symmetry

MDPI

Article

Fuzzy Logic and Its Application in the Assessment of Information Security Risk of Industrial Internet of Things

Seyit Kerimkhulle [1,*], Zhulduz Dildebayeva [2], Akylbek Tokhmetov [1,*], Akzhibek Amirova [1], Jamalbek Tussupov [1], Ulzhan Makhazhanova [1], Alibek Adalbek [1], Roman Taberkhan [1], Alma Zakirova [1] and Alua Salykbayeva [3]

[1] Department of Information Systems, L.N. Gumilyov Eurasian National University, 2, Satpayev Street, Astana 010008, Kazakhstan
[2] Department of Economics and Business, International Engineering Technological University, 89/21, Al-Farabi Avenue, Almaty 050060, Kazakhstan
[3] Department of Supply Chain Management, Tengizchevroil LLP, 3, Satpayev Street, Atyrau 060001, Kazakhstan
* Correspondence: kerimkul_sye@enu.kz (S.K.); tokhmetov_at_2@enu.kz (A.T.); Tel.: +7-701-391-7252 (S.K.); +7-705-651-7480 (A.T.)

Abstract: This article addresses the issue of information security in the Industrial Internet of Things (IIoT) environment. Information security risk assessment in the IIoT is complicated by several factors: the complexity and heterogeneity of the system, the dynamic nature of the system, the distributed network infrastructure, the lack of standards and guidelines, and the increased consequences of security breaches. Given these factors, information security risk assessment in the IIoT requires a comprehensive approach adapted to the peculiarities and requirements of a particular system and industry. It is necessary to use specialized risk assessment methods and to take into account the context and peculiarities of the system. The method of information security risk assessment in the IIoT, based on the mathematical apparatus of fuzzy set theory, is proposed. This paper analyzes information security threats for IIoT systems, from which the most significant criteria are selected. The rules, based on which decisions are made, are formulated in the form of logical formulas containing input parameters. Three fuzzy inference systems are used: one to estimate the probability of threat realization, another to estimate the probable damage, and a final one to estimate the information security risk for the IIoT system. Based on the proposed method, examples of calculating the information security risk assessment in the IIoT environment are provided. The proposed scientific approach can serve as a foundation for creating expert decision support systems for designing IIoT systems.

Keywords: IIoT; security; threat; risk; fuzzy logic application; linguistic variables; fuzzy decision making

Citation: Kerimkhulle, S.; Dildebayeva, Z.; Tokhmetov, A.; Amirova, A.; Tussupov, J.; Makhazhanova, U.; Adalbek, A.; Taberkhan, R.; Zakirova, A.; Salykbayeva, A. Fuzzy Logic and Its Application in the Assessment of Information Security Risk of Industrial Internet of Things. *Symmetry* **2023**, *15*, 1958. https://doi.org/10.3390/sym15101958

Academic Editor: Saeid Jafari

Received: 16 September 2023
Revised: 18 October 2023
Accepted: 19 October 2023
Published: 23 October 2023

1. Introduction

With the rapid evolution of the Industrial Internet of Things (IIoT), there is an urgent need to swiftly respond to, detect, and prevent intrusions. IIoT systems possess specialized features and encounter unique challenges when it comes to defending against cyber-attacks. Information security (IS) risk assessment plays a pivotal role in enterprise management practices, aiding in the identification, quantification, and mitigation of risks based on risk tolerance criteria and organizational objectives.

The necessity of a quick response to intrusions and their timely detection and prevention have arisen during the rapid development of the IIoT. IIoT systems have special features and face unique challenges working with cyber-attacks. IS risk assessment is an important part of the enterprise management practice that helps to identify, quantify, and minimize threats according to organizational risk acceptance criteria and goals.

The most extensive IIoT security research has been made in [1–3]. Hofer [1] presented a late 10-year review on cyber-physical systems architecture considering the concept of

Industry 4.0. Using an initial automatic search and iterative refinement, 213 papers were found and studied. In result, the vast majority of architectural styles were categorized and schematized. It is concluded that there is a general increase in security-oriented cyber-physical systems architecture proposals, but no discussion on security in detail. In [2], authors focus on the concepts of the IoT, the Industrial IoT, and Industry 4.0, emphasize issues related to their security and privacy, and present a systematic review of current studies and potential directions for addressing the challenges of the Industrial IoT. The same review article [3] provides a systematic literature review on IIoT security from 2011 until 2019, focusing on IIoT security requirements. Special attention is given to options where the relatively new Fog computing paradigm can be used to fulfil these requirements and serve to enhance IIoT security. Furthermore, it should be noted that in the aforementioned studies, the authors argue that the traditional security strategy is insufficient and not ready to protect modern IIoT systems.

In continuation of the topic, authors [4] pay attention to the fact that IT infrastructure threat identification models—such as Microsoft STRIDE (STRIDE is an acronym that describes the six major threats to information security: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service и Elevation of Privilege), OWASP (Open Web Application Security Project), and ENISA (European Network and Information Security Agency)—fully describe the threats of the Internet of Things, but cannot fully identify the threats of the Industrial IoT. This raises a concern related to determining the correct classification of threats to industrial systems. The first step towards threat qualification in industrial systems was made by authors [5]. The study analyzed potential security threats for industries adapting to IIoT. A taxonomy of IIoT attacks was proposed, which would aid in risk—, according to the authors. This taxonomy was considered in terms of four dimensions: attack vector, attack target, attack impact, and attack consequence. However, the disadvantage of this taxonomy is the limited number of threats considered, which does not allow one to fully cover the whole picture of the situation. Authors [6] considered the development of this direction, namely, some types of threats such as spoofing, SQL injection, and DOS attacks on the five-level IIoT architecture. The authors stated that further research is required to obtain a more accurate and complete classification of threats in the IIoT. Considering security models, two main groups can be distinguished: preventive models designed for risk assessment and existing models designed to detect attacks. After the research, it can be stated that there are a significant number of qualitative studies with proposed systems for detecting anomalies and attacks. Various tools such as graph-based methods, blockchain technology, and machine learning algorithms have been used for this purpose [7–10].

IIoT systems have their own dynamics and uniqueness correlated to new approaches for adopting risk assessment because they require special attention. At the moment, there are few studies on this topic. Let us consider a few studies, emphasizing the most significant of them. Authors of [11] proposed an Analytic Hierarchy Process (AHP)-based risk assessment model for IIoT cloud technology. IIoT cloud is a combination of machines, robotic arms, controllers, and drivers in a single platform. This IIoT network risk assessment method is particularly valuable for the core hardware on which cloud services are executed. On other hand, the model does not provide a new solution for decision making and does not address IIoT system assets identification and classification issues. According to [12], the IEC 62443 cybersecurity standard was proposed to implement a cyber-defense platform for industrial IoT systems. This standard contains a set of instructions and measures that need to be implemented to ensure not only the industrial system security but also the operational one. The paper proposes a new approach based on IEC 62443-3-2 and IEC 62443-4-2 to verify, through an in-depth risk assessment, the compliance of objects with basic security requirements. However, despite the advantages described in the paper, the assessment model does not consider security requirements such as system integrity and resource availability, and the model does not propose measures to address the effects of threats on the IIoT system. In [13], it is pointed out that the protection of industrial equipment of IIoT

systems is an obligation inherently linked to technological developments and IoT usage, which makes it important to identify the main vulnerabilities and associated risks and threats and to propose the most appropriate countermeasures. In this paper, a description of attacks on IIoT systems is presented, as well as a thorough analysis of solutions to these attacks as they have been proposed in the most recent sources. Authors [14] proposed a fuzzy association rule extraction algorithm based on a fuzzy matrix, and this is applied to the correlation of security events in a network environment. In addition, the embedded system is combined to build an IS risk assessment system and the performance of the system is specified according to the real situation.

An interesting approach to cyber risks in the mining industry is presented in [15]. The mentioned article discusses a method of cyber-attack risk analysis for different levels of automation in mining routines based on the use of fuzzy theory. The focus is a method that combines the Kaplan and Garrick approach and fuzzy theory. Fuzzy theory is implemented to estimate the risk parameters for the cyber-attack scenario execution in the mining industry. The proposed method can be used to identify the current state of the cybersecurity of mine shafts. The article [16] focuses on IS risk assessment and its importance to enterprise management. The authors point out that IS risk assessment helps to identify, quantify, and evaluate risks with respect to risk tolerance criteria and in-organizational objectives. The article also discusses various methods and tools for IS risk assessment such as Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVA), the CCTA Risk Analysis and Management Method (CRAMM), and risk surveillance. These are based on risk analysis, cost-benefit analysis, security subsystem selection, construction and testing, and examination of all aspects of security.

The review of articles on cybersecurity risk assessment methods/models confirms the importance and relevance of studying the problem of the IS of the industrial IoT, such as threat classification and security risk analysis of IIoT systems. An analysis of the studies indicates that a significant amount of research is dedicated to identifying the security measures, but the issue of preventive measures, including analysis and taxonomy of IS risks, is poorly studied.

The IIoT emerges as a network encompassing physical devices, machinery, sensors, and other elements of industrial production. These entities exchange data and interact with control systems to optimize and automate production processes. This paper introduces a method for evaluating IS within the IIoT environment, leveraging the principles of fuzzy logic [17].

Various standards and methods are used in assessing IS risks in the IIoT, including:

- ISO 27400:2022 [18]: This standard offers guidance on principles, information risk assessment, and appropriate IS and privacy controls to mitigate risks associated with the Internet of Things.
- ISA/IEC 62443 [19]: A series of international standards established by the IEC (International Electrotechnical Commission) specifying cybersecurity requirements for Automated Industrial Process Control Systems (APCSs) and Building Control and Management Systems (BCMSs).
- NIST SP 800-XX series of standards [20–22]: These standards provide security recommendations tailored to industrial control systems, considering their unique performance, reliability, and security requirements. The series encompasses various risk assessment methods and approaches.

This paper is organized as follows. Section 2 is devoted to the description of the methodology and algorithms used in the development of the proposed fuzzy information security risk assessment model for the IIoT environment. Section 3 presents the key findings and results of the study aimed at addressing information security issues in the IIoT environment. Section 4 discusses and compares different approaches to information security risk assessment. Some limitations of the study, practical implications, and suggestions for future research are given in the last chapter “Conclusions”.

2. Proposed Methodology

The purpose of this study is to develop a model for determining the level of risk of information security of the industrial IoT environment using a fuzzy logic system.

According to [20], risk is a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function—the adverse impacts that would arise if the circumstance or event occurs and the likelihood of occurrence. In [21], risk is the product of the probability of a security incident occurring and the damage that will be caused to the organization due to the incident. The probability of a security incident occurring depends on the probability that a threat will occur and the probability that the threat will be able to exploit vulnerabilities in the system successfully. We combine the latter two factors into the probability of a threat occurring and obtain the formula:

$$R = Y_1 \cdot Y_2 \quad (1)$$

where R—risk level, Y_1—probability of a threat occurring, Y_2—level of inflicted damage.

Correctly defining risk criteria is an important step in the risk assessment process as it allows a more accurate determination of the likelihood of risks occurring and the level of potential damage. In addition, identifying risk criteria is also an important step for the subsequent planning and implementation of risk management measures.

According to ISO/IEC 27005:2022 information security, cybersecurity, and privacy protection [22], criteria designed to assess the likelihood of threats occurring include:

1. Asset attractiveness;
2. Asset availability;
3. Asset value;
4. Asset confidentiality;
5. Asset integrity;
6. Software and technical controls;
7. Administrative controls;
8. Procedural controls;
9. Compliance of control measures with information security standards;
10. Previous incidents.

Asset attractiveness is a characteristic that indicates how appealing a particular asset is to potential wrongdoers who may attempt unauthorized access to the asset or its information.

Asset availability is a characteristic that describes how easily access to an asset can be obtained. In other words, if an asset is easily accessible, the probability of threat realization will be very high for that asset.

Asset value is a characteristic that shows how important an asset is to the organization. The value of an asset can be determined by its cost or its significance to the organization's business processes. If an asset has high value, it can lead to a higher probability of threat realization.

Asset confidentiality is a characteristic that reflects the degree of importance in maintaining the confidentiality of information related to the asset. Thus, if an asset is a source of confidential information, it can make it more attractive to potential wrongdoers.

Asset integrity is a characteristic that shows that the asset remains in its original state and is not subject to unauthorized changes or damage. If an asset has high integrity, it maintains its properties and functionality for an extended period without alterations.

Additionally, the first five criteria (asset attractiveness, asset availability, asset value, asset confidentiality, asset integrity) have been consolidated into a single criterion—asset significance, which facilitates the analysis and understanding of asset security within the IIoT system. The inclusion of these criteria into one comprehensive asset assessment criterion is due to their interdependence and their consolidated impact on asset assessment in the context of information security.

For the same reason, the four criteria: (1) software and technical control, (2) administrative control, (3) procedural control, and (4) compliance with information security standards have been consolidated into a single criterion—existing control, as these criteria describe the level of control existing within the organization.

As the third criterion, we have chosen previous incidents. This criterion evaluates whether attacks have been previously committed on the specific asset of an industrial IoT system. If they have, the probability of a threat occurrence will be higher because the wrongdoer is already familiar with this asset and may use past attack experience for the next one.

According to the Factor Analysis of Information Risk (FAIR) methodology [23], criteria designed to assess potential damage include:

1. Damage related to equipment replacement costs;
2. Downtime-related damage to the system;
3. Damage associated with response costs;
4. Reputational damage.

The first three criteria collectively impact financial damage; hence, we consolidated them into the "Financial Damage" criterion.

The "Reputational Damage" criterion reflects potential negative consequences for a company's reputation in the event of risky situations. It represents a kind of "non-material" damage, and we have designated it as a separate criterion, "Reputational Damage". Therefore, we have chosen two criteria to assess the level of incurred damage: Financial Damage and Reputational Damage (non-material losses).

Considering the selected criteria, a fuzzy model was developed to assess the level of information risk in industrial IoT systems. This model divides the process of assessing information risk into three sequential stages. In the first stage, the probability of threats occurring, Y_1, is evaluated. In the second stage, the assessment of damage inflicted on the protected assets of IIoT systems, Y_2, is calculated. In the third stage, the information security risk assessment, R, is computed.

In the process of implementing algorithms for assessing the probability of the occurrence of a threat and the level of inflicted damage, according to the standards and recommendations [18–22], it is necessary to compose input and output linguistic variables—membership functions of the corresponding analytical types. Next, it is necessary to create a rule base—a set of logical expressions that define a cause-and-effect relationship between input and output values. In conclusion, we carry out defuzzification—the calculation of a clear output value based on the resulting membership function of the output block. In particular, the following term sets are used here:

- Very Low (VL);
- Low (L);
- Medium (M);
- High (H);
- Very High (VH).

The next step in the research is:

- Determining the weights of input linguistic variables, the essence of which is to determine the weight of each input linguistic variable in the rule base. To calculate the weight of each criterion, the method of paired comparisons is used [24]. After filling in the matrix of paired comparisons, the eigenvector is calculated, and this makes it possible to find the weights of the criteria of linguistic variables. These, in turn, are used to calculate the risks of information security.
- Implementation of the information security risk assessment model based on fuzzy logic. This takes place in two research stages:
- Formation of a base of fuzzy production rules to determine the assessment of the probability of occurrence of a threat and assess the level of inflicted damage caused

both in interval values and in describing the nature of the risk in the following categories:

  - Very low risk;
  - Low risk;
  - Medium risk;
  - High risk;
  - Very high risk.

- Evaluation of the correctness of the risk level determination model, which summarizes the studies by obtaining the value:
- The probability of occurrence of threats and the level of possible damage, and
- The risk of information security of the industrial IoT environment.

3. Results

This section presents the key findings and results of the study aimed at solving information security problems in the IIoT environment. There are many factors that complicate the assessment of information security risks in the IIoT, such as system complexity, heterogeneity, agility, distributed infrastructure, a lack of standards and guidelines, and the increasing potential consequences of a security breach. The authors propose a comprehensive method for assessing information security risks based on the application of fuzzy set theory and the method of hierarchy analysis. The work analyzes information threats to IIoT systems and identifies the most significant criteria. A description of two fuzzy inference systems is presented, used to assess the likelihood of a threat occurring and the potential damage, on the basis of which an assessment of information security in the context of the IIoT is made. The authors also provide specific examples illustrating risk assessment calculations for information security in the IIoT environment based on the proposed method.

3.1. Algorithm for Assessing the Probability of Occurrence of a Threat

To assess the probability of occurrence of a threat, it is necessary to select input linguistic variables (LVs). According to standards and recommendations [18–22], the most preferable are the following LVs:

- C_1—asset attractiveness;
- C_2—existing control;
- C_3 —previous incidents.

The output variable is Y_1—*Probability of a threat occurring*. For linguistic evaluation of input and output variables, the following term sets are used: Very Low (VL); Low (L); Medium (M); High (H); Very High (VH). When setting input and output LVs, it is necessary to set membership functions for fuzzy sets that characterize the term sets of LVs.

Criteria 1: C_1—asset attractiveness. To assess attractiveness, a questionnaire was used with answers "Yes" or "No":

$$C_1 = \begin{cases} 1, & \text{if "Yes"}, \\ 0, & \text{if "No"}, \end{cases} \quad (2)$$

Indeed, for each of the following questions, an affirmative answer is 1, and a negative answer is 0:

1. Is the asset significant to the organization's business processes?
2. Is the asset important to the achievement of the organization's objectives?
3. Is the asset unique to the organization?
4. Are there alternatives that can replace the asset?
5. Does the asset contain sensitive data?
6. Are there safeguards that protect the confidentiality of the information asset?
7. Is the asset intact and not subject to change?
8. Are there safeguards that protect the integrity of the asset?
9. Is the asset easily accessible to the right users?

10. Are there safeguards that protect the asset from unauthorized access?

The maximum number of points is 10; the minimum is 0. To determine the values of the set of linguistic variables "Attractiveness of an asset", a survey of 10 experts with experience and knowledge in the field of information security was used. The results of the experiment in the form of an auxiliary matrix are presented in Table 1 (10 experts attributed the number of points equal to 1 to the term "Very low" and the number of points equal to 2 to the term "Very low"; 7 experts and 3 experts to the term "Low ", etc.)

Table 1. Auxiliary matrix.

Values of Base Terms	Number of Score									
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Very Low (VL)	10	7	2	0	0	0	0	0	0	0
Low (L)	0	3	7	5	2	0	0	0	0	0
Medium (M)	0	0	1	5	8	6	3	0	0	0
High (H)	0	0	0	0	0	4	5	6	1	0
Very High (VH)	0	0	0	0	0	0	2	4	9	10

To construct membership functions, we identify the maximum elements in the rows of the auxiliary table. The membership function is then calculated using the following formula [17]:

$$\mu(a_{ij}) = \frac{a_{ij}}{a_{imax}}, \tag{3}$$

where a_{ij} is the matrix element and a_{imax} is the maximum element of the row.

From the obtained values of the membership functions of the terms of the linguistic variable C_1 (asset attractiveness), we created Table 2.

Table 2. Resulting matrix.

Values of Base Terms	Number of Score (γ_{ij})									
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Very Low (VL)	1	0.7	0.2	0	0	0	0	0	0	0
Low (L)	0	0.43	1	0.71	0.29	0	0	0	0	0
Medium (M)	0	0	0.125	0.625	1	0.75	0.375	0	0	0
High (H)	0	0	0	0	0	0.5	0.8	1	0.17	0
Very High (VH)	0	0	0	0	0	0	0.2	0.4	0.9	1

Using the data from Table 2, we will plot the membership function LV "Asset attractiveness" (Appendix A, Figure A1).

Criteria 2: C_2,—existing control. The values of the input LV C_2—existing control are determined by the number of security measures in industrial systems and the change in the range [0, 8]. These measures include:

- Protection of network nodes;
- Monitoring of network activity;
- Authentication and authorization;
- Protection from physical attacks;
- Protection against malicious programs;
- Data security;
- Data backup;
- Training.

Hence, the normalized values of the LV C_2 can be determined using Formula (4):

$$C_2 = \frac{N_m}{8}, \tag{4}$$

where N_m—the number of Information Security methods used at an industrial facility—are found in Table 3.

Table 3. Normalized values of C_2.

N_m	1	2	3	4	5	6	7	8
C_2	0.125	0.250	0.375	0.500	0.625	0.750	0.875	1.000

Using the data from Table 3, we will plot the membership function LV "Existing control" (Appendix A, Figure A2).

Criteria 3: C_3—previous incidents. The numeric values of variables C_3—previous incidents—vary in the range [0, 100] and are determined by the percentage of computers attacked in IIoT systems per year and can be expressed by the formula [25]:

$$C_3 = \frac{N_p}{40\%}, \quad (5)$$

where N_p is the percentage of computers attacked in an IIoT system per year, and 40% is the maximum permissible value.

According to the data in Table 4, let us plot the membership functions of the LV "Previous incidents" (Appendix A, Figure A3).

Table 4. Normalized values of C_3.

N_p	5%	10%	15%	20%	25%	30%	35%	40% and Higher
C_3	0.125	0.250	0.375	0.500	0.625	0.750	0.875	1.000

Output variable Y_1—Probability of threat occurrence–is the process of determining the likelihood that a threat will occur in the future. The likelihood of threats being implemented may depend on various factors, such as the importance of information assets, the availability of appropriate security controls at the software, technical, administrative, and procedural control levels, as well as previous cases of security breaches.

Let us define terms for the output LV "Probability of threat occurrence": 'Very Low', 'Low', 'Moderate', 'High', 'Very High'. The descriptions of the terms are provided in Table 5.

Table 5. Description of the terms for the LV "Probability of threat occurrence".

Term	Meaning	Description
Very low	0–0.3	There are no objective prerequisites for the emergence of a threat
Low	0.2–0.5	Some prerequisites for the emergence of a threat exist, but the security measures taken significantly complicate its implementation
Average	0.4–0.7	Objective prerequisites for the emergence of a threat exist, and the number of security measures is sufficient to neutralize it
High	0.6–0.9	Objective prerequisites for the emergence of a threat exist, and the number of security measures is insufficient
Very high	0.8–1	Objective prerequisites for a threat exist, and security measures have not been taken

Using the data from Table 5, we will plot the membership function LV "Probability of threat occurrence" (Appendix A, Figure A4).

As a result, the input linguistic variables for the first stage were set, and the sets of terms and their membership functions were determined. These variables are used to determine the probability of a threat occurrence.

3.2. Algorithm for Assessing the Level of Inflicted Damage

In this section, the following criteria were used to assess the level of inflicted damage caused (input variables):

- C_4—Financial damage;
- C_5—Reputational damage.

The output variable Y_2 reflects the level of inflicted damage.

Criteria 4: C_4,—financial damage. The numerical value of the variable is [0, 100] and it is determined as a percentage of the costs of responding to an attack and restoring systems, fines, the cost of monitoring services, and damage from downtime and disruption of operations. To calculate it, we use the Return on Investment (ROI) method [26]:

$$C_4 = \frac{ALE}{D} \cdot 100\% \quad (6)$$

where ALE is the expected annual losses; D is the annual income. This allows us to obtain normalized values for the fourth criterion of financial damage (see Table 6).

Table 6. Normalized values of C_4.

	1%	**2%**	**3%**	**4%**	**5%**	**6%**	**7%**	**8%**	**9%**	**10%**
C_4	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0

Let us define terms for the output LV "Financial damage": 'Very Low', 'Low', 'Moderate', 'High', 'Very High'. The descriptions of the terms are provided in Table 7.

Table 7. Description of the terms for the LV "Financial damage".

Term	**Description**
Very low	Minor damage, less than 1% of annual income
Low	Low damage, 2–4% of annual income
Average	Noticeable damage, 4–7% of annual income
High	Large damage, 7–10% of annual income
Very high	Very large damage, more than 10% of annual income

Using the data from Table 7, we will plot the membership function LV "Financial damage" (Appendix A, Figure A5).

Criteria 4: C_5—Reputational damage. The numerical value of the variable [0, 100] is determined as a percentage of losses due to the negative attitude of customers, partners, and investors towards the company. Let us try to estimate reputational damage as expected losses due to the negative attitude of clients, partners, and investors, divided by annual income [27]:

$$C_5 = \frac{P}{D} \cdot 100\%, \quad (7)$$

where P reflects losses due to the negative attitude of customers, partners, and investors towards the company over the past year; D reflects annual income. This allows us to obtain normalized values for the fifth criterion of reputational damage (see Table 8).

Table 8. Normalized values of C_5.

	1%	**2%**	**3%**	**4%**	**5%**	**6%**	**7%**	**8%**	**9%**	**10%**
C_5	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0

We understand that reputational damage is difficult to quantify and such an estimate will be approximate. However, this approach can help estimate how much of an organization's annual revenue could be lost due to reputational damage following a cyberattack.

Let us define terms for the output LV "Reputational damage": 'Very Low', 'Low', 'Moderate', 'High', 'Very High'. The descriptions of the terms are provided in Table 9.

Table 9. Description of the terms for the LV "Reputational damage".

Term	Description
Very low	Minor damage, less than 1% of annual income
Low	Low damage, 2–4% of annual income
Average	Noticeable damage, 4–7% of annual income
High	Large damage, 7–10% of annual income
Very high	Very large damage, more than 10% of annual income

Using the data from Table 9, we will plot the membership function LV "Reputational damage" (Appendix A, Figure A6).

The output variable Y_2—the level of inflicted damage is the process of determining the financial, operational, reputational, and other losses that may arise as a result of an information security breach. Potential damage is the sum of all the costs that an organization will incur in the implementation of threats to the assets of an industrial IoT system.

Let us define terms for the output LV "Level of inflicted damage": 'Very Low', 'Low', 'Moderate', 'High', 'Very High'. The descriptions of the terms are provided in Table 10.

Table 10. Description of the terms for the LV "Level of inflicted damage".

Term	Meaning	Description
Very low	0–0.3	The level of damage caused has virtually no effect on the operation of the facility
Low	0.2–0.5	The level of damage caused slightly affects the operation of the facility
Average	0.4–0.7	The level of damage caused makes it difficult for the facility to operate
High	0.6–0.9	The level of damage caused has a significant impact on the operation of the facility
Very high	0.8–1	The level of damage caused greatly affects the operation of the facility

Using the data from Table 10, we will plot the membership function LV "Level of inflicted damage" (Appendix A, Figure A7).

As a result, the input linguistic variables for the second stage were set, and the sets of terms and their membership functions were determined. With the help of these variables, the level of inflicted damage is determined. The output LV "Level of inflicted damage" was also set, and term-sets were defined and described.

3.3. Determining the Weights of Input Linguistic Variables

To assess the risk of information security, it is necessary to determine the weight for each input linguistic variable in the rule base. Let n elements or n objects be given. Then the calculation of the weight of each criterion is made using the method of paired comparisons—a statistical tool that is used to assess the relative preferences between different options or alternatives [17]. Based on the results of the expert's survey, a matrix of paired comparisons is built $= (a_{ij}), i, j = 1, 2, \ldots, n$:

$$A = (a_{ij})_{i,\, j=1,\, 2,\, \ldots,\, n} = \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{bmatrix}, \quad (8)$$

where the number a_{ij} shows how many times, according to the expert, the degree of importance of one element x_i is greater than the degree of importance of element x_j in the set S, or in terms of the membership function, the value $\mu_s(x_i)$ is greater than $\mu_s(x_j)$. At the same time, the expert operates with these concepts guided by the comparison scale according to the Saaty method [24] (see Table 11).

Table 11. Scales for comparing two elements according to the Saaty method.

Comparing Two Elements	Value
Both elements are equally important : $\mu_S(x_i)$ equals $\mu_S(x_j)$	1
One element is slightly more important than another element : $\mu_S(x_i)$ is slightly larger than $\mu_S(x_j)$	3
One element is clearly more important than the other : $\mu_S(x_i)$ is greater than $\mu_S(x_j)$	5
One element is significantly more important than another element : $\mu_S(x_i)$ is noticeably larger than $\mu_S(x_j)$	7
One element is absolutely more important than another element : $\mu_S(x_i)$ is much larger than $\mu_S(x_j)$	9
Values intermediate in degree between those listed	2, 4, 6, 8

The elements of the matrix of paired comparisons, symmetrical with respect to the diagonal of the matrix, must satisfy the requirement:

$$a_{ij} = \frac{1}{a_{ij}}. \tag{9}$$

This condition (8) means that if the membership degree of element x_i is a_{ij} times stronger than the membership degree of element x_j, then the membership degree of element x_j must be $1/a_{ij}$ times stronger than the membership degree of element x_i. Then the problem of constructing the membership function is reduced to finding the eigenvector E of the matrix A corresponding to the largest eigenvalue of the matrix, that is, the vector that is the solution to the equation

$$A \cdot E = E \cdot e_{max} \tag{10}$$

where e_{max} is the largest eigenvalue of a matrix A.

Further, for each element of the matrix of pairwise comparisons, a certain weight ω_i, $i = 1, \ldots, n$, is determined, and the condition $\omega_1 + \ldots + \omega_n = 1$ is satisfied. Then we can construct a matrix V of relative weights:

$$V = (v_{ij})_{i,\, j=1,\, 2,\, \ldots,\, n} = \begin{bmatrix} \omega_1/\omega_1 & \omega_1/\omega_2 & \ldots & \omega_1/\omega_n \\ \omega_2/\omega_1 & \omega_2/\omega_2 & \ldots & \omega_2/\omega_n \\ \vdots & \vdots & \vdots & \vdots \\ \omega_n/\omega_1 & \omega_n/\omega_2 & \ldots & \omega_n/\omega_n \end{bmatrix} \tag{11}$$

where each element $v_{ij} > 0$ of the matrix of relative weights (38) is the ratio of the weight of the i-th object a_i to the weight of the j-th object a_j, i.e., $v_{ij} = \omega_i/\omega_j$ for any $i,\ j = 1,\ 2,\ \ldots,\ n$. Matrix elements located symmetrically with respect to the main diagonal are inverse to each other, i.e., $v_{ij} = 1/v_{ji}$ for any $i,\ j = 1,\ 2,\ \ldots,\ n$.

After filling in the matrix of paired comparisons (38), the eigenvector is calculated, and for this the sum and product method and the square root method are used ([24,25]):

$$e_i = \sqrt[n]{\prod_{j=1}^{n} a_{ij}},\ i = 1,\ 2,\ \ldots, n. \tag{12}$$

Next, to find the weights of the criteria, we use

$$\omega_i = \frac{e_i}{\sum_{j=1}^{n} e_j},\ i = 1,\ 2,\ \ldots, n. \tag{13}$$

In conclusion, we note that on the basis of the implementation of algorithms (8)–(13), we obtained expert and calculated results of the study:

- Expert estimates of respondents (i)–(v) on the values of pairwise comparison coefficients, $e_i^{(\mathrm{i})}, e_i^{(\mathrm{ii})}, \ldots, e_i^{(\mathrm{v})}$, $i = \overline{1,3}$—eigenvector and $\omega_i^{(\mathrm{i})}, \omega_i^{(\mathrm{ii})}, \ldots, \omega_i^{(\mathrm{v})}$, $i = \overline{1,3}$—values of weights according to criteria C_1, C_2 и C_3 (see Tables A1–A3, Appendix A);
- Calculated ω_i, $i = \overline{1,3}$ values of weights estimating the level Y_1—threat occurrence probability (see Table A3, Appendix A);
- Calculated $\omega_i^{(\mathrm{i})}, \omega_i^{(\mathrm{ii})}, \ldots, \omega_i^{(\mathrm{v})}$, and $\omega \cdot i = \overline{4,5}$ values $e_i^{(v)}$ according to criteria C_4 and C_5 assessing the level of Y_2—the damage caused (see Table A4, Appendix A).

3.4. Implementation of the Information Security Risk Assessment Model Based on Fuzzy Logic

3.4.1. Formation of a Base of Fuzzy Production Rules

The rule base of fuzzy inference systems is formed on the basis of predefined input and output linguistic variables. After fuzzy input and output variables, membership functions, as well as weight coefficients of criteria $C_1 - C_5$ were defined, the following were created:

- Information base of fuzzy production rules for evaluating Y_1—probability of occurrence of threats (total 125 rules)—with the values of the terms of the input linguistic variable C_1—attractiveness of assets—with a weight coefficient ω_1 = 0.4126; C_2—existing control—with a weight coefficient ω_2 = 0.3952; C_3—previous incidents—with weight coefficient ω_3 = 0.1929; Very low—0.2, Low—0.4, Medium—0.6, High—0.8; Very high—1.0 and the calculated values of the term boundaries of the output linguistic variable Y_1—probability of occurrence of a threat: Very low—[0.0; 0.3], Low—(0.3; 0.5], Medium—(0.5; 0.7], High—(0.7; 0.9], Very High—(0.9; 1.0]) (see Table A5, Appendix A).
- Aggregate fuzzy rules for assessing the probability of occurrence of a threat. Note that aggregation is the process of combining the output parameters of each rule into one fuzzy set. The rules for aggregating fuzzy products are carried out using the classical fuzzy logical operation "AND" of two elementary statements [24,28]. For example, the output variable Y_1 – the probability of occurrence of a threat occurring–takes on the value "Very Low" in rules No. 1, 2, 3, 6, and 26, which can be combined using a conjunction. As a result of the aggregation of the resulting rules, fuzzy causal relationships between antecedents and consequents were obtained (see Table A6, Appendix A).
- Information base of fuzzy production rules for evaluation Y_2—the level of inflicted damage caused by threats to the protected assets of IIoT systems (total 25 rules)–with the values of the terms of the input linguistic variable C_4—financial costs with a weight coefficient ω_4 = 0.5833 and C_5—damage to reputation with a weight coefficient ω_5 = 0.4167: Very low—0.2, Low—0.4, Medium—0.6, High—0.8; Very high—1.0, and the calculated value of the term boundaries of the output linguistic variable Y_2—manifestation of the damage: Very Low—[0.0; 0.3], Low—(0.3; 0.5), Medium—(0.5; 0.7), High—(0.7; 0.9), Very High—(0.9; 1.0] (see Table A7, Appendix A).
- Aggregated fuzzy rules for assessing the level of inflicted damage caused. As a result of the aggregation of the resulting rules, fuzzy causal relationships between antecedents and consequents were obtained (see Table A8, Appendix A).

As a result, we have obtained bases of fuzzy rules for determining the probability of occurrence of a threat and assessing the level of inflicted damage. These two parameters are used to calculate a clear output value of the risk level R, which has the following gradations:

- Very low risk: [0.0000; 0.0625), meaning a slight adverse impact on the activities of the organization and the assets of the organization;
- Low risk: [0.0625; 0.2025), meaning a limited adverse impact on the activities of the organization and the assets of the organization;

- Medium risk: [0.2025; 0.5625), meaning that threats can have a serious adverse effect on the activities of the organization, the assets of the organization, individuals, and other organizations;
- High risk: [0.5625; 0.7225), meaning that threats can have a serious or catastrophic adverse effect on the activities of the organization and the assets of the organization;
- Very high risk: [0.7225; 1.0000], meaning that threats can lead to multiple serious or catastrophic consequences for the organization's activities and the organization's assets.

3.4.2. Evaluation of the Correctness of the Model for Determining the Level of Risk

We will evaluate the correctness of the proposed information security risk model based on fuzzy logic in three scenarios.

Scenario 1: Average Risk. Let the values of the following linguistic variables arrive at the input of the model system to determine the level Y_1—the probability of occurrence of a threat:

- Attractiveness of assets, $C_1 = 0.25$;
- Existing control, $C_2 = 0.20$;
- Previous incidents, $C_3 = 0.55$.

Then, the fuzzification of five fuzzy statements—"Asset assessment is Very Low", "Asset assessment is Low", "Asset assessment is Medium", "Asset assessment is High" and "Asset assessment is Very High" for the input linguistic variable $C_1 - C_3$ asset assessment—gives the following values of the degree of truth of fuzzy statements:

- Attractiveness of assets, C_1: $\mu_1^{VL}(R) = 0.4$, $\mu_1^{L}(R) = 0.6$, $\mu_1^{M}(R) = 0.0$, $\mu_1^{H}(R) = 0.0$, $\mu_1^{VH}(R) = 0.0$;
- Existing control, C_2: $\mu_2^{VL}(R) = 0.3$, $\mu_2^{L}(R) = 0.7$, $\mu_2^{M}(R) = 0.0$, $\mu_2^{H}(R) = 0.0$, $\mu_2^{VH}(R) = 0.0$;
- Previous incidents, C_3: $\mu_3^{VL}(R) = 0.0$, $\mu_3^{L}(R) = 0.8$, $\mu_3^{M}(R) = 0.2$, $\mu_3^{H}(R) = 0.0$, $\mu_3^{VH}(R) = 0.0$.

Next, we determine the degree of truth of the conditions for each of the rules of the fuzzy inference system:

- If the condition of a fuzzy production rule is a simple fuzzy statement, then the degree of its truth corresponds to the value of the membership function of the corresponding term of the linguistic variable.
- If the condition represents a compound statement, then the degree of truth of the compound statement is determined using the logical operation of conjunction.

Therefore, according to the base of production rules (see Table A5, Appendix A) and the fuzzy inference system based on the conjunction operation (see Table A6, Appendix A), for level Y_1 the probability of occurrence of a threat occurring has a non-zero value for rules 3, 8, 28, and 33:

- Rule 3. Y_1 = M: $\mu(R_3) = \min(0.4; 0.3; 1.0) = 0.3$;
- Rule 8. Y_1 = M: $\mu(R_8) = \min(0.4; 0.7; 1.0) = 0.4$;
- Rule 28. Y_1 = M: $\mu(R_{28}) = \min(0.6; 0.3; 1.0) = 0.3$;
- Rule 33. Y_1 = M: $\mu(R_{33}) = \min(0.6; 0.7; 1.0) = 0.6$.

The truth values of all other rules are zero, so there is no need to take them into account. Indeed, the combination of the membership functions of all subsets is usually carried out classically, that is, by taking the maximum from the values of the membership functions of each subset:

$$\mu\left(R_{Y_1=M}\right) = \max(\mu(R_3); \mu(R_8); \mu(R_{28}); \mu(R_{33})) = 0.6 \quad (14)$$

Then, as a result of defuzzification, we obtain the value of the level of the output linguistic variable Y_1, the probability of occurrence of a threat occurring in the form of a

weighted average value by the degree of membership of values at which all applicable membership functions reach their maximum value (15):

$$Y_1 = \frac{\overline{R}_{Y_1=M} \cdot \mu\left(R_{Y_1=M}\right)}{\mu\left(R_{Y_1=M}\right)} = \frac{0.55 \cdot 0.6}{0.6} = 0.55, \quad (15)$$

where (see Figure A1, the histogram of dotted line with dot):

$$\overline{R}_{Y_1=M} = \frac{\min\limits_{Y_1=M} R + \max\limits_{Y_1=M} R}{2} = \frac{0.4 + 0.7}{2} = 0.55$$

Now, let the input of the system of information security risk assessment models based on fuzzy logic determine the level Y_2 (caused damage) and receive the values of the input parameters:

- Financial costs, $C_4 = 0.67$;
- Damage to reputation, $C_5 = 0.33$.

Then, the fuzzification of fuzzy statements by terms for the input linguistic variables $C_4 - C_5$ of the system of risk assessment models of the output linguistic variable Y_2, level of inflicted damage, gives the following values of the degree of truth of the fuzzy inference system:

- Financial costs, C_4: $\mu_4^{VL}(R) = 0.0$, $\mu_4^{L}(R) = 0.0$, $\mu_4^{M}(R) = 0.3$, $\mu_4^{H}(R) = 0.7$, $\mu_4^{VH}(R) = 0.0$;
- Damage to reputation, C_5: $\mu_5^{VL}(R) = 0.0$, $\mu_5^{L}(R) = 0.2$, $\mu_5^{M}(R) = 0.8$, $\mu_5^{H}(R) = 0.0$, $\mu_5^{VH}(R) = 0.0$.

According to the base of production rules (see Table A7, Appendix A) and the fuzzy inference system based on the conjunction operation (see Table A8, Appendix A), the level Y_2, the level of inflicted damage, has a non-zero value for rules 12, 13, 17, and 18:

- Rule 12. Y_2 = M: $\mu(R_{12})$ = min(0.3; 0.2) = 0.2;
- Rule 13. Y_2 = M: $\mu(R_{13})$ = min(0.3; 0.8) = 0.3;
- Rule 17. Y_2 = M: $\mu(R_{17})$ = min(0.7; 0.2) = 0.2;
- Rule 18. Y_2 = H: $\mu(R_{18})$ = min(0.7; 0.8) = 0.7.

The truth values of all other rules are zero, so there is no need to take them into account. Indeed, the maximum value of the input linguistic variables and the combined value of the membership functions of all subsets, respectively, gives:

$$\begin{gathered} \mu\left(R_{Y_2=M}\right) = \max(\mu(R_{12}); \mu(R_{13}); \mu(R_{17})) = 0.3, \\ \mu\left(R_{Y_2=H}\right) = \max(\mu(R_{18})) = 0.7 \end{gathered} \quad (16)$$

Then, as a result of defuzzification, we will obtain the value of the level of the output linguistic variable Y_2—level of inflicted damage—in the form of a weighted average value by the degree of membership of the values at which all applicable membership functions reach their maximum value (16):

$$\begin{aligned} Y_2 &= \frac{\overline{R}_{Y_2=M} \cdot \mu\left(R_{Y_2=M}\right) + \overline{R}_{Y_2=H} \cdot \mu\left(R_{Y_2=H}\right)}{\mu\left(R_{Y_2=M}\right) + \mu\left(R_{Y_2=H}\right)} \\ &= \frac{0.55 \cdot 0.3 + 0.75 \cdot 0.7}{0.3 + 0.7} = 0.69 \end{aligned} \quad (17)$$

where (see Figure A1, the histogram of dotted line with dot and the histogram of long dotted line):

$$\overline{R}_{Y_2=M} = \frac{\min\limits_{Y_2=M} R + \max\limits_{Y_2=M} R}{2} = \frac{0.4 + 0.7}{2} = 0.55,$$

$$\overline{R}_{Y_2=H} = \frac{\min\limits_{Y_2=H} R + \max\limits_{Y_2=H} R}{2} = \frac{0.6 + 0.9}{2} = 0.75$$

Having determined the values of the probability of the appearance of threats and the level of possible damage by using Formulas (1), (16) and (17), we will find the value of the information security risk:

$$R = Y_1 \cdot Y_2 = 0.55 \cdot 0.69 = 0.38 \quad (18)$$

Thus, we obtained the value which corresponds to the average of the information security risk.

Scenario 2: High Risk. Let the values of the following linguistic variables arrive at the input of the model system:

- Attractiveness of assets, $C_1 = 0.85$;
- Existing control, $C_2 = 0.70$;
- Previous incidents, $C_3 = 0.90$.

Then, fuzzification gives the following values of the degree of truth of fuzzy statements:

- Attractiveness of assets, C_1: $\mu_1^{VL}(R) = 0.0$, $\mu_1^{L}(R) = 0.0$, $\mu_1^{M}(R) = 0.0$, $\mu_1^{H}(R) = 0.5$, $\mu_1^{VH}(R) = 0.5$;
- Existing control, C_2:$\mu_2^{VL}(R) = 0.0$, $\mu_2^{L}(R) = 0.0$, $\mu_2^{M}(R) = 0.08$, $\mu_2^{H}(R) = 0.12$, $\mu_2^{VH}(R) = 0.0$;
- Previous incidents, C_3: $\mu_3^{VL}(R) = 0.0$, $\mu_3^{L}(R) = 0.0$, $\mu_3^{M}(R) = 0.0$, $\mu_3^{H}(R) = 0.2$, $\mu_3^{VH}(R) = 0.6$.

Therefore, according to the base of production rules (see Table A5, Appendix A) and the fuzzy inference system based on the conjunction operation (see Table A6, Appendix A), the level Y_1—the probability of occurrence of a threat occurring—has a non-zero value for rules 89, 90, 94, 95, 114, 115, 119, and 120:

- Rule 89. Y_1 = H: $\mu(R_{89}) = \min(0.5; 0.08; 0.2) = 0.08$;
- Rule 90. Y_1 = H: $\mu(R_{90}) = \min(0.5; 0.08; 0.6) = 0.08$;
- Rule 94. Y_1 = H: $\mu(R_{94}) = \min(0.5; 0.12; 0.2) = 0.12$;
- Rule 95. Y_1 = H: $\mu(R_{95}) = \min(0.5; 0.12; 0.6) = 0.12$;
- Rule 114. Y_1 = H: $\mu(R_{114}) = \min(0.5; 0.08; 0.2) = 0.08$;
- Rule 115. Y_1 = H: $\mu(R_{115}) = \min(0.5; 0.08; 0.6) = 0.08$;
- Rule 119. Y_1 = H: $\mu(R_{119}) = \min(0.5; 0.12; 0.2) = 0.12$;
- Rule 120. Y_1 = VH: $\mu(R_{120}) = \min(0.5; 0.12; 0.6) = 0.12$.

The value of membership functions for all subsets are:

$$\begin{gathered}\mu\left(R_{Y_1=H}\right) = \max(\mu(R_{89}); \mu(R_{90}); \mu(R_{94}); \mu(R_{95}); \mu(R_{114}); \\ \mu(R_{115}); \mu(R_{119})) = 0.12;\ \mu\left(R_{Y_1=VH}\right) = \mu(R_{120}) = 0.12\end{gathered} \quad (19)$$

Then, as a result of defuzzification, we obtain the value of the level of the output linguistic variable Y_1—the probability of occurrence of a threat:

$$\begin{aligned} Y_1 &= \frac{\overline{R}_{Y_1=H} \cdot \mu\left(R_{Y_1=H}\right) + \overline{R}_{Y_1=VH} \cdot \mu\left(R_{Y_1=VH}\right)}{\mu\left(R_{Y_1=H}\right) + \mu\left(R_{Y_1=VH}\right)} \\ &= \frac{0.75 \cdot 0.12 + 0.9 \cdot 0.12}{0.12 + 0.12} = 0.82 \end{aligned} \quad (20)$$

where (see Figure A1, the histogram of long dotted line and the histogram of solid line):

$$\overline{R}_{Y_1=H} = \frac{\min\limits_{Y_1=H} R + \max\limits_{Y_1=H} R}{2} = \frac{0.6+0.9}{2} = 0.75,$$

$$\overline{R}_{Y_1=VH} = \frac{\min\limits_{Y_1=VH} R + \max\limits_{Y_1=VH} R}{2} = \frac{0.8+1.0}{2} = 0.90$$

Now, let the input of the system of information security risk assessment models based on fuzzy logic determine the level Y_2—caused damage—and receive the values of the input parameters:

- Financial costs, $C_4 = 0.50$;
- Damage to reputation, $C_5 = 0.75$.

Then, the fuzzification of fuzzy statements by terms for the input linguistic variables $C_4 - C_5$ of the system of risk assessment models of the output linguistic variable Y_2—level of inflicted damage—gives the following values of the degree of truth of the fuzzy inference system:

- Financial costs, C_4: $\mu_4^{VL}(R) = 0.0$, $\mu_4^{L}(R) = 0.0$, $\mu_4^{M}(R) = 0.0$, $\mu_4^{H}(R) = 0.14$, $\mu_4^{VH}(R) = 0.0$;
- Damage to reputation, C_5: $\mu_5^{VL}(R) = 0.0$, $\mu_5^{L}(R) = 0.0$, $\mu_5^{M}(R) = 1.0$, $\mu_5^{H}(R) = 0.0$, $\mu_5^{VH}(R) = 0.0$.

According to the information base of the production rules (see Table A7, Appendix A) of the fuzzy inference system based on the conjunction operation (see Table A8, Appendix A), the level Y_2—level of inflicted damage—has a non-zero value for Rule 18:

- Rule 18. Y_2 = H: $\mu(R_{18}) = \min(0.14; 1.0) = 0.14$.

The value of membership functions for all subsets are:

$$\mu\left(R_{Y_2=H}\right) = \max(\mu(R_{18})) = 0.14 \tag{21}$$

Then, as a result of defuzzification, we obtain the value of the level of the output linguistic variable Y_2—level of inflicted damage:

$$Y_2 = \frac{\overline{R}_{Y_2=H} \cdot \mu\left(R_{Y_2=H}\right)}{\mu\left(R_{Y_2=H}\right)} = \frac{0.75 \cdot 0.14}{0.14} = 0.75 \tag{22}$$

where (see Figure A1, the histogram of long dotted line):

$$\overline{R}_{Y_2=H} = \frac{\min\limits_{Y_2=H} R + \max\limits_{Y_2=H} R}{2} = \frac{0.6 + 0.9}{2} = 0.75$$

Now determine the values of the probability of the appearance of threats and the level of possible damage by using Formulas (1), (20) and (22), and we will find the value of the information security risk:

$$R = Y_1 \cdot Y_2 = 0.82 \cdot 0.75 = 0.62 \tag{23}$$

Thus, we obtained the value which corresponds to the high information security risk.

Scenario 3: Low Risk. Let the values of the following linguistic variables arrive at the input of the model system:

- Attractiveness of assets, $C_1 = 0.40$;
- Existing control, $C_2 = 0.28$;
- Previous incidents, $C_3 = 0.32$.

Then, fuzzification gives the following values of the degree of truth of fuzzy statements:

- Attractiveness of assets, C_1: $\mu_1^{VL}(R) = 0.0$, $\mu_1^{L}(R) = 0.5$, $\mu_1^{M}(R) = 0.5$, $\mu_1^{H}(R) = 0.0$, $\mu_1^{VH}(R) = 0.0$;
- Existing control, C_2: $\mu_2^{VL}(R) = 0.19$, $\mu_2^{L}(R) = 1.0$, $\mu_2^{M}(R) = 0.0$, $\mu_2^{H}(R) = 0.0$, $\mu_2^{VH}(R) = 0.0$;
- Previous incidents, C_3: $\mu_3^{VL}(R) = 0.21$, $\mu_3^{L}(R) = 1.0$, $\mu_3^{M}(R) = 0.0$, $\mu_3^{H}(R) = 0.0$, $\mu_3^{VH}(R) = 0.0$.

Therefore, according to the base of production rules (see Table A5, Appendix A) and the fuzzy inference system based on the conjunction operation (see Table A6, Appendix A), the level Y_1—the probability of occurrence of a threat occurring—has a non-zero value for rules 89, 90, 94, 95, 114, 115, 119, and 120:

- Rule 26. Y_1 = VL: $\mu(R_{26}) = \min(0.5; 0.19; 0.21) = 0.19$;
- Rule 27. Y_1 = L: $\mu(R_{27}) = \min(0.5; 0.19; 1.0) = 0.19$;
- Rule 31. Y_1 = L: $\mu(R_{31}) = \min(0.5; 1.0; 0.21) = 0.21$;
- Rule 32. Y_1 = L: $\mu(R_{32}) = \min(0.5; 1.0; 1.0) = 0.5$;
- Rule 51. Y_1 = L: $\mu(R_{51}) = \min(0.5; 0.19; 0.21) = 0.19$;
- Rule 52. Y_1 = L: $\mu(R_{52}) = \min(0.5; 0.19; 1.0) = 0.19$;

– Rule 56. Y_1 = L: $\mu(R_{56})$ = min(0.5; 1.0; 0.21) = 0.21;
– Rule 57. Y_1 = L: $\mu(R_{57})$ = min(0.5; 1.0; 1.0) = 0.5.

The value of membership functions for all subsets are:

$$\begin{array}{c}\mu\left(R_{Y_1=VL}\right) = \mu(R_{26}) = 0.19; \mu\left(R_{Y_1=L}\right) = \max(\mu(R_{27}); \\ \mu(R_{31}); \mu(R_{32}); \mu(R_{51}); \mu(R_{52}); \mu(R_{56}); \mu(R_{57})) = 0.5\end{array} \quad (24)$$

Then, as a result of defuzzification, we obtain the value of the level of the output linguistic variable Y_1—the probability of occurrence of a threat:

$$\begin{array}{c}Y_1 = \frac{\overline{R}_{Y_1=VL} \cdot \mu\left(R_{Y_1=VL}\right) + \overline{R}_{Y_1=L} \cdot \mu\left(R_{Y_1=L}\right)}{\mu\left(R_{Y_1=VL}\right) + \mu\left(R_{Y_1=L}\right)} \\ = \frac{0.2 \cdot 0.19 + 0.35 \cdot 0.5}{0.19 + 0.5} = 0.31\end{array} \quad (25)$$

where (see Figure A1, the histogram dot line (VL) and the histogram dotted line (L)):

$$\overline{R}_{Y_1=VL} = \frac{\min\limits_{Y_1=VL} R + \max\limits_{Y_1=VL} R}{2} = \frac{0.1 + 0.3}{2} = 0.2,$$

$$\overline{R}_{Y_1=L} = \frac{\min\limits_{Y_1=L} R + \max\limits_{Y_1=L} R}{2} = \frac{0.2 + 0.5}{2} = 0.35$$

Now, let the input of the system of information security risk assessment models based on fuzzy logic determine the level Y_2—caused damage— and receive the values of the input parameters:

– Financial costs, C_4 = 0.16;
– Damage to reputation, C_5 = 0.84.

Then, the fuzzification of fuzzy statements by terms for the input linguistic variables $C_4 - C_5$ of the system of risk assessment models of the output linguistic variable Y_2—level of inflicted damage—gives the following values of the degree of truth of the fuzzy inference system:

– Financial costs, C_4: $\mu_4^{VL}(R) = 0.4$, $\mu_4^{L}(R) = 0.6$, $\mu_4^{M}(R) = 0.0$, $\mu_4^{H}(R) = 0.0$, $\mu_4^{VH}(R) = 0.0$;
– Damage to reputation, C_5: $\mu_5^{VL}(R) = 0.0$, $\mu_5^{L}(R) = 0.0$, $\mu_5^{M}(R) = 0.0$, $\mu_5^{H}(R) = 0.6$, $\mu_5^{VH}(R) = 0.0$.

According to the base of production rules (see Table A7, Appendix A) and the fuzzy inference system based on the conjunction operation (see Table A8, Appendix A), the level Y_2—level of inflicted damage—has a non-zero value for Rules 4 and 9:

– Rule 4. Y_2 = L: $\mu(R_4)$ = min(0.4; 0.6) = 0.4;
– Rule 9. Y_2 = M: $\mu(R_9)$ = min(0.6; 0.6) = 0.6.

The value of membership functions for all subsets are:

$$\mu\left(R_{Y_2=L}\right) = \mu(R_4) = 0.4,\ \mu\left(R_{Y_2=M}\right) = \mu(R_9) = 0.6 \quad (26)$$

Then, as a result of defuzzification, we obtain the value of the level of the output linguistic variable Y_2—level of inflicted damage:

$$\begin{array}{c}Y_2 = \frac{\overline{R}_{Y_2=L} \cdot \mu\left(R_{Y_2=L}\right) + \overline{R}_{Y_2=M} \cdot \mu\left(R_{Y_2=M}\right)}{\mu\left(R_{Y_2=L}\right) + \mu\left(R_{Y_2=M}\right)} \\ = \frac{0.35 \cdot 0.4 + 0.55 \cdot 0.6}{0.4 + 0.6} = 0.47\end{array} \quad (27)$$

where (see Figure A1, the histogram of dotted line and the histogram of dotted line with dot):

$$\overline{R}_{Y_2=L} = \frac{\min\limits_{Y_2=L} R + \max\limits_{Y_2=L} R}{2} = \frac{0.2 + 0.5}{2} = 0.35,$$

$$\overline{R}_{Y_2=M} = \frac{\min\limits_{Y_2=M} R + \max\limits_{Y_2=M} R}{2} = \frac{0.4 + 0.7}{2} = 0.55$$

Now determine the values of the probability of the appearance of threats and the level of possible damage by using Formulas (1), (25) and (27), and we will find the value of the information security risk:

$$R = Y_1 \cdot Y_2 = 0.31 \cdot 0.47 = 0.15 \quad (28)$$

We obtained the value which corresponds to the low level of information security risk in IIoT systems.

Thus, using test sets of fuzzy input variables, we obtained clear values of information security risk level. Using fuzzy input information, it is possible to predict the deterioration of the system's safety level and make timely decisions to prevent possible dangerous situations.

4. Discussion

Fuzzy logic methods have gained traction in recent research for assessing information risks. For instance, [29] introduces a risk assessment approach grounded in an attack tree model, utilizing both fuzzy set theory and probabilistic risk assessment technology. This innovative method is applied to the context of a ship control system risk scenario within industrial control systems. The analysis commences by identifying potential risks, constructing a tree-like attack model, and subsequently employing triangular fuzzy numbers and expert knowledge to gauge factors influencing end-node probabilities. Through fuzzy arithmetic, interval probabilities for both the root node and attack paths are determined, yielding the overall potential risks and probabilities of occurrence for each attack path.

Intriguingly, [30] explores cybersecurity risk assessment of industrial control systems through a unique lens. The paper proposes a methodology reliant on order divergence which measures α within an intuitionistic fuzzy framework characterized by interval values. Departing from conventional methods, where the weights of risk indices remain constant, this approach adapts a novel order α divergence measure to IVIFNs (Interval Intuitionistic Fuzzy Numbers). The integration of IVIFNs facilitates the description of estimated risk indices, while variable weight vectors derived from divergence closeness determine the weights of risk indices. The study presents strategies for node and attack path integration within attack defense trees, leading to risk scores calculation using a designated score function.

Addressing the significance of cybersecurity risk assessment within IIoT systems, [31] proposes a comprehensive model for dynamic IIoT risk assessment. This model, initiated by defining the IIoT context, encompasses diverse risk calculation algorithms, prominently highlighting approaches grounded in artificial intelligence and machine learning. The methodology's application is demonstrated through a case study involving an IIoT-based supervisory control and data acquisition system in a hydroelectric power plant.

In [32], the focus centers on the development of an access control model that dynamically analyzes the security risk of access requests through contextual IoT information. This model employs real-time contextual data associated with the requesting user to compute security risks for each access request. Attributes of the user, action severity, resource sensitivity, and user risk history are considered as inputs to assess and calculate the risk value, ultimately informing access decisions.

In [33], the authors introduce the IORs (Risk Indicator Objects), a notable contribution that leverages the MITRE ATT&CK knowledge base for ICS (Industrial Control Systems) to facilitate ongoing risk monitoring. This approach enables the utilization of existing variables for continuous risk analysis. IORs extend compromise indicators by integrating detection strategies with probabilistic inference, serving as a powerful tool for quantifying cybersecurity risks. The library, endorsed by professionals from major companies, now encompasses 95 IORs.

A compelling study, [34], proposes a model for vulnerability risk analysis based on the widely accepted CVSS (Common Vulnerability Scoring System). This innovative model addresses two key limitations of CVSS: (1) the need for additional indicators beyond those stipulated by CVSS, and (2) CVSS's primary usage within IT environments, rendering it less suitable for industrial settings. To overcome these issues, the study's first part offers an overview of the key protocols, standards, and buses within the IIoT landscape. The second part establishes a comprehensive framework for risk characterization in industrial environments, effectively addressing the limitations of the CVSS index.

A noteworthy contribution comes from the study outlined in [35], proposing a hierarchical structured model for information security risk assessment utilizing fuzzy logic. This new approach extends to the assessment of software risks in learning management systems. The novel risk assessment model is implemented on the MATLAB platform using fuzzy logic through a set of 15 fuzzy machines.

Similarly, [36] delves into the application of a fuzzy expert system for assessing the security of a University Information System (UIS). The authors employed the Visual Basic language and the MATLAB Fuzzy Logic toolkit to tackle the challenge of assessing compliance with the ISO/IEC 27,001 standard—a key foundation for modeling information system security.

In [37], the authors introduce a robust fuzzy model tailored to conducting information security risk assessment within IIoT systems. This model relies on the additive weighting method to establish weighting coefficients for each criterion and leverages fuzzy logic for its implementation. The authors showcase the practical execution of this model using the MATLAB system. Notably, the authors assert that fuzzy logic offers a suitable technological foundation for discerning information security risks and generating dependable practical outcomes.

In [38], the authors embark on an exploration of the cybersecurity landscape in ICS (Industrial Control Systems). The study encompasses several key aspects: (1) elucidating the fundamental principles and unique attributes underlying ICS functionality; (2) presenting a concise history of cyber-attacks targeting ICSs; (3) providing an overview of ICS security-less assessment; (4) conducting a review of "unique ICS" testbeds designed to capture interactions across different levels of ICSs; and (5) outlining current trends in ICS attack and defense strategies.

Turning attention to [39], the article delves into a critical challenge—assessing the creditworthiness of enterprises operating within the trade and services sector. Notably, this assessment poses particular intricacies for borrowers, especially small businesses. Such evaluation necessitates careful consideration of factors such as the developmental stage of small enterprises, their specific activities, and the inherent uncertainty tied to financial outcomes. The study analyzes an array of indicators, including industry and regional specifics, small enterprise activity measures, and financial and economic metrics pertinent to the service and trade domain. Decision-making rules are meticulously formulated in the shape of logical formulas embedded with crucial parameters.

5. Conclusions

This research is devoted to solving the problem of determining the level of IS risks in industrial IoT systems using fuzzy logic. Risk assessment as part of information security (risk management) is an essential tool in building defenses. The risk assessment process is designed to identify the risk to the system and determine the security measures taken to mitigate the risk. The proposed method is based on a new risk analysis model that takes into account multiple risk criteria, such as the attractiveness of the asset, the level of existing controls, the presence of previous threats, and financial and reputational losses as a result of the realization of threats. The main advantage of this method is that it realistically models the system environment, unlike the conventional risk model, which only considers the probability of an event and its impact.

Our method is based on multiple fuzzy inference system MFIS. The first fuzzy inference system FIS1 calculates the overall probability of the realization of threats on the system. The second fuzzy inference system FIS2 calculates the overall probability of damage to the system based on risk factors. The third step of the fuzzy inference system is to calculate the IS risk level based on the output data FIS1, FIS2. The proposed method can be used as a tool for assessing information security and risk analysis in any system.

In information security and risk analysis, the concept of symmetry plays an important role, which can be considered from the point of view of balance and harmony in information security management. Symmetry in this context can be associated with the balance between security and availability of data and resources. Just as symmetry in nature creates harmony and balance, in information security there is a need to find a balance between security measures that may be too strict and restrictive for users and the availability of data and resources that ensures the effective operation of the system.

Symmetry can also be associated with understanding symmetrical threats that can impact information security. Risk analysis involves identifying such threats and developing symmetrical countermeasures that can ensure balance and harmony in security. When information security incidents occur, symmetry can also be important in the context of the response. A symmetric response to incidents may include similar recovery measures to restore balance and functionality to the system.

Thus, there is a clear connection between the concept of symmetry and information security risk analysis, which manifests itself as the desire for balance and harmony in approaches to security and risk management.

In this paper, we have paid little attention to risk management planning, resolution, and control. More research should be conducted on risk management planning. In addition, risk needs to be re-monitored regularly to track the status of identified risks.

Author Contributions: Conceptualization, S.K. and A.T.; methodology, S.K. and A.T.; software, A.A. (Akzhibek Amirova), R.T. and U.M.; validation, S.K., A.T. and U.M.; formal analysis, Z.D., A.A. (Akzhibek Amirova), J.T., U.M., A.A. (Alibek Adalbek), R.T., A.Z. and A.S.; investigation, Z.D., J.T., A.Z., A.A. (Alibek Adalbek), R.T. and A.S.; resources, Z.D., J.T., A.Z., A.A. (Akzhibek Amirova), R.T. and A.S.; data curation, Z.D., J.T., A.Z. and A.S.; writing—original draft preparation, S.K. and A.T.; writing—review and editing, S.K. and A.T.; visualization, S.K., A.T. and U.M.; supervision, S.K. and A.T.; project administration, U.M.; funding acquisition, S.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Committee of Science of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No. AP09259435).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: We express gratitude to the Science Committee of the Committee of Science of the Ministry of Science and Higher Education of the Republic of Kazakhstan for its support of the realization this research (Grant No. AP09259435).

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

Appendix A

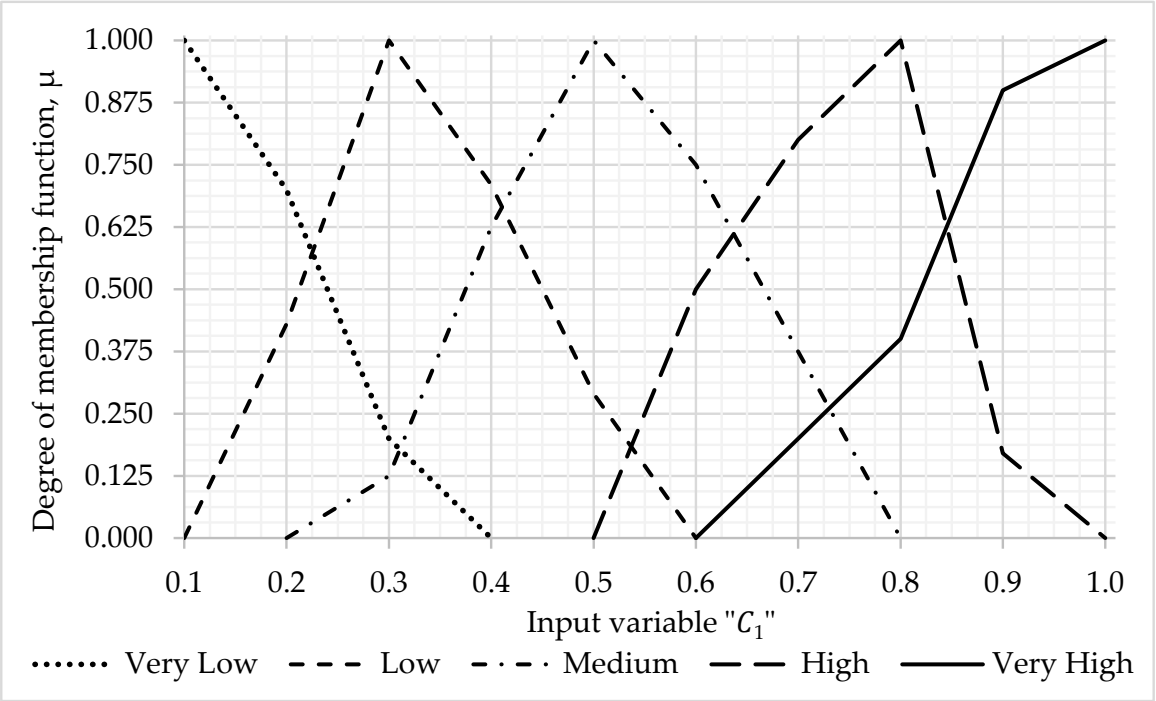

Figure A1. The plot of membership function LV "Asset attractiveness".

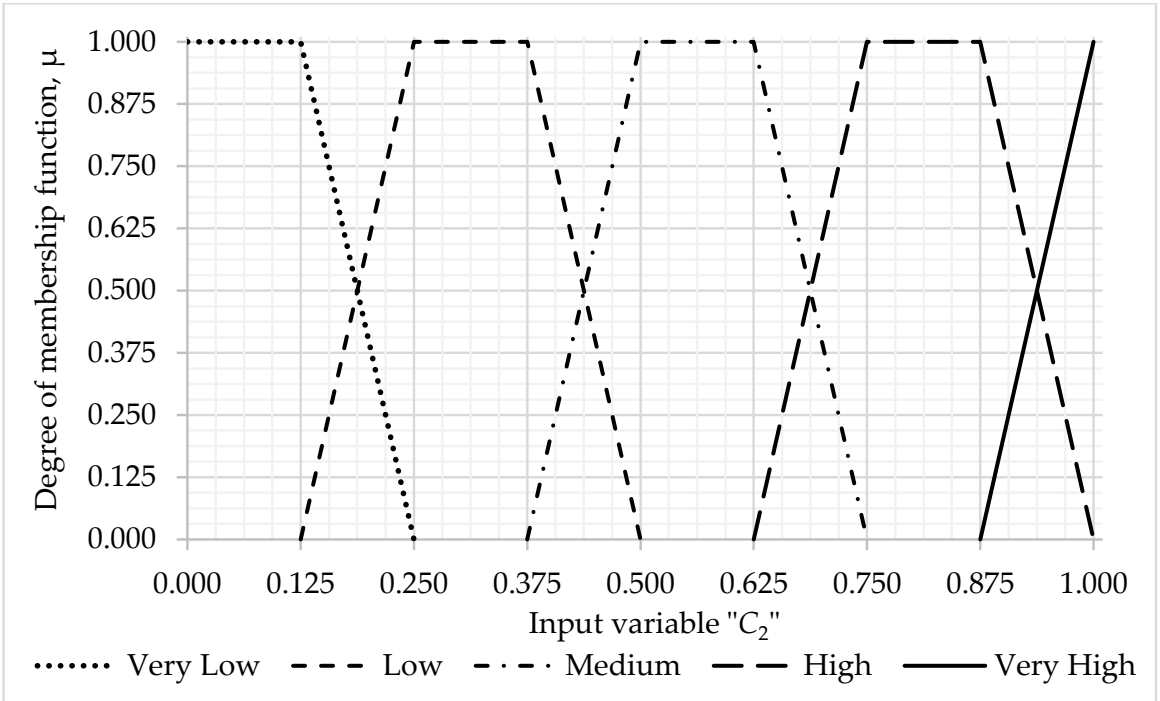

Figure A2. The plot of membership function LV "Existing control".

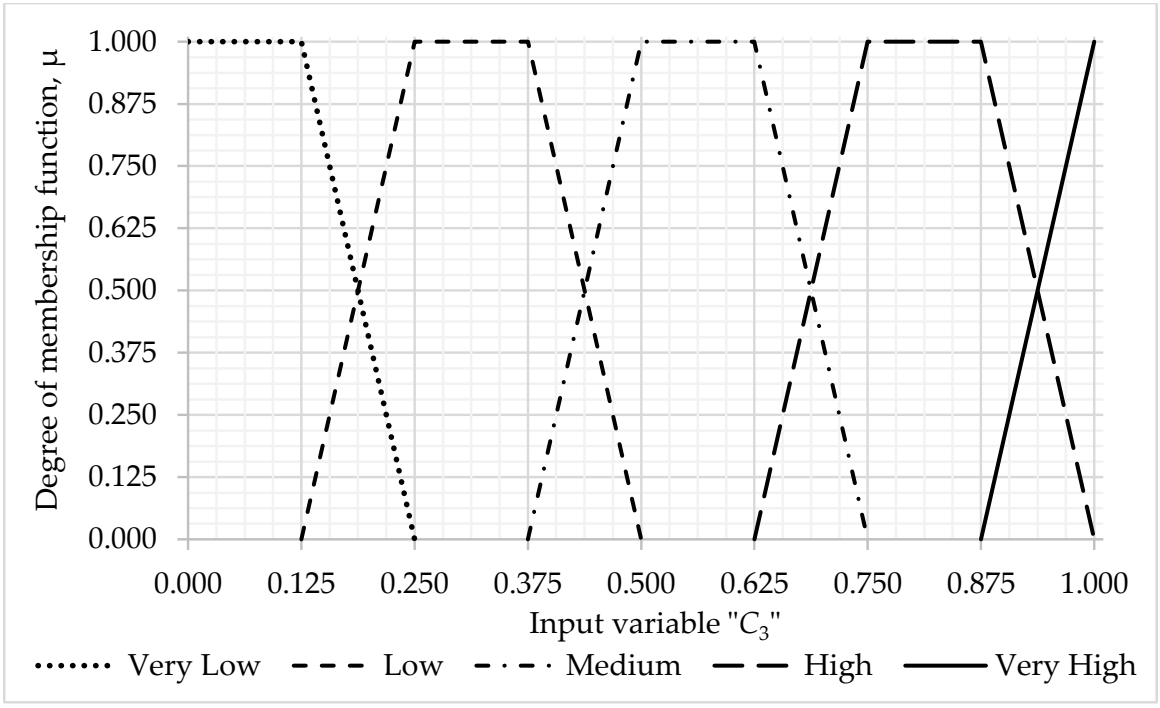

Figure A3. The plot of membership function LV "Previous incidents".

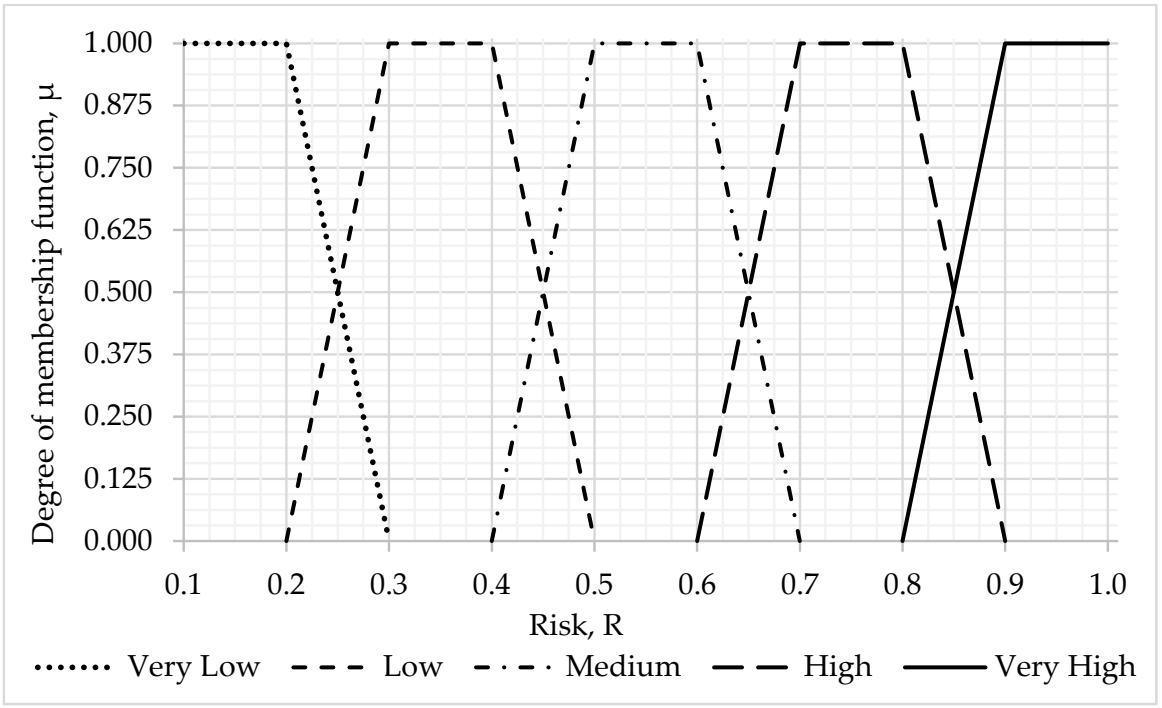

Figure A4. The plot of membership function LV "Probability of threat occurrence".

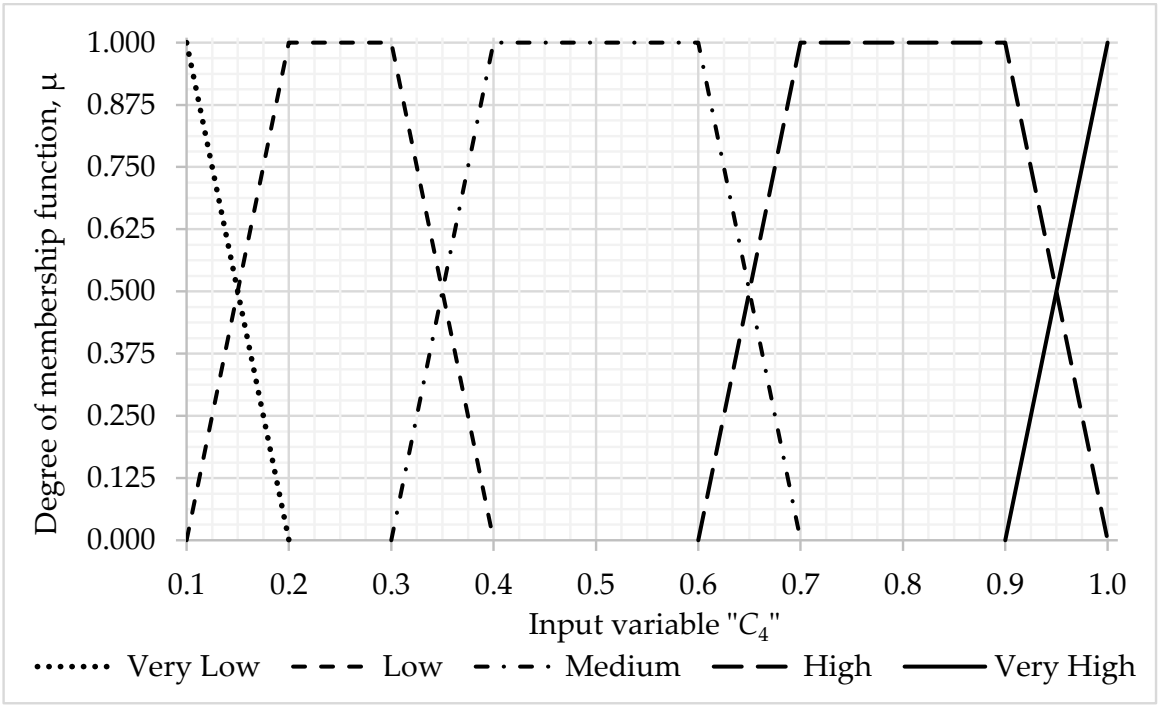

Figure A5. The plot of membership function LV "Financial damage".

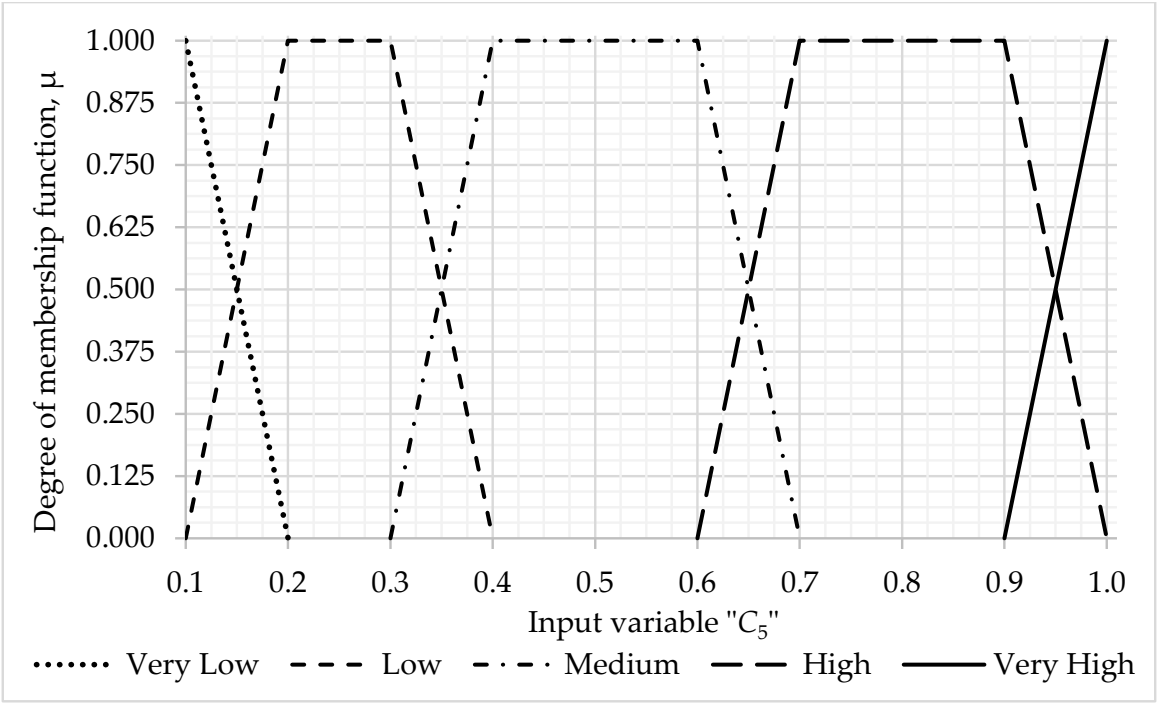

Figure A6. The plot of membership function LV "Reputational damage".

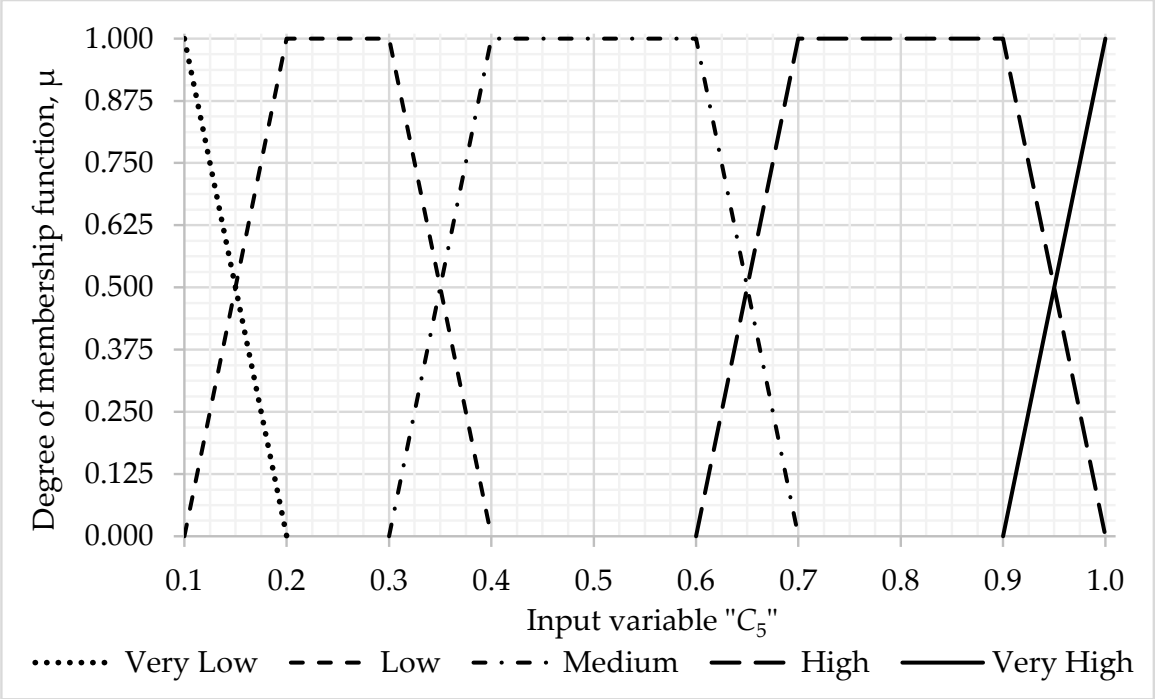

Figure A7. The plot of membership function LV "Level of inflicted damage".

Table A1. The results of assessments by experts (i) and (ii) by pairwise comparison coefficients, eigenvector, and weight values by criteria C_1, C_2, and C_3.

Input Variables	Expert (i)					Expert (ii)				
	C_1	C_2	C_3	$e_i^{(i)}$	$\omega_i^{(i)}$	C_1	C_2	V_3	$e_i^{(ii)}$	$\omega_i^{(ii)}$
Asset attractiveness (C_1)	1.0	0.5	3.0	1.14	0.3487	1.0	1.0	2.0	1.26	0.3474
Existing control (C_2)	2.0	1.0	2.0	1.59	0.4836	1.0	1.0	3.0	1.44	0.4434
Previous incidents (C_3)	0.3	0.5	1.0	0.55	0.1677	0.3	0.5	1.0	0.55	0.1692

Table A2. Results of evaluations by experts (iii) and (iv) by pairwise comparison coefficients, eigenvector, and weight values by criteria C_1, C_2, and C_3.

Input Variables	Expert (iii)					Expert (iv)				
	C_1	C_2	C_3	$e_i^{(iii)}$	$\omega_i^{(iii)}$	C_1	C_2	C_3	$e_i^{(iv)}$	$\omega_i^{(iv)}$
Asset attractiveness (C_1)	1.0	2.0	1.0	1.26	0.4126	1.0	0.5	2.0	1.00	0.3711
Existing control (C_2)	0.5	1.0	2.0	1.00	0.3275	0.5	1.0	3.0	1.14	0.4247
Previous incidents (C_3)	1.0	0.5	1.0	0.79	0.2599	0.5	0.3	1.0	0.55	0.2042

Table A3. The results of assessments by experts (v) by the coefficients of pairwise comparison, eigenvector, and weight values according to criteria C_1, C_2, and C_3 and the weight value of those assessing the probability of threats.

Input Variables	Expert (v)					Criteria Weights				
	C_1	C_2	C_3	$e_i^{(v)}$	$\omega_i^{(v)}$	$\omega_i^{(i)}$	$\omega_i^{(ii)}$	$\omega_i^{(iii)}$	$\omega_i^{(iv)}$	ω_i
Asset attractiveness (C_1)	1.0	2.0	1.0	1.26	0.5396	0.3487	0.3474	0.4126	0.3711	0.4119
Existing control (C_2)	0.5	1.0	2.0	1.00	0.2970	0.4836	0.4434	0.3275	0.4247	0.3952
Previous incidents (C_3)	1.0	0.5	1.0	0.79	0.1634	0.1677	0.1692	0.2599	0.2042	0.1929

Table A4. The results of assessments by experts (i)–(v) by the coefficients of pairwise comparison, eigenvector, and weight values according to criteria C_4, C_5, and the weight value estimating the level of inflicted damage.

Input Variables	Criteria Weights					
	$\omega_i^{(i)}$	$\omega_i^{(ii)}$	$\omega_i^{(iii)}$	$\omega_i^{(iv)}$	$\omega_i^{(v)}$	ω_i
Financial costs (C_4)	0.6667	0.3333	0.6667	0.7500	0.5000	0.5833
Reputation damage (C_5)	0.3333	0.6667	0.3333	0.2500	0.5000	0.4167

Table A5. The base of production rules for assessing Y_1—the probability of occurrence of threats.

(i)	(ii)	(iii)	(iv)	(v)	(vi)	(vii)	(viii)	(ix)	(i)	(ii)	(iii)	(iv)	(v)	(vi)	(vii)	(viii)	(ix)
1	VL	0.2	VL	1.0	VL	0.2	0.52	VL	64	M	0.6	M	0.6	H	0.8	0.64	M
2	VL	0.2	VL	1.0	L	0.4	0.55	VL	65	M	0.6	M	0.6	VH	1.0	0.68	M
3	VL	0.2	VL	1.0	M	0.6	0.59	VL	66	M	0.6	H	0.4	VL	0.2	0.44	M
4	VL	0.2	VL	1.0	H	0.8	0.63	L	67	M	0.6	H	0.4	L	0.4	0.48	M
5	VL	0.2	VL	1.0	VH	1.0	0.67	L	68	M	0.6	H	0.4	M	0.6	0.52	M
6	VL	0.2	L	0.8	VL	0.2	0.44	VL	69	M	0.6	H	0.4	H	0.8	0.56	H
7	VL	0.2	L	0.8	L	0.4	0.48	L	70	M	0.6	H	0.4	VH	1.0	0.60	H
8	VL	0.2	L	0.8	M	0.6	0.51	L	71	M	0.6	VH	0.2	VL	0.2	0.36	M
9	VL	0.2	L	0.8	H	0.8	0.55	L	72	M	0.6	VH	0.2	L	0.4	0.40	H
10	VL	0.2	L	0.8	VH	1.0	0.59	L	73	M	0.6	VH	0.2	M	0.6	0.44	H
11	VL	0.2	M	0.6	VL	0.2	0.36	L	74	M	0.6	VH	0.2	H	0.8	0.48	H
12	VL	0.2	M	0.6	L	0.4	0.40	L	75	M	0.6	VH	0.2	VH	1.0	0.52	H
13	VL	0.2	M	0.6	M	0.6	0.44	L	76	H	0.8	VL	1.0	VL	0.2	0.76	L
14	VL	0.2	M	0.6	H	0.8	0.47	L	77	H	0.8	VL	1.0	L	0.4	0.80	L
15	VL	0.2	M	0.6	VH	1.0	0.51	M	78	H	0.8	VL	1.0	M	0.6	0.84	M
16	VL	0.2	H	0.4	VL	0.2	0.28	L	79	H	0.8	VL	1.0	H	0.8	0.88	M
17	VL	0.2	H	0.4	L	0.4	0.32	L	80	H	0.8	VL	1.0	VH	1.0	0.92	M
18	VL	0.2	H	0.4	M	0.6	0.36	M	81	H	0.8	L	0.8	VL	0.2	0.68	M
19	VL	0.2	H	0.4	H	0.8	0.39	M	82	H	0.8	L	0.8	L	0.4	0.72	M
20	VL	0.2	H	0.4	VH	1.0	0.43	M	83	H	0.8	L	0.8	M	0.6	0.76	M
21	VL	0.2	VH	0.2	VL	0.2	0.20	M	84	H	0.8	L	0.8	H	0.8	0.80	M
22	VL	0.2	VH	0.2	L	0.4	0.24	M	85	H	0.8	L	0.8	VH	1.0	0.84	M
23	VL	0.2	VH	0.2	M	0.6	0.28	M	86	H	0.8	M	0.6	VL	0.2	0.61	M
24	VL	0.2	VH	0.2	H	0.8	0.32	M	87	H	0.8	M	0.6	L	0.4	0.64	M
25	VL	0.2	VH	0.2	VH	1.0	0.35	M	88	H	0.8	M	0.6	M	0.6	0.68	M
26	L	0.4	VL	1.0	VL	0.2	0.60	VL	89	H	0.8	M	0.6	H	0.8	0.72	H
27	L	0.4	VL	1.0	L	0.4	0.64	L	90	H	0.8	M	0.6	VH	1.0	0.76	H
28	L	0.4	VL	1.0	M	0.6	0.68	L	91	H	0.8	H	0.4	VL	0.2	0.53	M
29	L	0.4	VL	1.0	H	0.8	0.71	L	92	H	0.8	H	0.4	L	0.4	0.56	H
30	L	0.4	VL	1.0	VH	1.0	0.75	L	93	H	0.8	H	0.4	M	0.6	0.60	H
31	L	0.4	L	0.8	VL	0.2	0.52	L	94	H	0.8	H	0.4	H	0.8	0.64	H
32	L	0.4	L	0.8	L	0.4	0.56	L	95	H	0.8	H	0.4	VH	1.0	0.68	H
33	L	0.4	L	0.8	M	0.6	0.60	L	96	H	0.8	VH	0.2	VL	0.2	0.45	H
34	L	0.4	L	0.8	H	0.8	0.64	L	97	H	0.8	VH	0.2	L	0.4	0.49	H
35	L	0.4	L	0.8	VH	1.0	0.67	M	98	H	0.8	VH	0.2	M	0.6	0.52	H
36	L	0.4	M	0.6	VL	0.2	0.44	L	99	H	0.8	VH	0.2	H	0.8	0.56	H
37	L	0.4	M	0.6	L	0.4	0.48	L	100	H	0.8	VH	0.2	VH	1.0	0.60	VH
38	L	0.4	M	0.6	M	0.6	0.52	M	101	VH	1.0	VL	1.0	VL	0.2	0.85	M
39	L	0.4	M	0.6	H	0.8	0.56	M	102	VH	1.0	VL	1.0	L	0.4	0.88	M
40	L	0.4	M	0.6	VH	1.0	0.59	M	103	VH	1.0	VL	1.0	M	0.6	0.92	M
41	L	0.4	H	0.4	VL	0.2	0.36	M	104	VH	1.0	VL	1.0	H	0.8	0.96	M
42	L	0.4	H	0.4	L	0.4	0.40	M	105	VH	1.0	VL	1.0	VH	1.0	1.00	M
43	L	0.4	H	0.4	M	0.6	0.44	M	106	VH	1.0	L	0.8	VL	0.2	0.77	M
44	L	0.4	H	0.4	H	0.8	0.48	M	107	VH	1.0	L	0.8	L	0.4	0.81	M
45	L	0.4	H	0.4	VH	1.0	0.52	M	108	VH	1.0	L	0.8	M	0.6	0.84	M

Table A5. *Cont.*

(i)	(ii)	(iii)	(iv)	(v)	(vi)	(vii)	(viii)	(ix)	(i)	(ii)	(iii)	(iv)	(v)	(vi)	(vii)	(viii)	(ix)
46	L	0.4	VH	0.2	VL	0.2	0.28	M	109	VH	1.0	L	0.8	H	0.8	0.88	H
47	L	0.4	VH	0.2	L	0.4	0.32	M	110	VH	1.0	L	0.8	VH	1.0	0.92	H
48	L	0.4	VH	0.2	M	0.6	0.36	M	111	VH	1.0	M	0.6	VL	0.2	0.69	M
49	L	0.4	VH	0.2	H	0.8	0.40	H	112	VH	1.0	M	0.6	L	0.4	0.73	H
50	L	0.4	VH	0.2	VH	1.0	0.44	H	113	VH	1.0	M	0.6	M	0.6	0.76	H
51	M	0.6	VL	1.0	VL	0.2	0.68	L	114	VH	1.0	M	0.6	H	0.8	0.80	H
52	M	0.6	VL	1.0	L	0.4	0.72	L	115	VH	1.0	M	0.6	VH	1.0	0.84	H
53	M	0.6	VL	1.0	M	0.6	0.76	L	116	VH	1.0	H	0.4	VL	0.2	0.61	H
54	M	0.6	VL	1.0	H	0.8	0.80	L	117	VH	1.0	H	0.4	L	0.4	0.65	H
55	M	0.6	VL	1.0	VH	1.0	0.84	M	118	VH	1.0	H	0.4	M	0.6	0.69	H
56	M	0.6	L	0.8	VL	0.2	0.60	L	119	VH	1.0	H	0.4	H	0.8	0.72	H
57	M	0.6	L	0.8	L	0.4	0.64	L	120	VH	1.0	H	0.4	VH	1.0	0.76	VH
58	M	0.6	L	0.8	M	0.6	0.68	M	121	VH	1.0	VH	0.2	VL	0.2	0.53	H
59	M	0.6	L	0.8	H	0.8	0.72	M	122	VH	1.0	VH	0.2	L	0.4	0.57	H
60	M	0.6	L	0.8	VH	1.0	0.76	M	123	VH	1.0	VH	0.2	M	0.6	0.61	VH
61	M	0.6	M	0.6	VL	0.2	0.52	M	124	VH	1.0	VH	0.2	H	0.8	0.65	VH
62	M	0.6	M	0.6	L	0.4	0.56	M	125	VH	1.0	VH	0.2	VH	1.0	0.68	VH
63	M	0.6	M	0.6	M	0.6	0.60	M									

where (i)—is a serial number; (ii)–(iii)—the value of the term of the input linguistic variable C_1—Attractiveness of assets with a weighting coefficient $\omega_1 = 0.4126$; (iv)–(v)—value of the term of the input linguistic variable C_2—Existing control with a weight coefficient $\omega_2 = 0.3952$; (vi)–(vii)—value of the term of the input linguistic variable C_3—Previous incidents with a weight coefficient $\omega_3 = 0.1929$; (viii)–(ix)—calculated value of the term of the output linguistic variable Y_1—Probability of occurrence of a threat.

Table A6. Aggregated fuzzy rules for assessing Y_1—the probability of occurrence of a threat.

(i)	(ii)			(iii)
R_1	$(C_1 = VL) \wedge (C_2 = VL) \wedge (C_3 = VL) \vee$ $(C_1 = VL) \wedge (C_2 = VL) \wedge (C_3 = L) \vee$ $(C_1 = VL) \wedge (C_2 = VL) \wedge (C_3 = H) \vee$ $(C_1 = VL) \wedge (C_2 = VL) \wedge (C_3 = VH) \vee$ $(C_1 = VL) \wedge (C_2 = L) \wedge (C_3 = L) \vee$ $(C_1 = VL) \wedge (C_2 = L) \wedge (C_3 = M) \vee$ $(C_1 = VL) \wedge (C_2 = L) \wedge (C_3 = H) \vee$	$(C_1 = VL) \wedge (C_2 = VL) \wedge (C_3 = M) \vee$ $(C_1 = VL) \wedge (C_2 = L) \wedge (C_3 = VL) \vee$ $(C_1 = VL) \wedge (C_2 = H) \wedge (C_3 = VL) \vee$ $(C_1 = VL) \wedge (C_2 = H) \wedge (C_3 = L) \vee$ $(C_1 = L) \wedge (C_2 = VL) \wedge (C_3 = L) \vee$ $(C_1 = L) \wedge (C_2 = VL) \wedge (C_3 = M) \vee$ $(C_1 = L) \wedge (C_2 = VL) \wedge (C_3 = H) \vee$	$(C_1 = L) \wedge (C_2 = VL) \wedge (C_3 = VL)$ $(C_1 = L) \wedge (C_2 = M) \wedge (C_3 = VL) \vee$ $(C_1 = L) \wedge (C_2 = M) \wedge (C_3 = L) \vee$ $(C_1 = M) \wedge (C_2 = VL) \wedge (C_3 = VL) \vee$ $(C_1 = M) \wedge (C_2 = VL) \wedge (C_3 = L) \vee$ $(C_1 = M) \wedge (C_2 = VL) \wedge (C_3 = M) \vee$ $(C_1 = M) \wedge (C_2 = VL) \wedge (C_3 = H) \vee$	$Y_1 = VL$
R_2	$(C_1 = VL) \wedge (C_2 = L) \wedge (C_3 = VH) \vee$ $(C_1 = VL) \wedge (C_2 = M) \wedge (C_3 = VL) \vee$ $(C_1 = VL) \wedge (C_2 = M) \wedge (C_3 = L) \vee$ $(C_1 = VL) \wedge (C_2 = M) \wedge (C_3 = M) \vee$ $(C_1 = VL) \wedge (C_2 = M) \wedge (C_3 = H) \vee$ $(C_1 = VL) \wedge (C_2 = M) \wedge (C_3 = VH) \vee$ $(C_1 = VL) \wedge (C_2 = H) \wedge (C_3 = M) \vee$ $(C_1 = VL) \wedge (C_2 = H) \wedge (C_3 = H) \vee$ $(C_1 = VL) \wedge (C_2 = H) \wedge (C_3 = VH) \vee$ $(C_1 = VL) \wedge (C_2 = VH) \wedge (C_3 = VL) \vee$ $(C_1 = VL) \wedge (C_2 = VH) \wedge (C_3 = L) \vee$ $(C_1 = VL) \wedge (C_2 = VH) \wedge (C_3 = M) \vee$ $(C_1 = VL) \wedge (C_2 = VH) \wedge (C_3 = H) \vee$	$(C_1 = L) \wedge (C_2 = VL) \wedge (C_3 = VH) \vee$ $(C_1 = L) \wedge (C_2 = L) \wedge (C_3 = VL) \vee$ $(C_1 = L) \wedge (C_2 = L) \wedge (C_3 = L) \vee$ $(C_1 = L) \wedge (C_2 = L) \wedge (C_3 = M) \vee$ $(C_1 = L) \wedge (C_2 = L) \wedge (C_3 = H) \vee$ $(C_1 = L) \wedge (C_2 = VH) \wedge (C_3 = L) \vee$ $(C_1 = L) \wedge (C_2 = VH) \wedge (C_3 = M) \vee$ $(C_1 = M) \wedge (C_2 = VL) \wedge (C_3 = VH) \vee$ $(C_1 = M) \wedge (C_2 = L) \wedge (C_3 = M) \vee$ $(C_1 = M) \wedge (C_2 = L) \wedge (C_3 = H) \vee$ $(C_1 = M) \wedge (C_2 = L) \wedge (C_3 = VH) \vee$ $(C_1 = M) \wedge (C_2 = M) \wedge (C_3 = VL) \vee$ $(C_1 = M) \wedge (C_2 = M) \wedge (C_3 = L) \vee$ $(C_1 = M) \wedge (C_2 = M) \wedge (C_3 = M) \vee$ $(C_1 = M) \wedge (C_2 = M) \wedge (C_3 = H) \vee$ $(C_1 = M) \wedge (C_2 = H) \wedge (C_3 = VL) \vee$ $(C_1 = M) \wedge (C_2 = H) \wedge (C_3 = L) \vee$ $(C_1 = M) \wedge (C_2 = H) \wedge (C_3 = M) \vee$ $(C_1 = M) \wedge (C_2 = VH) \wedge (C_3 = VL) \vee$ $(C_1 = H) \wedge (C_2 = VL) \wedge (C_3 = VH) \vee$ $(C_1 = H) \wedge (C_2 = L) \wedge (C_3 = VL) \vee$	$(C_1 = L) \wedge (C_2 = M) \wedge (C_3 = VL) \vee$ $(C_1 = L) \wedge (C_2 = M) \wedge (C_3 = L) \vee$ $(C_1 = M) \wedge (C_2 = L) \wedge (C_3 = L) \vee$ $(C_1 = H) \wedge (C_2 = VL) \wedge (C_3 = VL) \vee$ $(C_1 = H) \wedge (C_2 = VL) \wedge (C_3 = L)$ $(C_1 = H) \wedge (C_2 = L) \wedge (C_3 = L) \vee$ $(C_1 = H) \wedge (C_2 = L) \wedge (C_3 = M) \vee$ $(C_1 = H) \wedge (C_2 = L) \wedge (C_3 = H) \vee$ $(C_1 = H) \wedge (C_2 = L) \wedge (C_3 = VH) \vee$ $(C_1 = H) \wedge (C_2 = M) \wedge (C_3 = L) \vee$ $(C_1 = H) \wedge (C_2 = M) \wedge (C_3 = M) \vee$ $(C_1 = H) \wedge (C_2 = H) \wedge (C_3 = VL) \vee$ $(C_1 = VH) \wedge (C_2 = VL) \wedge (C_3 = VL) \vee$ $(C_1 = VH) \wedge (C_2 = VL) \wedge (C_3 = L) \vee$ $(C_1 = VH) \wedge (C_2 = VL) \wedge (C_3 = M) \vee$ $(C_1 = VH) \wedge (C_2 = VL) \wedge (C_3 = H) \vee$ $(C_1 = VH) \wedge (C_2 = VL) \wedge (C_3 = VH) \vee$ $(C_1 = VH) \wedge (C_2 = L) \wedge (C_3 = VL) \vee$ $(C_1 = VH) \wedge (C_2 = L) \wedge (C_3 = L) \vee$ $(C_1 = VH) \wedge (C_2 = L) \wedge (C_3 = M) \vee$ $(C_1 = VH) \wedge (C_2 = M) \wedge (C_3 = VL)$	$Y_1 = L$
R_3	$(C_1 = L) \wedge (C_2 = L) \wedge (C_3 = VH) \vee$ $(C_1 = L) \wedge (C_2 = M) \wedge (C_3 = M) \vee$ $(C_1 = L) \wedge (C_2 = M) \wedge (C_3 = H) \vee$ $(C_1 = L) \wedge (C_2 = M) \wedge (C_3 = VH) \vee$ $(C_1 = L) \wedge (C_2 = H) \wedge (C_3 = VL) \vee$ $(C_1 = L) \wedge (C_2 = H) \wedge (C_3 = L) \vee$ $(C_1 = L) \wedge (C_2 = H) \wedge (C_3 = M) \vee$ $(C_1 = L) \wedge (C_2 = H) \wedge (C_3 = H) \vee$ $(C_1 = L) \wedge (C_2 = H) \wedge (C_3 = VH) \vee$ $(C_1 = L) \wedge (C_2 = VH) \wedge (C_3 = VL) \vee$	$(C_1 = M) \wedge (C_2 = M) \wedge (C_3 = VH) \vee$ $(C_1 = M) \wedge (C_2 = H) \wedge (C_3 = VL) \vee$ $(C_1 = M) \wedge (C_2 = H) \wedge (C_3 = L) \vee$ $(C_1 = M) \wedge (C_2 = H) \wedge (C_3 = M) \vee$ $(C_1 = M) \wedge (C_2 = VH) \wedge (C_3 = VL) \vee$	$(C_1 = VH) \wedge (C_2 = VL) \wedge (C_3 = VL) \vee$ $(C_1 = VH) \wedge (C_2 = VL) \wedge (C_3 = L) \vee$ $(C_1 = VH) \wedge (C_2 = VL) \wedge (C_3 = M) \vee$ $(C_1 = VH) \wedge (C_2 = VL) \wedge (C_3 = H) \vee$ $(C_1 = VH) \wedge (C_2 = VL) \wedge (C_3 = VH) \vee$ $(C_1 = VH) \wedge (C_2 = L) \wedge (C_3 = VL) \vee$ $(C_1 = VH) \wedge (C_2 = L) \wedge (C_3 = L) \vee$ $(C_1 = VH) \wedge (C_2 = L) \wedge (C_3 = M) \vee$ $(C_1 = VH) \wedge (C_2 = M) \wedge (C_3 = VL)$	$Y_1 = M$

Table A6. *Cont.*

(i)	(ii)			(iii)
R_4	$(C_1 = L) \wedge (C_2 = VH) \wedge (C_3 = H) \vee$ $(C_1 = L) \wedge (C_2 = VH) \wedge (C_3 = VH) \vee$ $(C_1 = M) \wedge (C_2 = H) \wedge (C_3 = H) \vee$ $(C_1 = M) \wedge (C_2 = H) \wedge (C_3 = VH) \vee$ $(C_1 = M) \wedge (C_2 = VH) \wedge (C_3 = L) \vee$ $(C_1 = M) \wedge (C_2 = VH) \wedge (C_3 = M) \vee$ $(C_1 = M) \wedge (C_2 = VH) \wedge (C_3 = H) \vee$ $(C_1 = M) \wedge (C_2 = VH) \wedge (C_3 = VH) \vee$ $(C_1 = H) \wedge (C_2 = M) \wedge (C_3 = H) \vee$ $(C_1 = H) \wedge (C_2 = M) \wedge (C_3 = VH) \vee$	$(C_1 = H) \wedge (C_2 = H) \wedge (C_3 = L) \vee$ $(C_1 = H) \wedge (C_2 = H) \wedge (C_3 = M) \vee$ $(C_1 = H) \wedge (C_2 = H) \wedge (C_3 = H) \vee$ $(C_1 = H) \wedge (C_2 = H) \wedge (C_3 = VH) \vee$ $(C_1 = H) \wedge (C_2 = VH) \wedge (C_3 = VL) \vee$ $(C_1 = H) \wedge (C_2 = VH) \wedge (C_3 = L) \vee$ $(C_1 = H) \wedge (C_2 = VH) \wedge (C_3 = M) \vee$ $(C_1 = H) \wedge (C_2 = VH) \wedge (C_3 = H) \vee$ $(C_1 = VH) \wedge (C_2 = L) \wedge (C_3 = H) \vee$ $(C_1 = VH) \wedge (C_2 = L) \wedge (C_3 = VH) \vee$	$(C_1 = VH) \wedge (C_2 = M) \wedge (C_3 = L) \vee$ $(C_1 = VH) \wedge (C_2 = M) \wedge (C_3 = M) \vee$ $(C_1 = VH) \wedge (C_2 = M) \wedge (C_3 = H) \vee$ $(C_1 = VH) \wedge (C_2 = M) \wedge (C_3 = VH) \vee$ $(C_1 = VH) \wedge (C_2 = H) \wedge (C_3 = VL) \vee$ $(C_1 = VH) \wedge (C_2 = H) \wedge (C_3 = L) \vee$ $(C_1 = VH) \wedge (C_2 = H) \wedge (C_3 = M) \vee$ $(C_1 = VH) \wedge (C_2 = H) \wedge (C_3 = H) \vee$ $(C_1 = VH) \wedge (C_2 = VH) \wedge (C_3 = VL) \vee$ $(C_1 = VH) \wedge (C_2 = VH) \wedge (C_3 = L)$	$Y_1 = H$
R_5	$(C_1 = H) \wedge (C_2 = VH) \wedge (C_3 = VH) \vee$ $(C_1 = VH) \wedge (C_2 = H) \wedge (C_3 = VH) \vee$	$(C_1 = VH) \wedge (C_2 = VH) \wedge (C_3 = M) \vee$ $(C_1 = VH) \wedge (C_2 = VH) \wedge (C_3 = H) \vee$	$(C_1 = VH) \wedge (C_2 = VH) \wedge (C_3 = VH) \vee$	$Y_1 = VH$

where (i)—is the ordinal number of the rules R_j, $j = \overline{1,5}$; (ii)—Rule; (iii)—Consequent.

Table A7. Information base of fuzzy production rules for assessing the level of inflicted damage.

(i)	(ii)	(iii)	(iv)	(v)	(vi)	(vii)	(i)	(ii)	(iii)	(iv)	(v)	(vi)	(vii)	(i)	(ii)	(iii)	(iv)	(v)	(vi)	(vii)
1	VL	1	VL	1	1.000	VL	10	L	2	VH	5	3.251	M	19	H	4	H	4	4.000	H
2	VL	1	L	2	1.417	VL	11	M	3	VL	1	2.166	L	20	H	4	VH	5	4.417	H
3	VL	1	M	3	1.834	L	12	M	3	L	2	2.583	M	21	VH	5	VL	1	3.332	M
4	VL	1	H	4	2.251	L	13	M	3	M	3	3.000	M	22	VH	5	L	2	3.749	H
5	VL	1	VH	5	2.668	M	14	M	3	H	4	3.417	M	23	VH	5	M	3	4.166	H
6	L	2	VL	1	1.583	L	15	M	3	VH	5	3.834	H	24	VH	5	H	4	4.583	VH
7	L	2	L	2	2.000	L	16	H	4	VL	1	2.749	M	25	VH	5	VH	5	5	VH
8	L	2	M	3	2.417	L	17	H	4	L	2	3.166	M							
9	L	2	H	4	2.834	M	18	H	4	M	3	3.583	H							

where (i)—is a serial number; (ii)–(iii)—the value of the term of the input linguistic variable C_4—Financial costs with a weighting coefficient $\omega_4 = 0.5833$; (iv)–(v)—the value of the term of the input linguistic variable C_5—Damage to reputation with a weight coefficient $\omega_5 = 0.4167$; (vi)–(vii)—calculated value of the term of the output linguistic variable Y_2—Manifestation of the damage caused.

Table A8. Aggregated fuzzy rules for assessing the level of inflicted damage.

(i)	(ii)			(iii)
R6	(C4 = VL) ∧ (C5 = VL) ∨	(C4 = VL) ∧ (C5 = L)		Y2 = VL
R7	(C4 = VL) ∧ (C5 = M) ∨ (C4 = VL) ∧ (C5 = H) ∨	(C4 = L) ∧ (C5 = VL) ∨ (C4 = L) ∧ (C5 = L) ∨	(C4 = L) ∧ (C5 = M) ∨ (C4 = M) ∧ (C5 = VL)	Y2 = L
R8	(C4 = VL) ∧ (C5 = VH) ∨ (C4 = L) ∧ (C5 = H) ∨ (C4 = L) ∧ (C5 = VH) ∨	(C4 = M) ∧ (C5 = L) ∨ (C4 = M) ∧ (C5 = M) ∨ (C4 = M) ∧ (C5 = H) ∨	(C4 = H) ∧ (C5 = VL) ∨ (C4 = H) ∧ (C5 = L) ∨ (C4 = VH) ∧ (C5 = VL)	Y2 = M
R9	(C4 = M) ∧ (C5 = VH) ∨ (C4 = H) ∧ (C5 = M) ∨	(C4 = H) ∧ (C5 = H) ∨ (C4 = H) ∧ (C5 = VH) ∨	(C4 = VH) ∧ (C5 = L) ∨ (C4 = VH) ∧ (C5 = M)	Y2 = H
R10	(C4 = VH) ∧ (C5 = H) ∨	(C4 = VH) ∧ (C5 = VH)		Y2 = VH

where (i)—is the ordinal number of rules R_j, $j = \overline{6,10}$; (ii)—Rule; (iii)—Consequent.

References

1. Hofer, F. Architecture, technologies and challenges for cyber-physical systems in industry 4.0: A systematic mapping study. In Proceedings of the 12th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM), Oulu, Finland, 11–12 October 2018; pp. 1–10. [CrossRef]
2. Sisinni, E.; Saifullah, A.; Han, S.; Jennehag, U.; Gidlund, M. Industrial Internet of Things: Challenges, opportunities, and directions. *IEEE Trans. Ind. Inform.* **2018**, *14*, 4724–4734. [CrossRef]
3. Tange, K.; De Donno, M.; Fafoutis, X.; Dragoni, N. A Systematic Survey of Industrial Internet of Things Security: Requirements and Fog Computing Opportunities. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 2489–2520. [CrossRef]
4. Yu, X.; Guo, H. A Survey on IIoT Security. In Proceedings of the Conference: IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS), Singapore, 28–30 August 2019; pp. 1–5. [CrossRef]
5. Panchal, A.; Khadse, V.; Mahalle, P. Security Issues in IIoT: A Comprehensive Survey of Attacks on IIoT and Its Countermeasures. In Proceedings of the Conference: 2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN), Lonavala, India, 23–24 November 2018; pp. 124–130. [CrossRef]
6. Shah, Y.; Sengupta, S. A survey on Classification of Cyber-attacks on IoT and IIoT devices. In Proceedings of the Conference: 2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 28–31 October 2020; pp. 0406–0413. [CrossRef]

7. Tamy, S.; Belhadaoui, H.; Rabbah, M.; Rabbah, N.; Rifi, M. An evaluation of machine learning algorithms to detect attacks in SCADA network. In Proceedings of the Conference: 2019 7th Mediterranean Congress of Telecommunications (CMT), Fez, Morocco, 24–25 October 2019; pp. 1–5. [CrossRef]
8. Al-Hawawreh, M.; Sitnikova, E. Industrial Internet of Things based ransomware detection using stacked variational neural network. In Proceedings of the 2019 Conference on Big Data and Internet of Things (BDIOT), Melbourn, VIC, Australia, 22–24 August 2019; pp. 126–130. [CrossRef]
9. Wang, H.; Chen, Z.; Zhao, J.; Di, X.; Liu, D. A Vulnerability Assessment Method in Industrial Internet of Things Based on Attack Graph and Maximum Flow. *IEEE Access* **2018**, *6*, 8599–8609. [CrossRef]
10. Li, Z.; Kang, J.; Yu, R.; Ye, D.; Deng, Q.; Zhang, Y. Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things. *IEEE Trans. Ind. Inform.* **2017**, *14*, 3690–3700. [CrossRef]
11. Huang, Y.-L.; Sun, W.-L. An AHP-Based Risk Assessment for an Industrial IoT Cloud. In Proceedings of the IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), Lisbon, Portugal, 16–20 July 2018; pp. 637–638. [CrossRef]
12. Hassani, H.L.; Bahnasse, A.; Martin, E.; Roland, C.; Bouattane, O.; Diouri, M.E. Vulnerability and security risk assessment in a IIoT environment in compliance with standard IEC 62443. *Procedia Comput. Sci.* **2021**, *191*, 33–40. [CrossRef]
13. Tsiknas, K.; Taketzis, D.; Demertzis, K.; Skianis, C. Cyber Threats to Industrial IoT: A Survey on Attacks and Countermeasures. *IoT* **2021**, *2*, 163–186. [CrossRef]
14. Wentian, C.; Huijun, Y. Research on Information Security Risk Assessment Method Based on Fuzzy Rule Set. *Wirel. Commun. Mob. Comput.* **2021**, 9663520. [CrossRef]
15. Tubis, A.; Werbińska-Wojciechowska, S.; Góralczyk, M.; Wróblewski, A.; Ziętek, B. Cyber-Attacks Risk Analysis Method for Different Levels of Automation of Mining Processes in Mines Based on Fuzzy Theory Use. *Sensors* **2020**, *20*, 7210. [CrossRef]
16. Kuzminykh, I.; Ghita, B.; Sokolov, V.; Bakhshi, T. Information Security Risk Assessment. *Encyclopedia* **2021**, *1*, 602–617. [CrossRef]
17. Zadeh, L.A. Is there a need for fuzzy logic? *Inf. Sci.* **2008**, *178*, 2751–2779. [CrossRef]
18. *ISO/IEC 27400:2022*; Cybersecurity–IoT Security and Privacy. ISO: Geneva, Switzerland, 2023. Available online: www.iso27001security.com (accessed on 21 July 2023).
19. *ISA/IEC 62443*; Series of Standards—Security for Industrial Automation and Control Systems. ISA: Eindhoven, The Netherlands, 2023. Available online: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards (accessed on 21 July 2023).
20. Force, J.T. *Guide for Conducting Risk Assessments*; NIST SP 800-30 Rev. 1; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2012. [CrossRef]
21. Force, J.T. *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*; NIST SP 800-37 Rev. 2; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2018. [CrossRef]
22. *ISO/IEC 27005:2022*; Information Security, Cybersecurity and Privacy Protection—Guidance on Managing Information Security Risks. ISO: Geneva, Switzerland, 2022. Available online: https://www.iso.org/standard/80585.html (accessed on 21 July 2023).
23. Freund, J.; Jones, J. *Measuring and Managing Information Risk: A FAIR Approach*; Butterworth-Heinemann: Oxford, UK, 2014; p. 408.
24. Saaty, T.L. There is no mathematical validity for using fuzzy number crunching in the analytic hierarchy process. *J. Syst. Sci. Syst. Eng.* **2006**, *15*, 457–464. [CrossRef]
25. Reports of the Kaspersky Lab Industrial Infrastructure Information Security Incident Response Center (Kaspersky ICS CERT). Available online: https://ics-cert.kaspersky.ru/publications/reports/2023/09/13/threat-landscape-for-industrial-automation-systems-statistics-for-h1-2023/ (accessed on 21 July 2023).
26. Arrow, K.J.; Kruz, M. *Public Investment, the Rate of Return, and Optimal Fiscal Policy*; RFF Press: New York, NY, USA, 2013; p. 218. [CrossRef]
27. Gaultier-Gaillard, S.; Louisot, J.P.; Rayner, J. Managing reputational risk—From theory to practice. In *Reputation Capital: Building and Maintaining Trust in the 21st Century*; Springer: Berlin/Heidelberg, Germany, 2009. [CrossRef]
28. Kureichik, V.M.; Kazharov, A. Using fuzzy logic controller in ant colony optimization. *Adv. Intell. Syst. Comput.* **2015**, *347*, 151–158. [CrossRef]
29. Shang, W.; Gong, T.; Chen, C.; Hou, J.; Zeng, P. Information Security Risk Assessment Method for Ship Control System Based on Fuzzy Sets and Attack Trees. *Secur. Commun. Netw.* **2019**, 3574675. [CrossRef]
30. Huijuan, G.; Lei, D.; Wenchao, X. Cybersecurity Risk Assessment of Industrial Control Systems Based on Order-α Divergence Measures Under an Interval-Valued Intuitionistic Fuzzy Environment. *IEEE Access* **2022**, *10*, 43751–43765. [CrossRef]
31. Stojanović, M.; Markovic-Petrovic, J. A Model for Dynamic Cyber Security Risk Assessment in the Industrial IoT Environment. In Proceedings of the Sinteza 2022—International Scientific Conference on Information Technology and Data Related Research, Online, 16 April 2022; pp. 230–237. [CrossRef]
32. Atlam, H.; Walters, R.; Wills, G.; Daniel, J. Fuzzy Logic with Expert Judgment to Implement an Adaptive Risk-Based Access Control Model for IoT. *Mob. Netw. Appl.* **2021**, *26*, 2545–2557. [CrossRef]
33. Adaros-Boye, C.; Kearney, P.; Josephs, M.; Ulmer, H. An Indicators-of-Risk Library for Industrial Network Security. In Proceedings of the Conference: ARES 2021: The 16th International Conference on Availability, Reliability and Security, Vienna, Austria, 17–20 August 2021. [CrossRef]

34. Figueroa-Lorenzo, S.; Añorga, J.; Arrizabalaga, S. A Survey of IIoT Protocols: A Measure of Vulnerability Risk Analysis Based on CVSS. *ACM Comput. Surv.* **2020**, *53*, 1–53. [CrossRef]
35. Abdymanapov, S.; Muratbekov, M.; Sharipbay, A.; Barlybayev, A. Fuzzy Expert System of Information Security Risk Assessment on the Example of Analysis Learning Management Systems. *IEEE Access* **2021**, *9*, 156556–156565. [CrossRef]
36. Sikman, L.; Latinovic, T.; Sarajlic, N. Modelling of Fuzzy Expert System for an Assessment of Security Information Management System UIS. *Tech. Gaz.* **2022**, *29*, 60–65. [CrossRef]
37. Amirova, A.; Tokhmetov, A. A model for risk analysis in the Industrial Internet of Things. *J. Theor. Appl. Inf. Technol.* **2021**, *99*, 3449–3459.
38. McLaughlin, S.; Konstantinou, C.; Wang, X.; Davi, L.; Sadeghi, A.; Maniatakos, M.; Karri, R. The Cybersecurity Landscape in Industrial Control Systems. *Proc. IEEE* **2016**, *104*, 1039–1057. [CrossRef]
39. Makhazhanova, U.; Kerimkhulle, S.; Mukhanova, A.; Bayegizova, A.; Aitkozha, Z.; Mukhiyadin, A.; Tassuov, B.; Saliyeva, A.; Taberkhan, R.; Azieva, G. The Evaluation of Creditworthiness of Trade and Enterprises of Service Using the Method Based on Fuzzy Logic. *Appl. Sci.* **2022**, *12*, 11515. [CrossRef]