security policies based on situational analysis. This is particularly important in Zero Trust and distributed cloud environments, where traditional models cannot account for attackers' behavioral dynamics and the interdependencies among ICS nodes.

In particular, the inclusion of a long short-term memory (LSTM) neural network enabled effective modeling of threat temporal dynamics, detection of latent trends, and adaptation to changes in attack patterns [18-19, 34]. Unlike static models, the LSTM approach enabled the system to respond proactively, predicting risk before an incident occurs. This is critical for reducing mean time to response (MTTR), mitigating residual risk, and minimizing incident-related losses.

The line graph (Figure 19) compares the classical RBAC model, the fuzzy logic-based model, and the combined LSTM + Fuzzy model across three key metrics: prediction accuracy, normalized response time (lower values are better), and adaptability. This allows for a visual assessment of the benefits of using modern intelligent approaches to cybersecurity risk management.

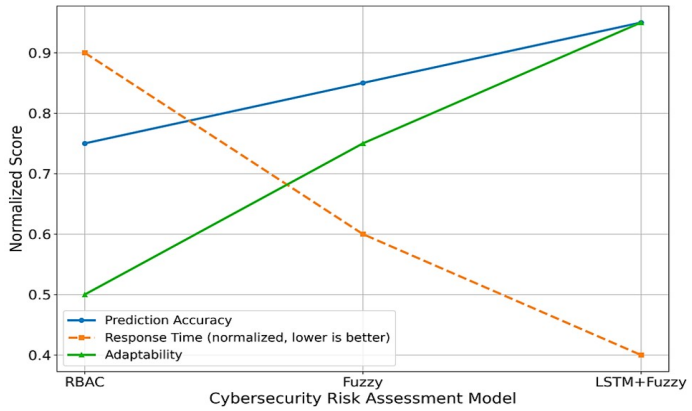


Figure 19: Comparative effectiveness of cybersecurity risk assessment methods

In addition, the use of fuzzy sets has made it possible to formalize expert linguistic assessments, which often accompany security analysis in practical settings where exact values are unavailable or vary over time [12, 29]. This provides greater flexibility and alignment with real-world scenarios, especially in distributed systems where the behavior of protected objects varies.

It is important to note that the proposed model supports multi-criteria analysis without reducing the criteria to a single integrated indicator, which helps avoid information loss during compromise decision-making. Instead, a mechanism for finding a Pareto-optimal solution has been implemented, in which improving one criterion at the expense of a significant deterioration in another is not permitted [24, 28, 34]. This approach is more resilient to conflicting security requirements, such as the trade-off between implementation cost and security level.

Integrating the model with the SIEM infrastructure (Splunk) has not only reduced the security administrator's workload through automated anomaly responses but also laid the foundation for explainable analytics [13]. The use of SHAP and LIME tools increases confidence in the results of the decision-making system, which is a key factor in the context of regulatory compliance and certification.

At the same time, a limitation of the model is its dependence on the quality of input data and the limited nature of training samples in specific domains (e.g., in energy or medical ICS) [22-23]. This can reduce the generalization ability of machine learning models in highly specialized environments. Further research should focus on improving adaptation to new threats without

requiring complete retraining, for example, through mechanisms such as online learning, federated learning, or self-supervised adaptation.

In addition, a promising direction is the use of neuro-fuzzy systems (Neuro-Fuzzy), which combine the interpretive capabilities of fuzzy logic with the learning ability of neural networks, and the application of graph neural networks (GNN) to analyze interdependencies among ICS components via attack graphs.

In summary, it can be stated that the proposed model provides a high degree of adaptability, explainability, and effectiveness in cyber risk management. Its use enables a transition from static security policies to context-oriented, self-learning, and dynamically optimized solutions that address modern challenges in information security for intelligent ICS.

The results obtained depend on the quality of the input data and the representativeness of the threat scenarios used in the modeling process. Limitations also arise from the need for expert configuration of fuzzy rules during the initial stage of model implementation. Generalizing the results to other classes of information and communication systems requires additional validation, accounting for the specifics of the domain.

Conclusions

The proposed multi-criteria model and experimental approach are reproducible, provided that similar input data, training parameters, and fuzzy inference rules are used. The solution architecture and the logic of the algorithmic loop allow for the replication of experimental studies and the adaptation of the model to other intelligent information and communication systems.

This paper presents an intelligent multi-criteria model for cybersecurity risk management, designed to operate under conditions of uncertainty, dynamic threats, and complex inter-component dependencies in intelligent information and communication systems. The proposed approach is based on the integration of fuzzy logic methods, machine learning (in particular, XGBoost and LSTM), and multi-criteria decision analysis with dynamic consideration of the threat context and residual risk. All mathematical models were verified for consistency and convergence, specifically within the fuzzy space Q and using XAI analysis (SHAP, $CR < 0.1$).

Formalizing the risk management task as a multi-criteria optimization problem with fuzzy constraints enabled flexible decision-making that accounts for criteria such as residual risk, cost, scalability, response time, and technical compatibility. The proposed mathematical model supports both quantitative and linguistic assessments, ensuring high interpretability and adaptability of the system to real-world operating conditions.

The practical implementation of the model demonstrated its suitability for integration into modern cyberinfrastructure. The implemented prototypes demonstrated high risk prediction accuracy (up to 92%), effective ranking of alternatives (consistency coefficient $CR < 0.1$), and a significant reduction in response time (up to 38%). The use of explainable machine learning components (SHAP, LIME) ensured transparency in decision-making and enabled auditing of security policies.

The developed model supports adaptive access policy updates, proactive detection of critical threat scenarios, prediction of residual risk, and optimal allocation of protection resources. The use of generalized fuzzy set projection enabled the overcoming of limitations of traditional models that reduce multi-criteria analysis to one-dimensional indicators.

The results obtained allow us to conclude that the developed system is an effective tool for risk management in ICS with increased requirements for robustness, adaptability, and explainability. The model's performance was validated on the open-source CICIDS-2017 and UNSW-NB15 test datasets, confirming its ability to detect and predict complex cyber threat scenarios in real-world network traffic conditions. It can be used in cloud environments, Zero Trust architectures, critical infrastructures, and corporate information security management systems.

Prospects for implementing the proposed system include integration with SOAR platforms for automated response, expansion to IoT environments, and adaptation to the requirements of the NIST SP 800-207 (Zero Trust Architecture) standard. Further research may focus on verifying the model's effectiveness in sectors with heightened security requirements, particularly in healthcare and energy information and communication systems.

Further research directions include: improving online adaptation mechanisms without fully retraining the model, expanding the threat scenario database using graph neural networks, and

integration with multi-level monitoring and incident data exchange platforms. Thus, the proposed model provides a foundation for building adaptive, self-learning, and robust cybersecurity systems capable of functioning effectively under conditions of high uncertainty and increasing threat complexity. However, a potential limitation of the model is its dependence on the quality of training data and limited generalizability in specific domains without additional tuning. Its suitability for typical attack scenarios was preliminarily evaluated based on the open datasets CICIDS-2017 and UNSW-NB15, which justifies the promise of further testing in intelligent ICS.

Declaration on Generative AI

While preparing this work, the authors used the AI programs Grammarly Pro to correct text grammar and Strike Plagiarism to search for possible plagiarism. After using this tool, the authors reviewed and edited the content as needed and took full responsibility for the publication's content.

References

[1] H. Atlam, M. Azad, M. Alassafi, A. Alshdadi, A. Alenezi, Risk-based access control model: A systematic literature review. Future Internet, 2020, 12(6), 103. doi:10.3390/fi12060103

[2] A. Jazairy, M. Brho, I. Manuj, T. Goldsby, Cyber risk management strategies and integration: toward supply chain cyber resilience and robustness. Int. J. Phys. Distrib. Logist. Manag., 2024, 54(11), 1-29. doi:10.1108/IJPDLM-12-2023-0445

[3] A. Barlybayev, A. Sharipbay, G. Shakhmetova, G., A. Zhumadillayeva, Development of a Flexible Information Security Risk Model Using Machine Learning Methods and Ontologies. Appl. Sci., 2024, 14(21), 9858. doi:10.3390/app14219858

[4] E. Bakhtavar, et al. Fuzzy cognitive maps in systems risk analysis: a comprehensive review. Complex Intell. Syst. 7, 621-637, 2021, doi:10.1007/s40747-020-00228-2

[5] S. Kerimkhulle, et.al., Fuzzy Logic and Its Application in the Assessment of Information Security Risk of Industrial Internet of Things. Symmetry, 2023, 15(10), 1958, doi:10.3390/sym15101958

[6] I. Hamid, M. Rahman, AI, machine learning, and deep learning in cyber risk management. Discov Sustain., 6, 389, 2025, doi:10.1007/s43621-025-01012-3

[7] A. Zadeh, B. Lavine, H. Zolbanin, D. Hopkins, A cybersecurity risk quantification and classification framework for informed risk mitigation decisions. Decis. Anal. J., 9, 100328, 2023, doi:10.1016/j.dajour.2023.100328

[8] S. Islam, N. Basheer, S. Papastergiou, et al. Intelligent dynamic cybersecurity risk management framework with explainability and interpretability of AI models for enhancing security and resilience of digital infrastructure. J Reliable Intell Environ 11, 12, 2025, doi:10.1007/s40860-025-00253-3

[9] N. Katnapally, et. al., Neural Network-Based Risk Assessment for Cybersecurity in Big Data-Oriented ERP Infrastructures. Educ. Adm. Theory Pract., 27(4), 1329-1341, 2021. doi:10.53555/kuey.v27i4.9073

[10] D. Kozhukhivskyi, O. Kozhukhivska, Developing a fuzzy risk assessment model for ERP systems. Radio Electron. Comput. Sci. Control., (1), 106, 2022, doi:10.15588/1607-3274-2022-1-12

[11] S. Shevchenko, Y. Zhdanova, O. Kryvytska, H. Shevchenko, S. Spasiteleva, Fuzzy cognitive mapping as a scenario approach for information security risk analysis. In: Cybersecurity Providing in Information and Telecommunication Systems II 2024, 3826. pp. 356-362.

[12] R. Shevchuk, V. Martsenyuk, Neural Networks Toward Cybersecurity: Domain Map Analysis of State-of-the-Art Challenges, In: IEEE Access, vol. 12, pp. 81265-81280, 2024, doi: 10.1109/ACCESS.2024.3411632

[13] W. Wu, H. Fouzi, B. Benamar, et al. Deep learning-based stacked models for cyber-attack detection in the industrial Internet of Things. Neural Comput. Applic, 2025, doi:10.1007/s00521-025-11418-9

[14] Y. Kostiuk, P. Skladannyi, N. Korshun, B. Bebeshko, K. Khorolska, Integrated protection strategies and adaptive resource distribution for secure video streaming over a Bluetooth network. In: Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, (CPITS-II 2024) October 26, 2024. Aachen: CEUR, 2024. Vol. 3826. Pp. 129-138.

[15] K. Zarzycki, Forgery Cyber-Attack Supported by an LSTM Neural Network: An Experimental Case Study. Sensors, 23(15), 6778, 2023, doi:10.3390/s23156778
[16] Y. Kostiuk, P. Skladannyi, V. Sokolov, O. Zhyltsov, Y. Ivanichenko, Effectiveness of Information Security Control using Audit Logs. In: Proceedings of the Workshop on Cybersecurity s in Information and Telecommunication Systems (CPITS 2025), 2025. Aachen: CEUR, 2025. Vol. 3991. P. 524-538.
[17] Z. Yasmeen, Designing Neural Network Frameworks for Big Data Analysis in ERP Systems to Counter Cyber Threats. J. Artif. Intell. Big Data Discip., 2025, 2(1), 18-27. doi:10.70179/2rt9k031
[18] I. Mashkina, S. Rzaieva, Y. Kostiuk, N. Mazur, Z. Brzhevska, Cybersecurity in Intelligent Transport Systems: Current Challenges and Solutions. In: Proceedings of the Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2025), 2025. Aachen: CEUR, 2025. Vol. 3991. P. 14-25.
[19] P. Cheimonidis, K. Rantos, Dynamic Risk Assessment in Cybersecurity: A Systematic Literature Review. Future Internet, 2023, 15(10), 324, doi:10.3390/fi15100324
[20] Y. Kostiuk, S. Rzaieva, K. Khorolska, N. Mazur, N. Korshun, Architecture of the software system for confidential access to information resources of computer networks. In: Proceedings of the Workshop Cyber Security and Data Protection, July 31, 2025, Lviv, Ukraine (CSDP 2025). Vol. 4042. P. 37-53.
[21] S. Rzaieva, et al., Methods of Modeling Database System Security, Cybersecurity in Information and Telecommunication Systems, 2024, 384-390.
[22] J. Wang, M. Neil, N. Fenton, A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model. Comput. Secur., 2020, 89, 101659. doi:10.1016/j.cose.2019.101659
[23] Y. Kostiuk, P. Skladannyi, Y. Samoilenko, K. Khorolska, B. Bebeshko, V. Sokolov, A system for assessing the interdependencies of information system agents in information security risk management using cognitive maps. In: Cyber Hygiene & Conflict Management in Global Information Networks, 2024, vol. 3925, pp. 249-264, CEUR-WS.
[24] R. Bitton, N. Maman, I. Singh, S. Momiyama, Y. Elovici, A. Shabtai, Evaluating the cybersecurity risk of real-world, machine learning production systems. ACM Comput. Surv., 2023, 55(9), Article 183, 1-36. doi:10.1145/3559104
[25] P. Skladannyi, Y. Kostiuk, S. Rzaieva, B. Bebeshko, N. Korshun, Adaptive Methods for Embedding Digital Watermarks to Protect Audio and Video Images in Information and Communication Systems. In: Proceedings of the Workshop on Classic, Quantum, and Post-Quantum Cryptography, August 5, 2025, Kyiv, Ukraine (CQPC 2025). Vol. 4016. P. 13-31.
[26] R. Jiang, L. Wan, Network Information Security Risk Assessment Method Based on Machine Learning Algorithm. In: Fu, W., Yun, L. (eds) Advanced Hybrid Information Processing. ADHIP 2022. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 2023, vol. 469. Springer, Cham., doi:10.1007/978-3-031-28867-8_30
[27] L. Bernardo, S. Malta, J. Magalhães, An Evaluation Framework for Cybersecurity Maturity Aligned with the NIST CSF. Electron., 2025, 14 (7), 1364, doi:10.3390/electronics14071364