big data and cognitive computing

MDPI

Article

Adaptive Management of Multi-Scenario Projects in Cybersecurity: Models and Algorithms for Decision-Making

Vadim Tynchenko [1,2,*], Alexander Lomazov [3], Vadim Lomazov [4,5], Dmitry Evsyukov [1], Vladimir Nelyub [1,6], Aleksei Borodulin [1], Andrei Gantimurov [1] and Ivan Malashin [1,*]

1 Artificial Intelligence Technology Scientific and Education Center, Bauman Moscow State Technical University, 105005 Moscow, Russia; alexey.borodulin@emtc.ru (A.B.)
2 Department of Information and Control Systems, Reshetnev Siberian State University of Science and Technology, 660037 Krasnoyarsk, Russia
3 Department of Data Analysis and Machine Learning, Financial University, 125167 Moscow, Russia; alomazov@yandex.ru
4 Department of Mathematics, Physics, Chemistry and Information Technologies, Belgorod State Agricultural University Named After V. Gorin, 308503 Belgorod, Russia
5 Department of Applied Informatics and Information Technology, Belgorod State University, 308015 Belgorod, Russia
6 Scientific Department, Far Eastern Federal University, 690922 Vladivostok, Russia
* Correspondence: vadimond@mail.ru (V.T.); ivan.p.malashin@gmail.com (I.M.); Tel.: +7-926-875-7128 (I.M.)

Abstract: In recent years, cybersecurity management has increasingly required advanced methodologies capable of handling complex, evolving threat landscapes. Scenario network-based approaches have emerged as effective strategies for managing uncertainty and adaptability in cybersecurity projects. This article introduces a scenario network-based approach for managing cybersecurity projects, utilizing fuzzy linguistic models and a Takagi–Sugeno–Kanga fuzzy neural network. Drawing upon L. Zadeh's theory of linguistic variables, the methodology integrates expert analysis, linguistic variables, and a continuous genetic algorithm to predict membership function parameters. Fuzzy production rules are employed for decision-making, while the Mamdani fuzzy inference algorithm enhances interpretability. This approach enables multi-scenario planning and adaptability across multi-stage cybersecurity projects. Preliminary results from a research prototype of an intelligent expert system—designed to analyze project stages and adaptively construct project trajectories—suggest the proposed approach is effective. In computational experiments, the use of fuzzy procedures resulted in an over 25% reduction in errors compared to traditional methods, particularly in adjusting project scenarios from pessimistic to baseline projections. While promising, this approach requires further testing across diverse cybersecurity contexts. Future studies will aim to refine scenario adaptation and optimize system response in high-risk project environments.

Keywords: cybersecurity; adaptive project management; scenario network; decision support; linguistic variable; fuzzy production rule; fuzzy inference

check for updates

Citation: Tynchenko, V.; Lomazov, A.; Lomazov, V.; Evsyukov, D.; Nelyub, V.; Borodulin, A.; Gantimurov, A.; Malashin, I. Adaptive Management of Multi-Scenario Projects in Cybersecurity: Models and Algorithms for Decision-Making. *Big Data Cogn. Comput.* **2024**, *8*, 150. https://doi.org/10.3390/bdcc8110150

Academic Editors: Biao Han, Xiaoyan Wang, Xiucai Ye and Na Zhao

Received: 27 September 2024
Revised: 30 October 2024
Accepted: 1 November 2024
Published: 4 November 2024

Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

The rapid advancement of digital technologies has transformed not only the way businesses operate but also the landscape of cybersecurity. As organizations increasingly rely on digital solutions, they become more vulnerable to an evolving array of cyber threats. These threats range from sophisticated hacking attempts to insider risks, often resulting in significant financial and reputational damage. As reported in the literature, these emerging risks are accompanied by a growing need for robust cybersecurity measures that can adapt to the dynamic threat environment [1–3]. Furthermore, the fast-paced technological innovations present opportunities for enhancing cybersecurity practices, making it essential for organizations to remain vigilant and proactive in their defenses [4,5].

Given the complexities and high stakes involved, long-term cybersecurity projects require a flexible and adaptive management approach. This necessity arises from the fact that project conditions frequently change based on the outcomes of individual stages, emerging threats, and advancements in technology. Moreover, cybersecurity projects often entail substantial financial investments, particularly for small and medium-sized enterprises (SMEs), where the cost of implementing comprehensive security measures can be especially burdensome [6–8]. As a result, effective decision support mechanisms in adaptive project management for the development and implementation of cybersecurity systems become critically important, ensuring that resources are allocated efficiently and risks are managed effectively.

The complexity and unstructured nature of the cybersecurity domain further require the use of intelligent decision-making methods. Traditional approaches, such as the widely adopted precedent-based methodology, often encounter limitations due to the scarcity of historical data regarding the effectiveness of information security systems against new and emerging threats [9,10]. The lack of precedents complicates the ability of decision-makers to rely on past experiences when navigating the intricacies of cybersecurity project management. Therefore, there is a pressing need for innovative frameworks that can accommodate the unique challenges of this field.

The structure of this article is outlined as follows. It begins with Section 2, which reviews the existing literature and methodologies relevant to information security management, identifying gaps and opportunities for enhancement. Following this, Section 3 outlines various frameworks and approaches that organizations can adopt to evaluate and improve their cybersecurity strategies. This is succeeded by Section 4, which analyzes the findings from the research, addressing their implications for practitioners and policy-makers in the field. Next, Section 5 considers how expert opinions may evolve over time and the potential impacts of these changes on decision-making processes. This leads to Section 6, where methods for navigating project stages and making informed decisions based on dynamic circumstances are proposed. The article concludes with a summary of key insights and recommendations for future research in adaptive project management for cybersecurity.

2. Related Works

Critical infrastructure (CI) encompasses essential systems and services crucial to societal and national stability. Given today's dynamic cyber threats, disruptions to CI can severely impact public safety and economic security. Sarker et al. [11] focus on "Rule-based AI" for CI cybersecurity, emphasizing transparency, interpretability, and trustworthiness, which are vital for decision-making. They present a multi-faceted study on rule-based AI modeling, including a taxonomy of rule generation methods that blend expert knowledge with data-driven insights. The paper explores applications across CI sectors—such as threat detection and mitigation—and highlights challenges, opportunities, and future research directions for advancing cybersecurity in CI.

With increasingly severe and frequent cyber-attacks, organizations seek stronger defenses, leveraging cyber threat intelligence (CTI) mining to transform threat data into actionable intelligence for proactive defense. Sun et al.'s [12] research focused on CTI mining, offering a taxonomy based on key cybersecurity applications like attack tactics, hacker profiles, indicators of compromise, and threat hunting. Despite challenges with data volume, real-time analysis, and false positives, CTI mining enhances threat detection and response capabilities. The survey highlights current methodologies, challenges, and future research directions, underscoring CTI's potential to advance cybersecurity resilience.

As cybersecurity systems generate increasing volumes of unstructured data, utilizing natural language processing (NLP) has become essential for detecting anomalies and intrusions. Sharma et al. [13] provide an overview of NLP techniques for cybersecurity, covering motivations, challenges, and types of relevant data. Key NLP methods—such as named entity recognition, sentiment analysis, topic modeling, and document classification—

are discussed for their roles in anomaly and intrusion detection. A structured taxonomy and literature review highlight current NLP-driven approaches, and their strengths, limitations, and research gaps. This analysis lays a foundation for future NLP advancements to improve proactive threat detection and response capabilities in cybersecurity.

Digital twins (DTs) are transformative in industry and research, enabling virtual representations of physical systems for enhanced monitoring, maintenance, and resilience. However, they introduce cybersecurity challenges as they increase exposure to intellectual property risks and real-time synchronization vulnerabilities. Sacker et al. [14] explore AI and explainable AI (XAI) approaches for addressing these challenges in DTs, emphasizing transparent, interpretable cybersecurity models. A taxonomy of AI/XAI methods is presented, aiding analysts in anomaly detection, threat mitigation, and system resilience. The study identifies current gaps, potential applications, and research avenues for advancing secure, trustworthy DT environments through XAI-driven cybersecurity solutions.

The increasing reliance on digital technology has made cybersecurity critical for protecting systems from cyber-attacks. Sacker et al. [15] explore how artificial intelligence (AI) can advance cybersecurity by enabling intelligent, automated, and robust defenses against complex threats such as malware, zero-day attacks, and phishing. Focusing on AI-based modeling and adversarial learning, the study provides insights into AI's role in enhancing security intelligence across varied cyber applications. Key methods, including adversarial machine learning, are discussed alongside future research directions to address emerging cybersecurity challenges. This overview aims to guide the development of resilient AI-based security solutions for safeguarding digital infrastructures.

Malatji et al. [16] explore the intersection of artificial intelligence (AI) and cybersecurity, focusing on the challenges and opportunities presented by AI technologies. They introduce the AI Cybersecurity Dimensions (AICD) Framework, which serves as a multidimensional tool for academics, policy-makers, and industry professionals to understand and address AI-driven cyber threats. The research delves into the dynamics of offensive AI, highlighting the necessity for adaptive defenses and ethical considerations, as well as the risks posed by adversarial AI. Through comprehensive literature reviews and textual analyses, the study emphasizes the need for interdisciplinary approaches to bridge gaps in cybersecurity discourse. The AICD Framework aims to facilitate a holistic understanding and practical interventions in the evolving AI-infused cybersecurity landscape, advocating for collaborative efforts in research and practice to effectively tackle these intricate challenges.

Alqurashi et al. [17] point out the importance of cybersecurity in safeguarding digital systems, economic stability, and national security. They utilize topic modeling to analyze 15,751 academic articles from the Web of Science and 5831 industry articles from *Security Magazine*, employing techniques like BERTopic, UMAP, and HDBSCAN to identify trends and themes in cybersecurity research. Their findings reveal 24 knowledge clusters, highlighting macro-clusters in technology, smart city applications, organization, public security, governance, and education. The study identifies increasing attention on malware and cyber-attack mitigation, especially post-2020. It emphasizes the need for a unified approach integrating academic and industry perspectives to enhance cybersecurity strategies, while also recognizing challenges such as data source limitations and biases. Future research will focus on expanding datasets and refining methodologies to improve insights into evolving cybersecurity threats.

Table 1 summarizes the key directions and findings of these studies. Each entry reflects a unique aspect of cybersecurity, whether it involves the use of artificial intelligence, natural language processing, or threat analysis through cyber threat intelligence (CTI).

Table 1. Summary of cybersecurity studies.

Reference	Focus	Applied Model	Results
Sarker et al. (2024) [15]	Rule-based AI for cybersecurity in critical infrastructure (CI)	Rule-based AI modeling, taxonomy of rule generation	Multi-faceted study identifying applications and challenges in CI cybersecurity.
Sun et al. (2023) [12]	Cyber threat intelligence (CTI) mining for proactive defense against cyber threats	Taxonomy of CTI applications	Enhanced threat detection and response, highlighting future research directions.
Sharma et al. (2023) [13]	Natural language processing (NLP) techniques for anomaly and intrusion detection	Named entity recognition, sentiment analysis, etc.	Structured taxonomy and literature review identifying strengths, limitations, and research gaps.
Sacker et al. (2024) [14]	AI and explainable AI (XAI) approaches to address cybersecurity challenges in digital twins (DTs)	Taxonomy of AI/XAI methods	Identification of gaps and potential applications for secure DT environments.
Sacker et al. (2023) [15]	AI-driven cybersecurity solutions for complex threats, including malware and phishing	AI-based modeling, adversarial learning	Insights into AI's role in enhancing security intelligence and resilience.
Malatji et al. (2024) [16]	AI Cybersecurity Dimensions (AICD) Framework for understanding AI-driven cyber threats	AICD Framework	AICD Framework as a tool for holistic understanding and practical interventions.
Alqurashi et al. (2024) [17]	Topic modeling to analyze trends in cybersecurity research across academic and industry sources	BERTopic, UMAP, HDBSCAN	Identification of 24 knowledge clusters; increased focus on malware and mitigation strategies.

This paper proposes an approach that combines expert systems [18] with a fuzzy linguistic description [19] of intermediate project results, followed by a fuzzy logical inference [20,21] to guide the selection of subscenarios for future project execution. By leveraging expert knowledge about new threats and emerging information security technologies, this method enables accurate risk predictions, facilitating scientifically grounded decision-making in the adaptive management of cybersecurity projects.

3. Models and Methods for Assessing Information Security Management in Organizations

In line with the concept of performance management (also known as results-oriented management) [22], we define the goal of a cybersecurity project as achieving specific, planned values for the organization's information security management indicators. Thus, the project's indicative information model can be represented as a series of project indicators C across all stages t_i, $i = 1, 2, \ldots, I$, of the project's implementation:

$$M = \langle C(t_i), i = 1, 2, \ldots, I \rangle \tag{1}$$

In alignment with the framework provided in [23], cybersecurity indicators are considered to address key tasks in secure information management. These tasks include the structured assignment and distribution of roles to support trust among personnel and the establishment of effective access control and registration management processes [24]. To mitigate malware and cyber threats, antivirus protection tools are emphasized alongside the responsible use of internet resources [25]. Cryptographic protection for information is implemented to ensure data integrity and confidentiality. Furthermore, the secure execution of information technology processes is supported by comprehensive document management protocols [26]. Lastly, particular attention is given to the handling of personal data, thereby safeguarding privacy and ensuring regulatory compliance.

The assessment of an organization's information security management is determined by a hierarchy of group and individual indicators, as illustrated in Figure 1, which allows the evaluation of compliance with cybersecurity requirements across the following areas

(denoted by a symbol with one index) and subdomains (denoted by a symbol with two indices, where the first reflects the area):

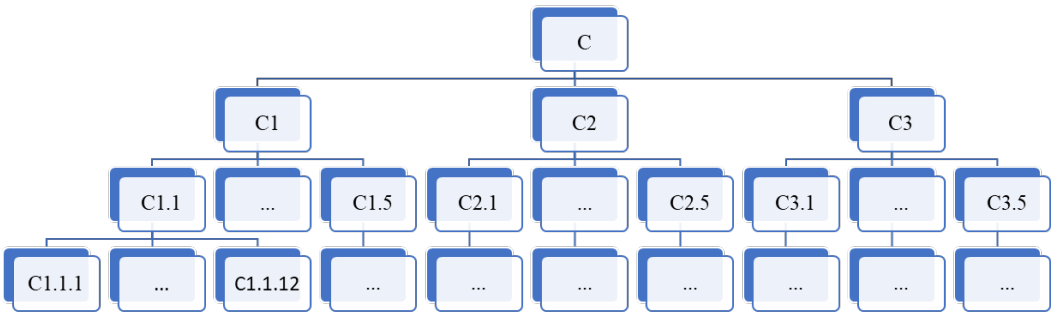

Figure 1. Hierarchical representation of security management metrics.

The framework for cybersecurity management is structured around three core components: the overall organization of the information security service (C1) [27], risk analysis and breach management (C2) [28], and ongoing system analysis and modernization (C3) [29].

The C1 component covers the foundational aspects of information security, focusing on the establishment and operation of the security service. It includes the organization and operational guidelines for the information security team (C1.1) and the precise definition and adjustment of the security system's scope (C1.2). Internal documents governing security activities are developed and updated as needed (C1.3), supporting decision-making processes led by management regarding system implementation and operation (C1.4). Finally, this component emphasizes the importance of staff training and awareness programs to reinforce information [30] security protocols (C1.5).

Risk assessment and management for potential security breaches fall under the C2 component. It begins with selecting and refining approaches for assessing risks (C2.1) and progresses to the development (C2.2) and implementation (C2.3) of detailed risk management plans. Additionally, this component encompasses the detection and response to security incidents (C2.4) as well as continuity planning to ensure the organization's operational resilience and recovery capabilities after disruptions (C2.5), which is relevant not only for cybersecurity incidents but also for other types of disruptions. This broader applicability aligns with C1.1.11 and suggests the need for a more flexible structure, such as a directed acyclic craph (DAG), to effectively represent the interdependencies within continuity and recovery planning

Continuous improvement in and assessment of the security system define the C3 component. Routine monitoring and control of security measures are prioritized (C3.1), along with internal (C3.2) and external audits (C3.3) for evaluating system integrity. Performance is periodically reviewed (C3.4), supplemented by management reviews to ensure alignment with strategic goals (C3.5). Decision-making is conducted on both tactical (C3.6) and strategic (C3.7) levels to guide immediate and long-term improvements, ensuring the system evolves with emerging cybersecurity needs.

Within this hierarchy, each two-level indicator corresponds to a group of primary three-level indicators, which are derived from expert evaluations. For instance, the indicator C1.1 encompasses several three-level indicators, each reflecting different aspects of the organization and functioning of the information security service, as detailed below:

The C1.1 standards outline essential conditions for the effective operation and governance of an organization's information security service. These begin with ensuring the security team has sufficient personnel capable of implementing, operating, controlling, and maintaining the information security system effectively (C1.1.1), complemented by the adequacy of resources required to achieve defined security goals and objectives (C1.1.2). A dedicated budget is critical for supporting the operational and strategic needs of the service (C1.1.3).

The authority of the information security service plays a crucial role, enabling it to organize, prepare, and control the execution of security plans (C1.1.4). Additionally, the service must hold the right to propose necessary modifications to the organization's overall security policy (C1.1.5) and implement changes to internal documents governing security protocols (C1.1.6). Setting security requirements across the organization falls under its purview (C1.1.7), as does ensuring compliance with these policies, especially for employees with elevated access privileges (C1.1.8).

The information security service must also be empowered to monitor security-related events (C1.1.9) and participate actively in investigating incidents, including recommending sanctions for unauthorized actions (C1.1.10). In the event of disruptions, the service plays a critical role in restoring information systems (C1.1.11) and contributes to the ongoing creation, maintenance, and enhancement of the organization's security systems (C1.1.12).

The values of the three-level indicators (e.g., C1.1.1–C1.1.12) are determined on a scale from 0 to 1 based on expert surveys. Each expert evaluates these indicators according to the following set of values: {0; 0.25; 0.5; 0.75; 1.0}, as shown in Table 2. The numerical values reflect the expert's judgment on various aspects of the organization's information security performance.

Table 2. Correspondence between numerical indicator values and expert judgments.

Numerical Value	Expert Judgment
0	No compliance
0.25	Low compliance
0.5	Medium compliance
0.75	High compliance
1.0	Full compliance

If there are several experts (denoted as N, which is preferred), the complete set of experts, $Ex = \{ex_n, n = 1, 2, \ldots, N\}$, is divided into disjoint classes, $Ex_j, j = 1, 2, \ldots, J$. Each class is assigned a weighting coefficient w_j, reflecting the relative importance of the judgments from the experts in that class, where w is a probability vector.

The following conditions for weight coefficients are satisfied:

- $w_j \geq 0, \quad j = 1, 2, \ldots, J$ (non-negativity condition);
- $w_1 + w_2 + \cdots + w_J = 1$ (normalization condition).

The numerical value of an indicator is calculated as the weighted average of expert evaluations. For example, the value of indicator $C_{1.1.1}$ is determined by the formula

$$C_{1.1.1} = \sum_{\mathrm{j}=1}^{\mathrm{J}} \sum_{\mathrm{n}=1}^{\mathrm{N}} \left(v_{jn} \cdot w_j \cdot C_{1.1.1n} \right) \tag{2}$$

where $C_{1.1.1n}$ is the evaluation of indicator $C_{1.1.1}$ by expert ex_n, and v_{jn} is an indicator showing the membership of expert ex_n to class Ex_j: $v_{jn} = 1$ if $ex_n \in Ex_j$, and $v_{jn} = 0$ otherwise.

Transitioning from third-level (three-index) indicators to second-level (two-index) indicators involves summing over the last index, while maintaining weighted summation. The weighting coefficients correspond to the relative significance of the third-level indicators. For instance, the indicator for the organization and functioning of the information security service $C_{1.1}$ is calculated as

$$C_{1.1} = \sum_{j} \sum_{e \in Ex_j} w_e \cdot C_{1.1.1e}. \tag{3}$$

Here, $C_{1.1.r}$ is a third-level indicator related to $C_{1.1}$ ($r = 1, 2, \ldots, 12$), and $w_{1.1.r}$ ($w_{1.1.r} \geq 0$) is the corresponding weighting coefficient for $C_{1.1.r}$. The following condition holds for the weighting coefficients, where w is a probability vector:

$$w_{1.1.1} + w_{1.1.2} + \cdots + w_{1.1.12} = 1 \tag{4}$$

The transition from second-level to first-level indicators also follows the weighted summation approach. For example, the overall organization of the information security service C_1 is determined by

$$C_1 = \sum_{r=1}^{5} (w_{1.r} \cdot C_{1.r}) \tag{5}$$

where $C_{1.r}$ is a second-level indicator related to C_1 ($r = 1, 2, \ldots, 5$), and $w_{1.r}$ ($w_{1.r} \geq 0$) is the weighting coefficient for $C_{1.r}$. The following condition applies:

$$w_{1.1} + w_{1.2} + \cdots + w_{1.5} = 1 \tag{6}$$

To determine the weight coefficients, standard methods for processing expert opinions can be used, such as ranking methods [31] or paired/multiple comparison methods [32].

In the following stages of the project, we will limit our analysis to a system of integral indicators $C = \langle C_1, C_2, C_3 \rangle$, where the values are determined through a hierarchical transition based on expert evaluations.

4. Results and Discussion

4.1. Project Scenario Network

The project is modeled as a time-ordered sequence of cybersecurity management measures, each representing a stage in project implementation. At the conclusion of each stage (except the last), adaptive project management allows the subsequent set of measures to be selected based on the following:

- The results of the current and several preceding stages;
- A set of external factors affecting future project implementation.

Thus, the project is described as a scenario network (see Figure 2), which can be represented as a directed acyclic graph with one source (a vertex with zero in-degree) and one sink (a vertex with zero out-degree).

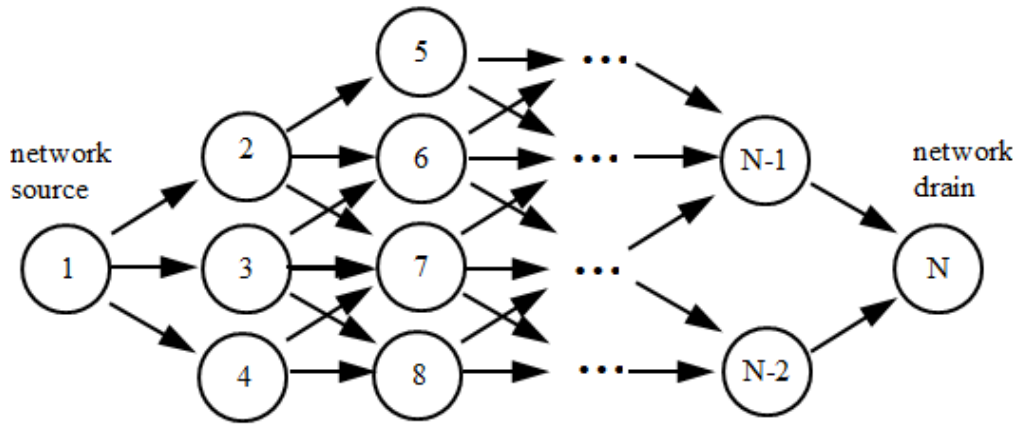

Figure 2. Graphical representation of the project's scenario network (example).

Unlike activity-on-node networks [33], where nodes and edges represent events and actions, the following are the features of a scenario network:

- The vertices of the network correspond to the project stages;
- The arcs indicate the sequence of these stages;
- The network source corresponds to the initial stage;
- The network sink corresponds to the final stage.

The trajectory of the project is the path from the network's source to the sink.

4.2. Fuzzy Linguistic Description of Project Indicators and External Factors

At the end of stage t, the project outcomes are described as

$$C(t) = \langle C_1(t), C_2(t), C_3(t) \rangle \tag{7}$$

Along with these outcomes, we consider a system of external factors $FACT(t, \tau)$, which affect the implementation of the subsequent τ stages:

$$FACT(t, \tau) = \langle Fact_k(t+1), Fact_k(t+2), \ldots, Fact_k(t+\tau) \rangle \tag{8}$$

where K ($k = 1, 2, \ldots, K$) represents the number of external factors. The influence of information security threats can also be considered among these factors, with numerical estimates derived from the approach in [34].

However, numerical values alone do not capture the significance of project indicators and external factors for future implementation. Experts can assess their significance verbally, using terms such as "Low", "Medium", and "High". This leads to the introduction of linguistic variables for project indicators and external factors, defined as

$$LingC_1(t) = \langle NameC_1, Un, T_{base}, G, M_{C_1}(t) \rangle \tag{9}$$

$$LingFact_k(t) = \langle NameLingFact_k, Un, T_{base}, G, M_{Fact_k}(t) \rangle \tag{10}$$

where $t = 1, 2, \ldots, T$ and $k = 1, 2, \ldots, K$. Here, $NameC_1, NameLingFact_k$ refer to the names of linguistic variables; $Un = [0, 1]$ represents the numerical values of the indicators and factors; $T_{base} = \{$"Low", "Medium", "High"$\}$ defines the base term set; and G is a set of syntactic rules for generating terms. The membership functions for these terms may be trapezoidal (see Figure 3).

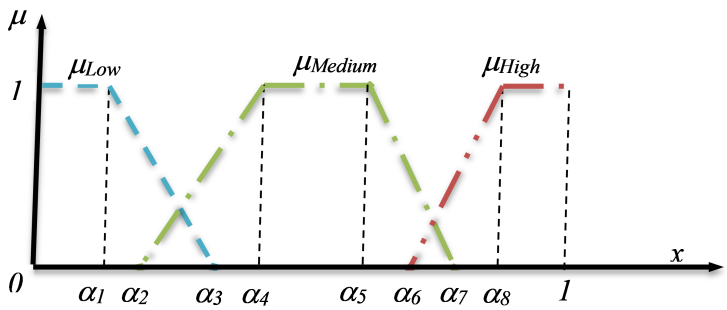

Figure 3. Membership functions $\mu_{Low}, \mu_{Medium}, \mu_{High}$ defining the semantics of linguistic variables $LingC_1(t), LingC_2(t), LingFact_k(t)$ for $k = 1, 2, \ldots, K$.

The semantics of these terms are determined by a vector of parameters:

$$ParIndT_{base}(t) = (\alpha_1(t), \alpha_2(t), \ldots, \alpha_8(t)) \tag{11}$$

where α_1, α_3 define the term "Low"; $\alpha_2, \alpha_4, \alpha_5, \alpha_7$ define "Medium"; and α_6, α_8 define "High". These parameters vary for each linguistic variable $LingC_1(t), LingFact_k(t)$.

For short-term projects, the parameter dependence on project stages can be neglected, assuming $ParIndT_{base}$ remains constant. However, in long-term cybersecurity projects subject to significant instability, adapting the semantics of linguistic terms allows for more accurate descriptions and better-informed management decisions.

5. Accounting for Possible Changes in the Semantics of Verbal Expert Assessments

When utilizing verbal expert assessments for the intermediate results of long-term projects in the field of information security management, it is important to recognize that expert judgments about the levels of indicator values achieved throughout the project's implementation largely depend on the general context associated with the specific phase of

the project. Without loss of generality, we assume that these verbal expert assessments can take values from the following set:

$$T_{\text{base}} = \{L(\text{“Low”}), M(\text{“Medium”}), H(\text{“High”})\} \tag{12}$$

In the current landscape of information security, two major trends are highly relevant:

- Increasing requirements for the level of information security in organizations (enterprises), driven by the rising integration of modern digital technologies into organizational and production activities, which in turn increases the potential damage caused by unauthorized access and other security breaches (*TrendReq*).
- Advancements in the capability to ensure information security within organizations, linked to the development of both organizational legal measures and hardware/software solutions and their application technologies (*TrendCap*).

Consequently, the quantitative values of certain information security management indicators, initially rated as “High” by experts in the early stages of the project, may later be downgraded to “Medium” or even “Low” in subsequent stages. Thus, when planning projects in the field of information security management, a crucial task is forecasting changes in the semantics of basic terms, described by the vector function

$$\text{ParIndT}_{\text{base}}(t) \tag{13}$$

where $t = 1, 2, \ldots, T$ represents the number of the project execution stage.

Given the high level of uncertainty typical of forecasting based on expert opinions, we propose using fuzzy [35] linguistic modeling to address this problem. We introduce linguistic variables LingTrendReq and LingTrendCap, analogous to $\text{LingC}(t)$ and $\text{LingFact}_k(t)$, but with term membership functions defined by a generalized Gaussian function:

$$\mu(x) = \frac{1}{1 + r(\frac{x-\beta}{\sigma})^{2\gamma}} \tag{14}$$

The set of parameters β, σ, γ varies for each basic term of the linguistic variables. The type of membership functions employed is shown in Figure 4.

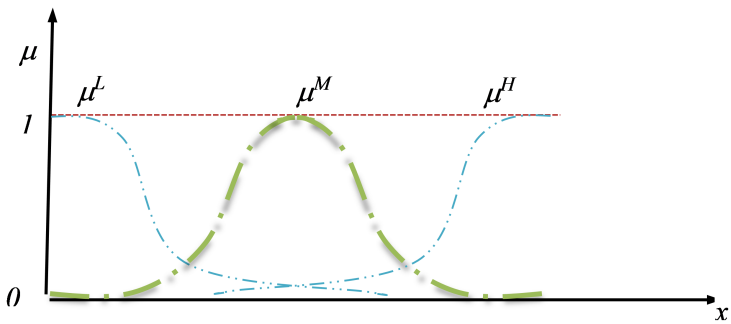

Figure 4. Graphs of membership functions μ_L, μ_M, μ_H, defining the semantics of the terms.

We assume that the relationship between $\text{TrendReq}(t)$, $\text{TrendCap}(t)$, and the values of $\alpha_i(t)$ (for $i = 1, 2, \ldots, 8$) can be described by Sugeno's fuzzy production rules with linear functions on the right-hand sides of the rules. These rules, in this case, have the following form:

$$\text{IF } (\text{TrendReq}(t) = \text{“Low”}, \text{TrendCap}(t) = \text{“Low”})$$
$$\text{THEN } \alpha_i^{LL}(t+1) = \alpha_i^{LL}(t) + \beta_i^{LL}(t) + \gamma_i^{LL}(t)\text{TrendReq}(t) + \delta_i^{LL}(t)\text{TrendCap}(t);$$
$$\text{IF } (\text{TrendReq}(t) = \text{“Low”}, \text{TrendCap}(t) = \text{“Medium”})$$
$$\text{THEN } \alpha_i^{LM}(t+1) = \alpha_i^{LM}(t) + \beta_i^{LM}(t) + \gamma_i^{LM}(t)\text{TrendReq}(t) + \delta_i^{LM}(t)\text{TrendCap}(t);$$

and so forth, for all possible combinations of *TrendReq* and *TrendCap* values. The index t runs from 1 to $T-1$, and $i = 1, 2, \ldots, 8$.

Using these relations, the values of $\alpha_i^s(t)$ (where $s \in S = \{$LL, LM, LH, ML, MM, MH, HL, HM, HH$\}$) are calculated. The parameters $\alpha_i(t)$ are then found as weighted averages of these values, with the weights $v_i^s(t)$ representing the degree of truth of the corresponding fuzzy production rules:

$$\alpha_i(t) = \frac{\sum_{s \in S} v_i^s(t)\alpha_i^s(t)}{\sum_{s \in S} v_i^s(t)} \tag{15}$$

To determine the values of $\alpha_i^s(t)$, a five-layer Takagi–Sugeno–Kang fuzzy neural network is constructed, as shown in Figure 5.

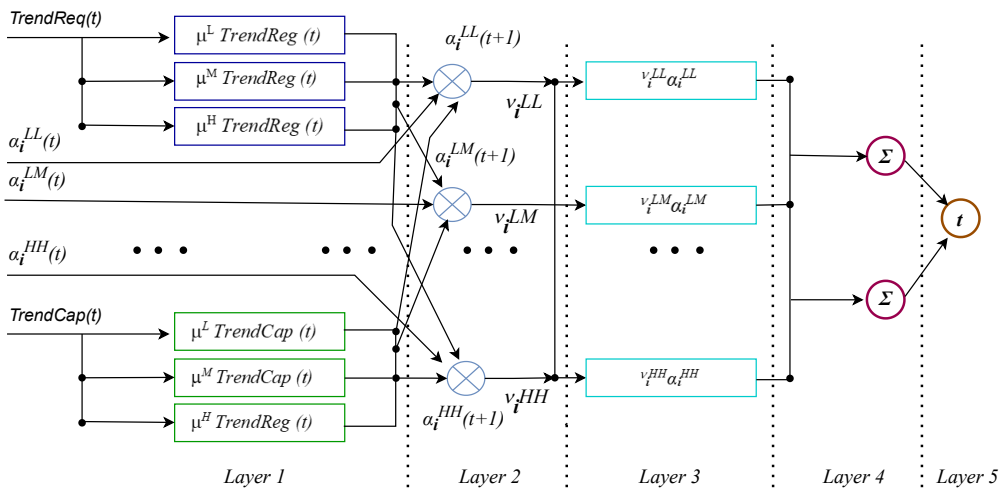

Figure 5. Five-layer Takagi–Sugeno–Kang fuzzy neural network for determining membership function parameters that define the semantics of linguistic variables $\text{LingC}_1(t)$, $\text{LingC}_2(t)$, $\text{LingC}_3(t)$, and $\text{LingFact}_k(t)$.

The inputs to this network are the current parameter values $\alpha_i(t)$, which determine the semantics of the terms at the current stage, along with numerical expert assessments of the trends *TrendReq* and *TrendCap*. The network operates as follows:

- The first layer performs fuzzification by determining generalized Gaussian membership functions for the input values.
- In the second layer, the left-hand sides of the fuzzy production rules are aggregated, calculating v_i^s, and the right-hand functions are computed to find α_i^s;
- The third layer calculates the product of α_i^s and v_i^s for all $s \in S$;
- The fourth layer sums the products $\alpha_i^s v_i^s$ and v_i^s over $s \in S$;
- The fifth layer outputs the next-stage parameter value $\alpha_i(t+1)$.

Training the network is achieved by finding the membership function parameters $\mu_L(x), \mu_M(x), \mu_H(x)$ for the trend variables *TrendReq* and *TrendCap*, as well as the coefficients $\beta_i^s, \gamma_i^s, \delta_i^s$ for the production rules. The training is carried out using the continuous genetic algorithm (CGA) developed by Abo-Hammour [36], which can be optimized using advanced strategies such as hybrid tournament–roulette selection [37] and adaptive control of new generation formation [38].

6. Decision Support for Selecting a Subscenario in Project Implementation

Given the specifics of cybersecurity projects, we introduce simplifying assumptions to limit the class of graphical project descriptions under consideration:

- **Lim1:** Equinitiality and equifinality (all scenarios have a common initial and final stage);

- **Lim2:** Existence of a basic scenario (the main scenario is defined, and resources are calculated for its implementation; all other scenarios are treated as deviations from the basic scenario);
- **Lim3:** Limited branching (branching stages are only part of the basic scenario);
- **Lim4:** Limited merging (subscenarios starting from a branching stage must conclude at a stage in the basic scenario before the next branching);
- **Lim5:** Limited subscenarios (each branching stage produces four types of subscenarios: optimistic, basic, pessimistic, and catastrophic).

A graphical representation of a fragment of the project's structural model, considering these limitations (**Lim1** to **Lim5**), shows the branching into optimistic (**OS**), basic (**BS**), pessimistic (**PS**), and catastrophic (**CS**) subscenarios, with a final stage that may not achieve the project's goals. This model is illustrated in Figure 6.

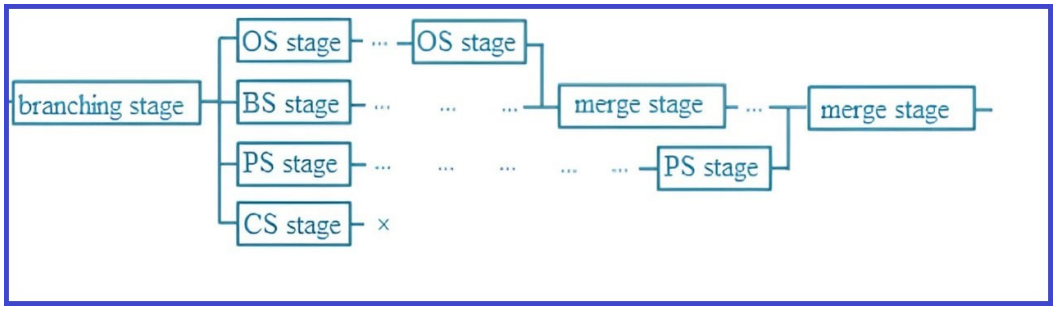

Figure 6. Fragment of the project's structural model considering limitations **Lim1** to **Lim5**.

The target indicative model at the branching stage is described by a set of target indicators C_1, C_2, C_3, evaluated at the current stage t and several previous stages, up to memory depth h:

$$C(t,h) = \langle\langle C_1, C_2, C_3\rangle(t), \langle C_1, C_2, C_3\rangle(t-1), \ldots, \langle C_1, C_2, C_3\rangle(t-h)\rangle \tag{16}$$

The decision rule for selecting a subscenario is expressed through a system of fuzzy production rules:

$$\eta_{\text{Optim}} \text{ if } F_{\text{Optim}} \text{ then ContrInd–Optim}, \quad \eta_{\text{Base}} \text{ if } F_{\text{Base}} \text{ then ContrInd–Base}, \tag{17}$$

$$\eta_{\text{Pessim}} \text{ if } F_{\text{Pessim}} \text{ then ContrInd–Pessim}, \quad \eta_{\text{Catastr}} \text{ if } F_{\text{Catastr}} \text{ then ContrInd–Catastr}, \tag{18}$$

where $\eta_{\text{Optim}}, \eta_{\text{Base}}, \eta_{\text{Pessim}}, \eta_{\text{Catastr}}$ are the confidence degrees of the respective rules (ranging from 0 to 1), and *ContrInd* is a linguistic variable that takes values from the set {Optim, Base, Pessim, Catastr}. The formulas $F_{\text{Optim}}, F_{\text{Base}}, F_{\text{Pessim}}, F_{\text{Catastr}}$ are fuzzy propositional formulas concerning the target indicators $C(t,h)$ and external factors $\text{FACT}(t,\tau)$ corresponding to each subscenario.

The precise forms of these functions are determined by the specific characteristics of the project, and they can be viewed as a knowledge model of the project's subject area. To select a subscenario based on these production rules, we propose using the Mamdani algorithm without defuzzification. The process flow is shown in Figure 7.

The iterative nature of the procedure involves gradually increasing the memory depth h. The stopping condition is triggered by the decision-maker (e.g., when the solutions from the current and previous iterations coincide), ensuring the use of minimal memory depth. The procedure provides the decision-maker with results in the form

$$\big\langle(\text{Optim}, \mu_{\text{Optim}}), (\text{Base}, \mu_{\text{Base}}), (\text{Pessim}, \mu_{\text{Pessim}}), (\text{Catastr}, \mu_{\text{Catastr}})\big\rangle \tag{19}$$

where $\mu_{\text{Optim}}, \mu_{\text{Base}}, \mu_{\text{Pessim}}, \mu_{\text{Catastr}}$ represent the degree of preference for each subscenario (ranging from 0 to 1). This approach not only offers a recommended subscenario but also

provides additional information on the confidence in the recommendation, allowing the decision-maker to factor in personal experience and non-formalized preferences.

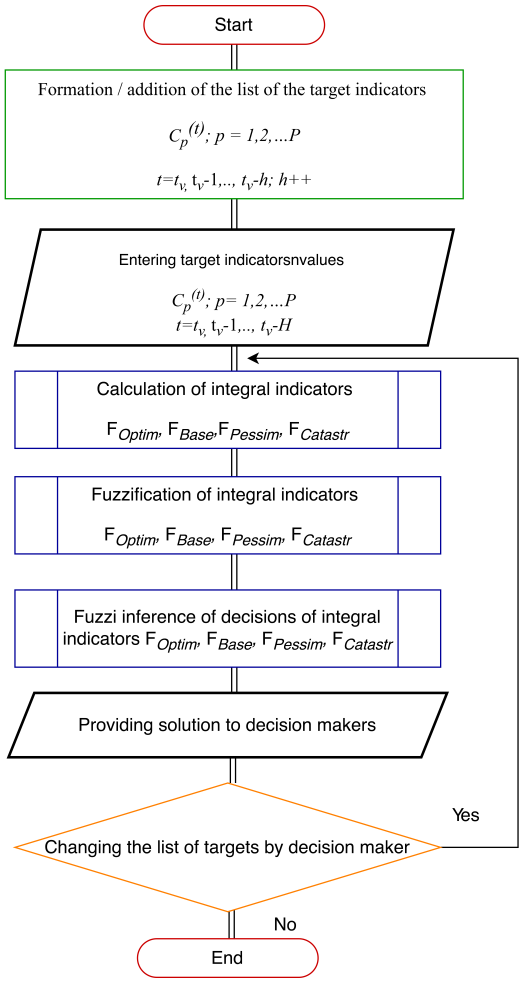

Figure 7. Iterative decision-making procedure for selecting project subscenarios.

However, it is important to note that increasing memory depth at the branching stage may result in error accumulation in input data, potentially affecting the solution's quality. Therefore, decision-makers should be allowed to iteratively modify the list of target indicators and adjust memory depth to improve outcomes.

As part of the evaluation of the developed decision support tools, computational experiments were conducted to identify errors in subscenario selection caused by input data inaccuracies. The true values of the integral control indicator *ContrInd* were represented by samples $x_i, i = 1, 2, \ldots, N$ of a uniformly distributed random variable in the range $[0, 1]$, while the error $e_i, i = 1, 2, \ldots, N$ was sampled from a normally distributed random variable N(0,0.1). The possible decisions are presented in Table 3.

Table 3. Decisions for selecting the base scenario.

	Really Optim	**Really Base**	**Really Pessim**
Defined as Optim	T- O	F-O+	–
Defined as Base	F-P-	T-P	F-P+
Defined as Pessim	–	F-O-	T-O

In this table, negative superscripts indicate underestimation of project results, while positive superscripts indicate overestimation.

Table 4 compares error rates between crisp and fuzzy selection of project subscenarios.

Table 4. Comparison of error rates in crisp and fuzzy selection of subscenarios.

	T- P	T-O	T-O	F-P+	F-P-	F-O+	F-O-
Crisp Selection	0.461	0.083	0.292	0.024	0.046	0.041	0.053
Fuzzy Selection	0.483	0.079	0.296	0.018	0.044	0.029	0.051

Since the most critical errors are false positives (*F-P+*, *F-O+*), which are less frequent with fuzzy inference, and the other error rates are nearly identical, the proposed fuzzy approach is preferable for subscenario selection.

7. Conclusions

In this study, we developed a hierarchy of project indicators in cybersecurity management and proposed methods for determining their values. We applied fuzzification to the project's integral indicators, enabling a linguistic description of the project. Based on these linguistic values at the branching stage, fuzzy production rules were formulated to guide the selection of subscenarios, ensuring adaptability in project management. Decision support was implemented through the Mamdani fuzzy inference procedure [20,39].

The comparison of error rates between crisp and fuzzy methods in computational experiments demonstrated a 25% reduction in errors when using fuzzy procedures. Future research may focus on enhancing decision support tools by incorporating additional forms of uncertainty (e.g., using the Z-number approach) and leveraging modern simulation methods for discrete system behavior.

Author Contributions: Conceptualization, V.T. and I.M.; data curation, D.E.; formal analysis, V.T., V.L., A.L., D.E., and A.G.; funding acquisition, A.B., V.N., and A.G.; investigation, V.N., A.G., and I.M.; project administration, A.B., V.N., and A.G.; resources, A.L.; software, V.L.; supervision, A.B., V.N., and A.G.; validation, V.L., A.L., and D.E.; writing—original draft, V.T. and V.L.; writing—review and editing, I.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding

Institutional Review Board Statement: Not applicable

Informed Consent Statement: Not applicable

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Peltier, T.R. *Information Security Risk Analysis*, 3rd ed.; CRC Press Taylor & Francis Group: Boca Raton, FL, USA, 2005.
2. Seacord, R.C.; Householder, A.D. A Structured Approach to Classifying Security Vulnerabilities. 2005. Available online: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=6baac91ec76b059d7d7807c6706d8279d5afac08 (accessed on 26 September 2024).
3. Kuzminykh, I.; Ghita, B.; Sokolov, V.; Bakhshi, T. Information Security Risk Assessment. *Encyclopedia* **2021**, *1*, 602–617. [CrossRef]
4. Hoffmann, R.; Napiórkowski, J.; Protasowicki, T.; Stanik, J. Risk Based Approach in Scope of Cybersecurity Threats and Requirements. *Procedia Manuf.* **2020**, *44*, 655–662. [CrossRef]
5. Yusif, S.; Hafeez-Baig, A. A Conceptual Model for Cybersecurity Governance. *J. Appl. Secur. Res.* **2021**, *16*, 490–513. [CrossRef]
6. Gordon, L.; Loeb, M.; Zhou, L. Investing in Cybersecurity: Insights from the Gordon-Loeb Model. *J. Inf. Secur.* **2021**, *7*, 49–59. [CrossRef]
7. Lee, I. Cybersecurity: Risk Management Framework and Investment Cost Analysis. *Bus. Horizons* **2021**, *64*, 659–671. [CrossRef]
8. Franco, M.F.; Lacerda, F.M.; Stiller, B. A Framework for the Planning and Management of Cybersecurity Projects in Small and Medium-Sized Enterprises. *Rev. GestãO Proj. (GeP)* **2022**, *13*, 10–37. [CrossRef]
9. Dobrynin, A.; Gudkov, M.; Koinov, R. A Precedent Approach to Incident Management in Automated Process Control Systems. *Softw. Syst. Comput. Methods* **2020**, *2020*, 45–52. [CrossRef]
10. Kulakov, S.; Trofimov, V.; Dobrynin, A.; Taraborina, E. Precedent Approach to the Formation of Programs for Cyclic Objects Control. *IOP Conf. Ser. Mater. Sci. Eng.* **2018**, *354*, 012002. [CrossRef]

11. Sarker, I.H.; Janicke, H.; Ferrag, M.A.; Abuadbba, A. Multi-aspect rule-based AI: Methods, taxonomy, challenges and directions toward automation, intelligence and transparent cybersecurity modeling for critical infrastructures. *Internet Things* **2024**, *25*, 101110. [CrossRef]
12. Sun, N.; Ding, M.; Jiang, J.; Xu, W.; Mo, X.; Tai, Y.; Zhang, J. Cyber threat intelligence mining for proactive cybersecurity defense: A survey and new perspectives. *IEEE Commun. Surv. Tutor.* **2023**, *25*, 1748–1774. [CrossRef]
13. Sharma, S.; Arjunan, T. Natural Language Processing for Detecting Anomalies and Intrusions in Unstructured Cybersecurity Data. *Int. J. Inf. Cybersecur.* **2023**, *7*, 1–24.
14. Sarker, I.H.; Janicke, H.; Mohsin, A.; Gill, A.; Maglaras, L. Explainable AI for cybersecurity automation, intelligence and trustworthiness in digital twin: Methods, taxonomy, challenges and prospects. *ICT Express* **2024**, *10*, 935–958. [CrossRef]
15. Sarker, I.H. Multi-aspects AI-based modeling and adversarial learning for cybersecurity intelligence and robustness: A comprehensive overview. *Secur. Priv.* **2023**, *6*, e295. [CrossRef]
16. Malatji, M.; Tolah, A. Artificial intelligence (AI) cybersecurity dimensions: A comprehensive framework for understanding adversarial and offensive AI. In *AI and Ethics*; Spinger: Berlin/Heidelberg, Germany, 2024; pp. 1–28.
17. Alqurashi, F.; Ahmad, I. A data-driven multi-perspective approach to cybersecurity knowledge discovery through topic modelling. *Alex. Eng. J.* **2024**, *107*, 374–389. [CrossRef]
18. Kozhakhmet, K.; Bortsova, G.; Inoue, A.; Atymtayeva, L. Expert System for Security Audit Using Fuzzy Logic. In Proceedings of the Midwest Artificial Intelligence and Cognitive Science Conference, Cincinnati, OH, USA, 21–22 April 2012; Kazakh-British Technical University: Almaty, Kazakhstan, 2012
19. Zadeh, L.A. The Concept of a Linguistic Variable and its Application to Approximate Reasoning. *Inf. Sci.* **1975**, *1*, 119–249. [CrossRef]
20. Zadeh, L. A Note on Z-Numbers. *Inf. Sci.* **2011**, *181*, 2923–2932. [CrossRef]
21. Khorasani, E.S.; Patel, P.; Rahimi, S.; Houle, D. An Inference Engine Toolkit for Computing with Words. *J. Ambient. Intell. Humaniz. Comput.* **2013**, *4*, 409–410. [CrossRef]
22. Vignieri, V. Performance Management in the Public Sector. In *Global Encyclopedia of Public Administration, Public Policy, and Governance*; Springer International Publishing: Cham, Switzerland, 2018; pp. 1–8.
23. The Standard of the Bank of Russia STO BR IBBS-1.2-2014: Ensuring Information Security of Organizations of the Banking System of the Russian Federation. 2014. Available online: https://cbr.ru/statichtml/file/59420/st-12-14.pdf (accessed on 28 October 2024).
24. Patwary, A.A.N.; Naha, R.K.; Garg, S.; Battula, S.K.; Patwary, M.A.K.; Aghasian, E.; Amin, M.B.; Mahanti, A.; Gong, M. Towards secure fog computing: A survey on trust management, privacy, authentication, threats and access control. *Electronics* **2021**, *10*, 1171. [CrossRef]
25. Aslan, Ö.; Aktuğ, S.S.; Ozkan-Okay, M.; Yilmaz, A.A.; Akin, E. A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics* **2023**, *12*, 1333. [CrossRef]
26. Das, M.; Tao, X.; Liu, Y.; Cheng, J.C. A blockchain-based integrated document management framework for construction applications. *Autom. Constr.* **2022**, *133*, 104001. [CrossRef]
27. Pizam, A.; Ozturk, A.B.; Hacikara, A.; Zhang, T.; Balderas-Cejudo, A.; Buhalis, D.; Fuchs, G.; Hara, T.; Meira, J.; Revilla, R.G.M.; et al. The role of perceived risk and information security on customers' acceptance of service robots in the hotel industry. *Int. J. Hosp. Manag.* **2024**, *117*, 103641. [CrossRef]
28. Santos-Olmo, A.; Sánchez, L.E.; Rosado, D.G.; Serrano, M.A.; Blanco, C.; Mouratidis, H.; Fernández-Medina, E. Towards an integrated risk analysis security framework according to a systematic analysis of existing proposals. *Front. Comput. Sci.* **2024**, *18*, 183808. [CrossRef]
29. Jomhari, N.; Alias, N.A.A.; Ellah, A.A.A.; Magableh, A.A.; Ghazali, E.M. A Multi-Criteria Decision-Making for Legacy System Modernization With FUCOM-WSM Approach. *IEEE Access* **2024**, *12*, 48608–48619. [CrossRef]
30. Liu, Y.; Hu, Y.; Shen, K.; Qiu, J.; Neusypin, K.A. Integral Reinforcement Learning-Based Angular Acceleration Autopilot for High Dynamic Flight Vehicles. *Appl. Soft Comput.* **2024**, *158*, 111582. [CrossRef]
31. Adam, F.; Humphreys, P. *Encyclopedia of Decision Making and Decision Support Technologies*; Hershey: New York, NY, USA, 2008; Volume 1.
32. Saaty, T.L. Relative Measurement and Its Generalization in Decision Making: Why Pairwise Comparisons Are Central in Mathematics for the Measurement of Intangible Factors - The Analytic Hierarchy/Network Process. *Rev. R. Span. Acad. Sci. Ser. A Math.* **2008**, *102*, 251–318. [CrossRef]
33. Burkov, V.N.; Burkova, I.V.; Gorgidze, I.A.; Burkov, V.N.; Burkova, I.V.; Gorgidze, I.A.; Gochitashvili, L.I.; Kajaia, T.N.; Lominadze, T.N.; Khartishvili, M.P. The Method of Network Programming for the Project Management. In *Information and Computer Technologies—Theory and Practice: Proceedings of the International Scientific Conference ICTMC-2010 Devoted to the 80th Anniversary of I.V. Prangishvili*; Nova Science Publishers Inc.: Hauppauge, NY, USA, 2012; pp. 131–147
34. Lomazov, V.A.; Gostischeva, T.V.; Klimova, N.A. Fuzzy Threat Analysis and the Choice of Options for the Information Security System of an Innovative Project. *Mod. High-Tech Technol.* **2017**, *10*, 26–31.
35. Ptuskin, A.; Levner, E.; Kats, V. Cyclic Multi-Hoist Scheduling with Fuzzy Processing Times in Flexible Manufacturing Lines. *Appl. Soft Comput.* **2024**, *165*, 112014. [CrossRef]
36. Russell, S.J.; Norvig, P. *Artificial Intelligence: A Modern Approach*; Prentice Hall: Englewood Cliffs, NJ, USA, 2020.

37. Takagi, T.; Sugeno, M. Fuzzy Identification of Systems and Its Applications to Modeling and Control. *IEEE Trans. Syst. Man, Cybern.* **1985**, *SMC-15*, 116–132. [CrossRef]
38. Sugeno, M.; Kang, G. Structure Identification of Fuzzy Model. *Fuzzy Sets Syst.* **1988**, *28*, 15–33. [CrossRef]
39. Kang, B.; Wei, D.; Li, Y.; Deng, Y. Method of Converting Z-Number to Classical Fuzzy Number. *J. Inf. Comput. Sci.* **2012**, *9*, 703–709.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.