INFORMATICA, 2019, Vol. 30, No. 1, 187–211

DOI: http://dx.doi.org/10.15388/Informatica.2019.203

Information Security Risk Assessment in Critical Infrastructure: A Hybrid MCDM Approach

Zenonas TURSKIS[1], Nikolaj GORANIN[2]* Assel NURUSHEVA[3], Seilkhan BORANBAYEV[3]

[1] *Institute of Sustainable Construction, Faculty of Civil Engineering,*
Vilnius Gediminas Technical University, Sauletekio al. 11, LT-10223 Vilnius, Lithuania
[2] *Faculty of Fundamental Sciences, Vilnius Gediminas Technical University,*
Sauletekio al. 11, LT-10223 Vilnius, Lithuania
[3] *Department of Information Systems, L.N. Gumilyov Eurasian National University,*
Satpayev st., 2, 010008 Astana, Kazakhstan
e-mail: zenonas.turskis@vgtu.lt, nikolaj.goranin@vgtu.lt, sboranba@yandex.kz

Received: September 2018; accepted: January 2019

Abstract. The risk analysis has always been one of the essential procedures for any areas. The majority of security incidents occur because of ignoring risks or their inaccurate assessment. It is especially dangerous for critical infrastructures. Thus, the article is devoted to the description of the developed model of risk assessment for the essential infrastructures. The goal of the model is to provide a reliable method for multifaceted risk assessment of information infrastructure. The purpose of the article is to present a developed model based on integrated MCDM approaches that allow to correctly assess the risks of the critical information infrastructures.

Key words: information security, fuzzy, risk assessment, infrastructure, AHP, Delphi method, Eckenrode method, MCDM.

1. Introduction and Problem Statement

Nowadays, we often come up against a situation where companies use information infrastructures without due regard for their information security, reliability, fault tolerance, etc. The companies save time and do not spend financial resources on tools for risk analysis and experts. As a result, the number of information security incidents increases. Such dynamics are not acceptable for critical infrastructures due to the possible globalization of their incidents' consequences.

The rapid development of the IT sector leads to accelerated application and introduction of digital innovations, including blockchain technologies, open data, robotization and artificial intelligence, biometric authentication, crowdfunding, big data, etc. Digital technology development raises the need to increase the level of information security and

*Corresponding author.

reliability of implemented technologies (Boranbayev *et al.*, 2018b). It is well known that modern society is becoming increasingly dependent on information technology, its continuous and trouble-free operation, respectively, on its reliability and security (Boranbayev *et al.*, 2018a). At the same time, the amount of known/reported cybersecurity crimes keeps growing (Olifer *et al.*, 2017).

Research aimed at risk assessment is becoming more widespread (Grabauskyte *et al.*, 2018; Ijadi Maghsoodi *et al.*, 2018). Risk assessment is an important aspect of decision making in industry, government, financial, environmental, and other sectors (Tamilselvi, 2018). It is widely used in considering various aspects of the operations and safety of large complex systems that can adversely affect the health and safety of society (Bell, 1989). So risk assessment has been identified as an essential element of effective decision-making, management, and development of information infrastructures but often it has been missed (Boehm, 1991).

Some information and automated systems are responsible for the vital services of modern society. For example, the systems such as water management heating, and public transport depend on the proper functioning of information and automated systems that support their operations. These support infrastructures, usually called critical ones, are crucial elements for the functioning of the economy and society.

Information security, reliability and fault tolerance of the critical infrastructures are one of the primary and priority tasks of any country (Miao *et al.*, 2010). Countries around the world are experiencing failures and incidents caused by different causes in the essential infrastructure sector (Yusta *et al.*, 2011). For systems, risk analysis is an investment that will ensure future high quality and reliability of systems (Cagliano *et al.*, 2015). Reducing operational risks and errors is the key to improving the security and accessibility of cloud services (Hu *et al.*, 2017). To manage risks in the critical information infrastructures (CII), the decision support systems should integrate the multi-alternative design and multi-criteria decision-making approaches (Kaklauskas *et al.*, 2018).

According to ISO 27005, the determining of risk level is based on indicators of its impact on infrastructure and the probability of risk realization. These indicators can be calculated by standard methods for small and medium-sized organizations. However, companies that provide critical services must accurately identify the dangerous risks and mitigate them promptly. Otherwise, the realization of undetected or incorrectly assessed risks can lead to catastrophic situations, significant financial and human losses, etc. The purpose of the article is to present a developed model based on integrated multi-criteria decision-making (MCDM) approach that allows to correctly evaluate the risks of the information infrastructures.

2. Risks

According to ISO 27005, the risk of information security is the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the company.

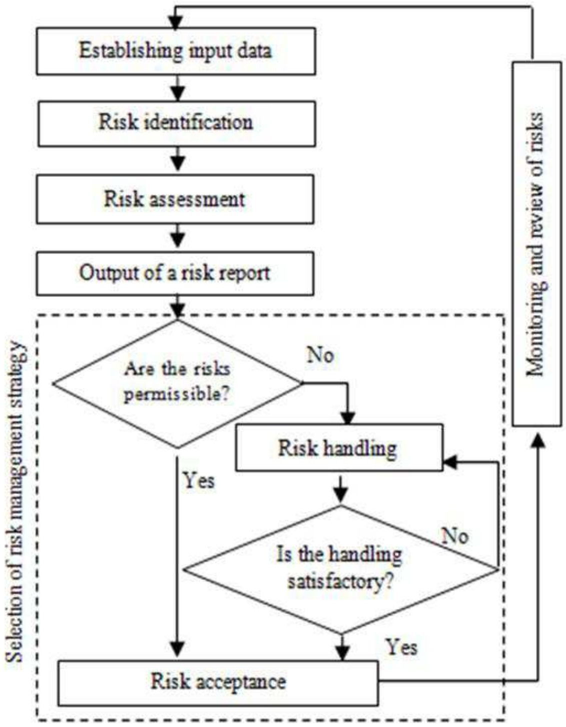
Establishing input data
Risk identification
Risk assessment
Output of a risk report
Are the risks permissible?
No
Risk handling
Yes
Is the handling satisfactory?
No
Yes
Risk acceptance
Selection of risk management strategy
Monitoring and review of risks

Fig. 1. Components of the risk management process for information systems.

2.1. *Risk Management Description*

Risk management is a significant, costly, not time-consuming, and straightforward process (Haimes, 1991). It often requires the involvement of experts, resources, etc. (Vrhovec *et al.*, 2015). The advantages that it gives significantly outweigh the outlay cost and expended funds (Han, 2015).

Risk management involves taking measures aimed at reducing the frequency of threat implementation and reducing the damage from them (Boranbayev *et al.*, 2018c). Depending on the received risk indicators, the owner of the information system must choose a risk management strategy. There are four main risk management strategies:

1) Risk acceptance;
2) Risk mitigation;
3) Risk avoidance;
4) Risk transfer to third parties.

The components of the risk management process for information systems are shown in Fig. 1.

The necessity and effectiveness of using the risk management process in the design and operation of the software are confirmed by many studies (Sangaiah *et al.*, 2018).

As you can see from (Fig. 1), firstly the input data are installed. Further, the identification and assessment of risks are carried out. Based on them, a risk report is formed. Also, it is necessary to determine whether the handling is required for identified risks. If there are risks at the output that need modification to an acceptable level, then the handling phase of risks (mitigation) occurs (Caplinskas *et al.*, 2012). It is possible that risk-handling will not immediately yield the result in an acceptable level of residual risk.

The primary purpose of the article is to present the developed model, which allows to evaluate risks in order to determine which should be neutralized firstly.

As part of the research to develop a risk assessment model for CII, the study was conducted on factors affecting their safe and reliable operation.

New methods of risk analysis are continually being developed (Boranbayev *et al.*, 2018d). These include association rules (Garcia *et al.*, 2008), genetic algorithms (Pfeifer *et al.*, 2015), models of processes (Aloini *et al.*, 2012), and cluster analysis (Bannerman, 2008). Each method has its unique advantages and disadvantages.

The topic of risk analysis in various sectors is the most important topic that many researchers are paying attention to these days (Navickiene *et al.*, 2018). The goal of the model is to prevent or reduce the threats of negative financial and non-financial consequences associated with the use of information infrastructures, as well as external factors affecting information infrastructures. The model is aimed at minimizing risks in the organization's activities related to the violation of the integrity, confidentiality, and availability of information infrastructures arising from the deliberate destructive impact of employees or third parties. The model also takes into account the criticality of the checked information infrastructures, possible direct and indirect losses, as well as the probability of risk realization.

One of the essential steps to ensure the reliability and security of the information infrastructures is to take measures to mitigate the level of failures by identifying the most dangerous and harmful elements that pose a risk to the system and eliminate them (Lo and Liou, 2018).

2.2. *Literature Review of Methods for Risk Assessment*

Most organizations that specialize in solving information security problems offer various methods for assessing information risks. Known techniques can be divided into single-stage and multi-stage ones according to the type of decision-making procedure used in them. In a one-step methodology ("Risk Matrix"), risk assessment is performed using a one-time decisive procedure. In a multi-stage methodology (NIST, CRAMM), risk assessment is performed with a preliminary assessment of key parameters. The mechanism of risk assessment based on fuzzy logic is an expert system, in which certain rules form the knowledge base. For example, "table" logic or logic reflecting the relationships formed by "if, ..., then" rules. The method for assessing the critical threats, assets and vulnerabilities OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) is a methodology based on strategic risk assessment (Bamakan and Dehghanimohammadabadi, 2015).

The analysis of the companies' choice of risk assessment tools and methods showed that the FMEA – Failure Modes and Effects Analysis (Baynal *et al.*, 2018), FTA – Fault Tree Analysis (Giraud and Galy, 2018), Bow-Tie Analysis (Muniz *et al.*, 2018), HAZOP – Hazards and Operability Studies (Taylor, 2017) and LOPA – Layer of Protection Analysis (Yan and Xu, 2018) are the most common tools used in the most significant and industrial organizations. These tools assess potential risks and try to keep them within acceptable limits (Yasseri and Mahani, 2013).

Many studies were is reviewed for improving FMEA (Lo and Liou, 2018). For example, FMEA combined with methods, such as Grey Relational Analysis (GRA) (Zhou and Thai, 2016), the Visekriterijumska Optimizacija i Kompromisno Resenje (VIKOR) method (Safari *et al.*, 2016), the Decision-Making Trial and Evaluation Laboratory (DEMATEL) method (Govindan and Chaudhuri, 2016), MULTIMOORA (Zhao *et al.*, 2017) and others. To apply FMEA-WASPAS, an approach was proposed (Can, 2018).

The issue of measuring according to some criteria is known as MCDM (Zolfani *et al.*, 2013; Zavadskas *et al.*, 2009; Medineckiene *et al.*, 2015). Scientists used MCDM approaches previously in risk management. The processes using MCDM approaches for the issue of managing risks for a nuclear and radiation emergency were presented by (Papamichail and French, 2012). An overview of risk assessment using MCDM approaches was presented in the researches (Linkov *et al.*, 2006) and (Ananda and Herath, 2009). Evaluating risk assessment approaches for solid waste management were reviewed in (Allesch and Brunner, 2014). Criteria such as safety and risk in the context of maintenance and reliability can be widely found among the criteria evaluated in MCDM approaches (de Almeida *et al.*, 2015). Besides, MCDM methods were applied in different areas of activity (Zavadskas *et al.*, 2013; Sivilevicius *et al.*, 2008; Saparauskas *et al.*, 2011; Turskis *et al.*, 2015). Effective use of the MCDM method is presented in Zavadskas *et al.* (2012, 2015a, 2015b).

The researches on the use of various methods for risk assessment were reviewed (de Almeida *et al.*, 2015). Some of them are AHP (Ma *et al.*, 2013), MAUT/MAVT (Garcez and de Almeida, 2014), Weighted sum (Akbari *et al.*, 2014), TOPSIS (Jozi and Majd, 2014), NSGA (Woodward *et al.*, 2014), ELECTRE (Macary *et al.*, 2014), ANP (Tavana *et al.*, 2013), PROMETHEE (Bates *et al.*, 2014), and other methods (Jin *et al.*, 2014).

In our case, according to Saaty and Ergu (2015), the MCDM method was chosen. Hybrid MCDM approach was applied. Earlier hybrid MCDM methods were proposed to use in Zavadskas *et al.* (2016a, 2016b).

3. Methods

In this article, the model for implementing the methodology for risk analysis (Fig. 2) is considered in more detail. Below are the main steps of information security risk analysis.

At the beginning of the process, the experts identified the main CII that require the risk assessment. Also, they determined threats affecting the risk implementation, and the characteristics of the threats, which allow identifying the degree of adverse impact of the threat realization on the CII (Fig. 3).

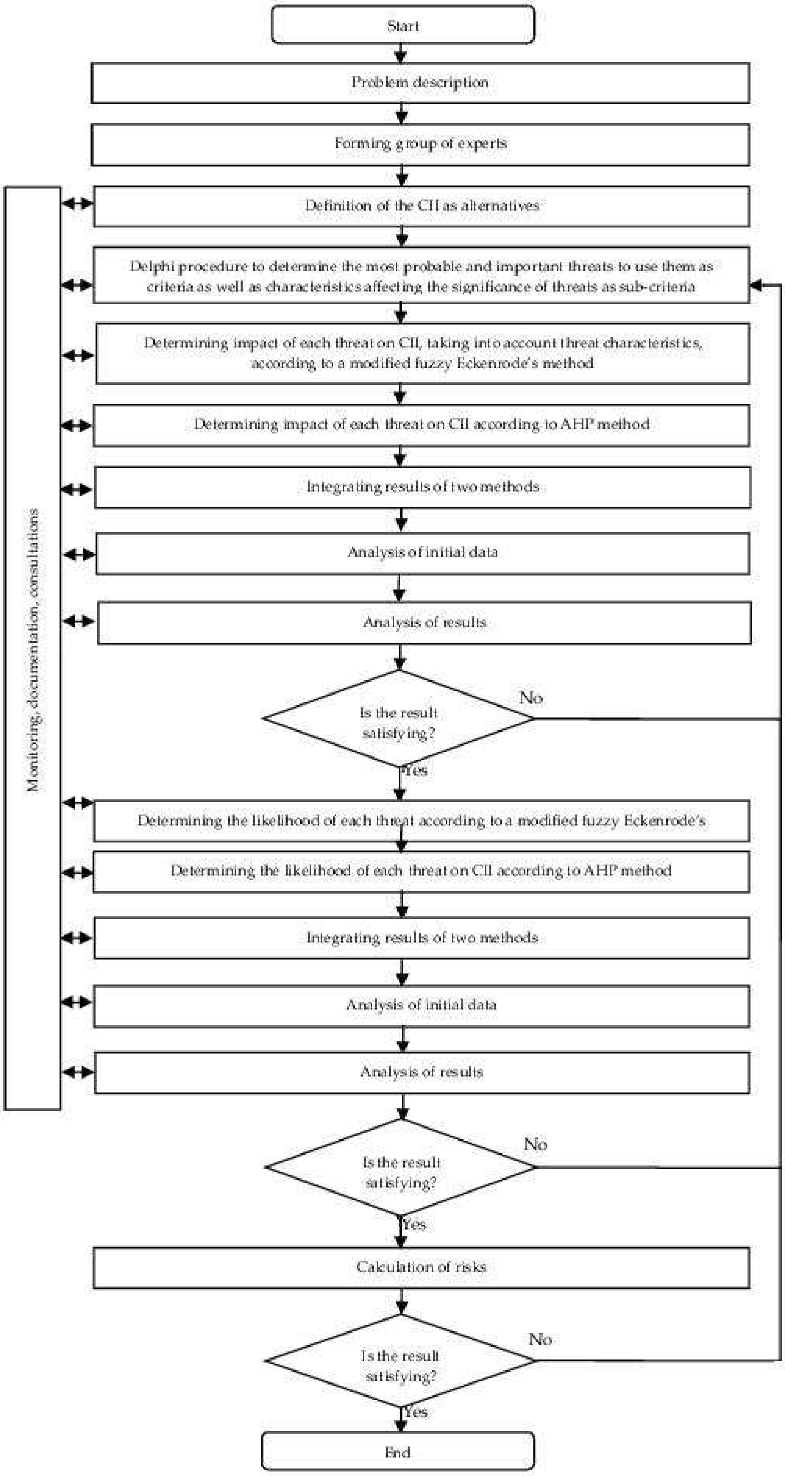
Start
Problem description
Forming group of experts
Definition of the CII as alternatives
Delphi procedure to determine the most probable and important threats to use them as criteria as well as characteristics affecting the significance of threats as sub-criteria
Determining impact of each threat on CII, taking into account threat characteristics, according to a modified fuzzy Eckenrode's method
Determining impact of each threat on CII according to AHP method
Integrating results of two methods
Analysis of initial data
Analysis of results
Is the result satisfying?
No
Yes
Determining the likelihood of each threat according to a modified fuzzy Eckenrode's
Determining the likelihood of each threat on CII according to AHP method
Integrating results of two methods
Analysis of initial data
Analysis of results
Is the result satisfying?
No
Yes
Calculation of risks
Is the result satisfying?
No
Yes
End
Monitoring, documentation, consultations

Fig. 2. The proposed framework for the risk assessment process.

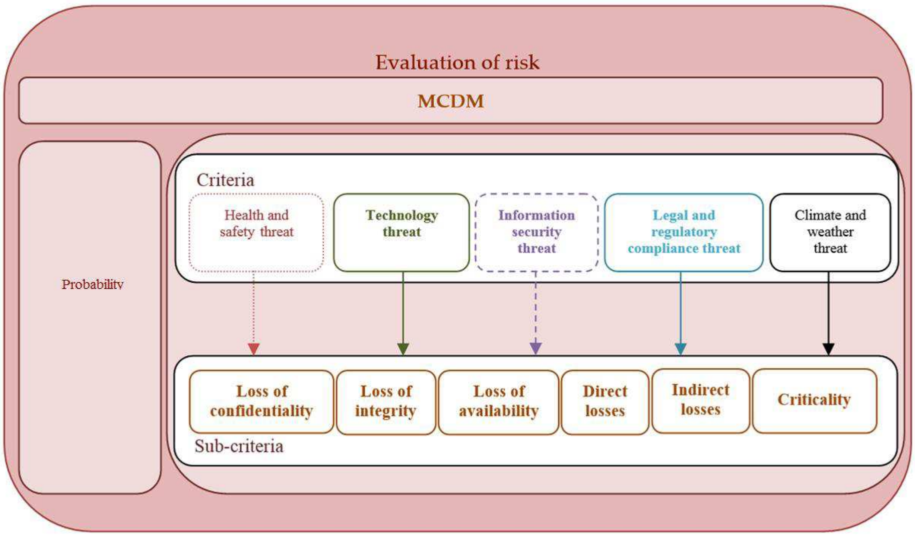

Fig. 3. Flowchart of the risk evaluation.

To assess risks, an expert needs to work on identifying types of threats. The list of threats is based on existing threats that create conditions for the entire information system to malfunction related to information security attributes (C – confidentiality, I – integrity, A – accessibility).

In the proposed model Integrated Delphic–Eckenrode's Likert-Type Scale-Based Fuzzy Rating and AHP methods were applied. AHP method is one of the most popular ones among MDM methods (Saaty and Erdener, 1979).

3.1. *Brief Review of Methodology of an Integrated Delphic-Eckenrode's Likert-Type Scale-Based Fuzzy Rating* (Turskis *et al.*, 2019)

The group decision-making processes are necessary to design and evaluate a set of different alternatives. One of the most important tasks is to reject those alternatives that do not meet lower bounds of the important criteria values. For a long time, a rigorous agreement was seen as a final group's opinion. In most cases, a group of experts who make real-life decisions have no strict and steady opinion about the same criteria and alternatives. An agreement of the group is reached when the most dominant players agree with the criteria ratings and performances of the considered alternatives. Real-life problems' modelling and solution lead the group of decision-makers to situations when models are based on vague logic. Besides, most often the models are based on the criteria rating in words. Such type of ratings cannot be replaced by the strict (crisp) numerical values. The fuzzy set theory allows decision takers to apply partially obtained information into the issue solving framework (Turskis *et al.*, 2012). A fuzzy set is characterized by a membership (characteristic) function which assigns to each object a grade of membership ranging (Zadeh, 1965). Different types of membership functions are available. In this research, the most commonly used triangular membership function is used (Dubois and Prade, 1978). A fuzzy triangular number will be denoted as (α, β, γ) (α – lower value of the fuzzy number, β – modal value of the fuzzy number, γ – upper value of the fuzzy number).

It is required to identify the importance of the activities of the different process managers before starting to assess the critical challenges of workplace safety's management, efficiency level of safety solutions and quality improvement. In order to achieve this, experts can use weighting methods for criteria. There are a lot of different subjective approaches for assessing weights: SWARA (Kersuliene *et al.*, 2010; Keshavarz-Ghorabaee *et al.*, 2018), FARE (FActor RElationship) (Ginevicius, 2011), and others.

Nominal group technique Delphi (Linstone and Turoff, 2002) is a useful tool for solving complicated problems which need expert data. It is a group decision-making process and includes idea generation, problem description, data assessment, and generation of feasible alternatives.

Likert scales are known as a tool for the measurement and assessment of attitudes. The reason for this is that the Likert scale is a straightforward tool to use and can be analysed effectively as interval or fuzzy scales (Allen *et al.*, 2017).

Eckenrode (1965) presented seminal work on criteria weights elicitation. Rating is sufficient for personal assessment, and it is especially useful for group decision making. It works well because it forces the expert to get clarity on his criteria and create a shared set of criteria. Eckenrode's Rating method is selected and modified by applying the basics of fuzzy sets theory in this study.

Risk assessment for each information infrastructure and analysis of the adequacy of risk management measures are carried out by experts.

3.2. *Problem Solution: Fuzzy Group Multi-Criteria Method in Assessing the Impact of Threat Implementation on the CII and Threat Probability*

To ensure sustainable functioning of CII, stakeholders should implement risk management processes. An integrated method of determination of criteria significance is developed to achieve the goals as mentioned earlier. The problem could be solved based on the survey of experts' data. There was formed a team of five experts, who have a university degree in IT and information security as well as actively work with risk management.

The standard seven-stage Delphi procedure is applied in the case research. Firstly, a facilitator describes to the participants the purpose and the procedure of the issue. Secondly, members of the group silently explain their opinion about the solution (criteria), with a short explanation in writing, not consulting or discussing their ideas with other participants. It ensures that all participants get an opportunity to make an equal contribution. Thirdly, a facilitator encourages a sharing and a discussion of reasons for the choices made (criteria) by each group member to identify common ground. Fourthly, participants verbally explain in details all presented ideas which are not clear for all participants of the groups or further details about any of the ideas that colleagues have produced and which may not be apparent to them. Fifthly, a facilitator eliminates duplicate solutions (criteria) from the list of all solutions, and the members proceed to rank the solutions starting from the most important to the least important. Sixthly, a facilitator includes a prioritizing procedure of the recorded ideas concerning the original problem. Following the voting and ranking process, a facilitator asks participants who have a different opinion about ranks from average criteria ranking some questions. Seventhly, a final ranking and rating of criteria should be done (Turskis *et al.*, 2019).

3.3. *Selection of Criteria and Sub-Criteria*

When solving problems by the MCDM method, first of all, a set of possible alternatives is formed, consisting of the CII. Next step is the selection of criteria and sub-criteria.

Criteria for risk assessment can be different. They depend on the infrastructure for which the risk is determined. In this case, the threats were taken as criteria. The experts determine the choice of threats aimed at the information infrastructure according to the Delphi method. The participants of the experts form a group, based on Sherwood *et al.* (2005). Then experts ranked and rated the impact of threats and probability of threats in the prevention of accidents at work. Based on the results, the following five threats that are most associated with cybersecurity were identified as criteria:

1) Health and safety threat (T1) – the threat to the personal health and safety of staff, customers and members of the population.

2) Technology threat (T2) – the threat of failure to plan, manage and monitor the performance of technology-related projects, product, services, processes, staff and delivery channels.

3) Information security threat (T3) – the threat of unauthorized disclosure or modification to information, or loss of availability of information, or inappropriate use of information.

4) Legal and regulatory compliance threat (T4) – the threat of failure to comply with the laws of the states in which business operations are carried out, or failure to comply with any regulatory, reporting, and taxation standards, or failure to comply with contracts, or failure of contracts to protect business interests.

5) Climate and weather threat (T5) – the threat of loss or damage caused by unusual climate conditions, including drought, heat, flood, cold, storm, and winds.

Each of the threats has its characteristics. According to Kosseff (2018), it is necessary to promote "identification, confidentiality, and integrality of public and private information, systems, and networks". Mena *et al.* (2018) focused on IoT inherent vulnerabilities and their implications to the fundamental information security challenges in confidentiality, integrity, and availability.

In this paper, the characteristics of the threats were taken as sub-criteria. It was proposed to choose sub-criteria, which focus on almost every aspect of security, i.e. protection of data from beginning to end. This work focuses on major six aspects of security, i.e. confidentiality, availability, integrity, direct losses, indirect losses, and criticality.

Thus, the following sub-criteria were chosen to solve the MCDM problem:

1) Loss of availability. Availability is the property of being accessible and usable upon demand by an authorized entity. Loss of availability can conclude performance degradation, short-term/long-term interruption, total loss (destruction).

2) Loss of confidentiality. Confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities, or processes. Confidentiality refers to keeping information secret from unauthorized entities (Sherman *et al.*, 2018). Loss of confidentiality can lead to internal disclosure, external disclosure of information, and others.

3) Loss of integrity. Integrity is the property of protecting the accuracy and completeness of assets. Loss of integrity can conclude accidental modification, deliberate modification, incorrect results, incomplete results, etc.

4) Direct losses are losses arising naturally, according to the usual course of things, from the breach of contract itself, and are therefore foreseeable and recoverable. Often these include financial costs.

5) Indirect losses are losses that arise from a particular circumstance of the case. Indirect losses, often referred to as "consequential losses", are not inflicted by the peril itself but describe losses which were suffered as a result or consequence of the direct loss. For example, reputational risks.

6) Criticality is the quality, state, or degree of being of the highest importance. In RCM terms, criticality is based on the consequence of failure. It is an essential criterion for information infrastructures provided critical services.

3.4. *The Importance of Threat Impact on CII*

According to the analysis of severity (Lough *et al.*, 2008), the importance of severity can be divided into five categories: insignificant (the client noticed a very slight failure), low (slight irritation of the client), medium (causes customer dissatisfaction, customer is annoyed), high (product does not work, client evils) and very high (the client is at risk, the safety rules are violated).

At the same time, some methods of risk analysis apply a 10-point scale for ranking the severity of risks (Table 1).

Table 1
Weight ranking scale based on Immawan *et al.* (2018).

Rating	Description	Definition
10	Extremely dangerous	Failure could cause the death of a person or infrastructure breakdown
8–9	Very dangerous	Failure could cause a significant injury or major infrastructure disruption with the interruption in service
6–7	Dangerous	Failure could cause a minor to moderate injury with a high degree of personal dissatisfaction or significant infrastructure issues requiring repairs
5	Moderate danger	Failure could cause a minor injury with some person dissatisfaction or significant infrastructure issues
3–4	Low to moderate danger	Failure could cause a very minor or no injury but annoys customers or results in minor infrastructure issues that can be overcome with minor modifications to the infrastructure or business
2	Slight danger	Failure could cause no injury, and the customer is unaware of the issue; however, the potential for minor injury exists
1	No danger	Failure causes no injury and has no impact on the infrastructure

Table 2
Weight ranking scale for the impact of the threats on CII.

Threat impact	Value	Threat impact level	Fuzzy triangular numbers		
abbreviation			α	β	γ
ED	10	Extremely dangerous	0.9	1	1
VD(H)	9	Very dangerous (high level)	0.8	0.9	1
VD(M)	8	Very dangerous (medium level)	0.8	0.9	1
D(H)	7	Dangerous (high)	0.6	0.7	0.8
D(M)	6	Dangerous (medium level)	0.5	0.6	0.7
MD	5	Moderate danger	0.4	0.5	0.6
LM(H)	4	Low to moderate danger (high level)	0.3	0.4	0.5
LM(M)	3	Low to moderate danger (medium level)	0.2	0.3	0.4
SD	2	Slight danger	0.1	0.2	0.3
ND	1	No danger	0	0.1	0.2

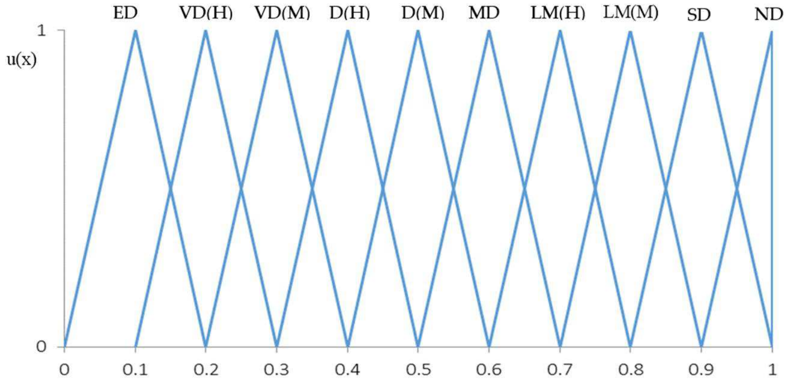

Fig. 4. Likert-type scale to determine the threat impact on CII.

The 10-level scale has more exact results of calculations. The weight depending on their importance determines further criteria. More critical criteria get higher weight values.

Based on the scale proposed in Table 1, the Likert-type scale is presented (Table 2, Fig. 4).

Rating: The raw rating assigned by the judge to each criterion, taking into account the sub-criteria, against the scale of 0 to 10 (10 most valuable) is treated as follows (Tables 3–4):

$$w_{cj} = \frac{p_{cj}}{\sum_{c=1}^{m} p_{cj}}, \tag{1}$$

where w_{cj} – weight computed for criterion c from the rating given by judge j, p_{cj} – rating given by judge j to criterion c, and w_c is calculated as follows:

$$w_c = \frac{\sum_{j=1}^{n} w_{cj}}{\sum_{j=1}^{n}\sum_{c=1}^{m} w_{cj}}. \tag{2}$$

Table 3
Impact of the threats on CII lexical evaluation based on Likert-type scale.

Impact of	Loss of availability experts					…	Criticality experts				
threats on CII	E_1	E_2	E_3	E_4	E_5	…	E_1	E_2	E_3	E_4	E_5
I_1	VD(M)	VD(M)	VD(H)	VD(H)	VD(H)	…	ED	ED	ED	VD(H)	ED
I_2	D(H)	VD(M)	D(M)	D(M)	D(H)	…	VD(H)	VD(H)	ED	VD(H)	VD(H)
I_3	D(M)	D(H)	D(H)	D(H)	D(M)	…	VD(M)	VD(M)	VD(M)	VD(M)	VD(M)
I_4	LM(H)	LM(M)	SD	SD	LM(M)	…	LM(H)	MD	D(M)	LM(H)	D(M)
I_5	D(M)	VD(H)	D(H)	D(M)	VD(M)	…	VD(M)	D(H)	D(M)	MD	MD

Using rules of fuzzy arithmetic, the equations (1) and (2) are modified as follows:

$$\begin{aligned}
\tilde{w}_{cj} &= \frac{\tilde{p}_{cj}}{\sum_{c=1}^{m}\tilde{p}_{cj}} = \left(\frac{p_{c\alpha j}}{\sum_{c=1}^{m}p_{c\gamma j}}; \frac{p_{c\beta j}}{\sum_{c=1}^{m}p_{c\beta j}}; \frac{p_{c\gamma j}}{\sum_{c=1}^{m}p_{c\alpha j}}\right),\\
\tilde{w}_{c} &= (w_{c\alpha}; w_{c\beta}; w_{c\gamma}) = \frac{\sum_{j=1}^{n}\tilde{w}_{cj}}{\sum_{j=1}^{n}\sum_{c=1}^{m}\tilde{w}_{cj}}\\
&= \left(\frac{\sum_{j=1}^{n}w_{c\alpha j}}{\sum_{j=1}^{n}\sum_{c=1}^{m}w_{c\gamma j}}; \frac{\sum_{j=1}^{n}w_{c\beta j}}{\sum_{j=1}^{n}\sum_{c=1}^{m}w_{c\beta j}}; \frac{\sum_{j=1}^{n}w_{c\gamma j}}{\sum_{j=1}^{n}\sum_{c=1}^{m}w_{c\alpha j}}\right),
\end{aligned} \tag{3}$$

where $w_{j\alpha} = \min_k y_{jk}$, $j = \overline{1,n}$, $k = \overline{1,p}$, is minimum possible value of j-th criterion, $w_{j\beta} = (\prod_{k=1}^{p} y_{jk})^{\frac{1}{p}}$, $j = \overline{1,n}$, is the most possible value of j-th criterion and $w_{j\gamma} = \max_k y_{jk}$, $j = \overline{1,n}$, $k = \overline{1,p}$, is the maximal possible value of j-th criterion.

A defuzzification should be applied before final decisions are made. The defuzzification is a process of producing a quantifiable result in crisp logic, given fuzzy logic, and corresponding membership degrees. A common and useful defuzzification technique is a centre of gravity. This method is selected in the case study (Turskis *et al.*, 2019).

$$w_c = \frac{1}{3}(w_{c\alpha} + w_{c\beta} + w_{c\gamma}). \tag{4}$$

The experts were requested to rate the main threats according to linguistic significance scale. Finally, linguistic variables are converted to fuzzy numbers and ranks determined (Tables 3–4, Fig. 5).

Fuzzy threat impact on CII values defuzzified as follows (Fig. 5).

The last stage is a calculation of a relative impact index (RI) of each considered threat (Fig. 6):

$$RI_c = \frac{w_c}{\max_c w_c}. \tag{5}$$

3.5. *Calculation of Probability of Threats Implementation*

Based on the method described above, the probability of threats implementation was defined (Tables 5–8, Fig. 7).

Fuzzy threat probability level values defuzzified as follows (Figs. 8, 9).

Table 4
Impact of the threats on CII expressed by fuzzy triangular numbers corresponding to the linguistic scale.

	E_1			E_2			E_3			E_4			E_5		
	α	β	γ	α	β	γ	α	β	γ	α	β	γ	α	β	γ
Loss of availability sub-criterion															
I_1	0.7	0.8	0.9	0.7	0.8	0.9	0.8	0.9	1	0.8	0.9	1	0.8	0.9	1
I_2	0.6	0.7	0.8	0.7	0.8	0.9	0.5	0.6	0.7	0.5	0.6	0.7	0.6	0.7	0.8
I_3	0.5	0.6	0.7	0.6	0.7	0.8	0.6	0.7	0.8	0.6	0.7	0.8	0.5	0.6	0.7
I_4	0.3	0.4	0.5	0.2	0.3	0.4	0.1	0.2	0.3	0.1	0.2	0.3	0.2	0.3	0.4
I_5	0.5	0.6	0.7	0.8	0.9	1	0.6	0.7	0.8	0.5	0.6	0.7	0.7	0.8	0.9
Loss of confidentiality sub-criterion															
I_1	0.3	0.4	0.5	0.1	0.2	0.3	0.2	0.3	0.4	0.2	0.3	0.4	0.1	0.2	0.3
I_2	0.2	0.3	0.4	0.2	0.3	0.4	0.1	0.2	0.3	0.1	0.2	0.3	0.1	0.2	0.3
I_3	0.2	0.3	0.4	0.2	0.3	0.4	0	0.1	0.2	0.2	0.3	0.4	0.1	0.2	0.3
I_4	0.1	0.2	0.3	0	0.1	0.2	0.1	0.2	0.3	0.1	0.2	0.3	0.1	0.2	0.3
I_5	0.1	0.2	0.3	0.1	0.2	0.3	0	0.1	0.2	0.1	0.2	0.3	0	0.1	0.2
Loss of integrity sub-criterion															
I_1	0.7	0.8	0.9	0.7	0.8	0.9	0.6	0.7	0.8	0.8	0.9	1	0.6	0.7	0.8
I_2	0.5	0.6	0.7	0.5	0.6	0.7	0.3	0.4	0.5	0.3	0.4	0.5	0.3	0.4	0.5
I_3	0.3	0.4	0.5	0.3	0.4	0.5	0.3	0.4	0.5	0.3	0.4	0.5	0.5	0.6	0.7
I_4	0.1	0.2	0.3	0.1	0.2	0.3	0.1	0.2	0.3	0.1	0.2	0.3	0.2	0.3	0.4
I_5	0.3	0.4	0.5	0.3	0.4	0.5	0.3	0.4	0.5	0.1	0.2	0.3	0.3	0.4	0.5
Direct losses sub-criterion															
I_1	0.7	0.8	0.9	0.7	0.8	0.9	0.6	0.7	0.8	0.8	0.9	1	0.6	0.7	0.8
I_2	0.6	0.7	0.8	0.6	0.7	0.8	0.6	0.7	0.8	0.5	0.6	0.7	0.6	0.7	0.8
I_3	0.5	0.6	0.7	0.5	0.6	0.7	0.3	0.4	0.5	0.3	0.4	0.5	0.5	0.6	0.7
I_4	0.1	0.2	0.3	0.1	0.2	0.3	0.1	0.2	0.3	0.1	0.2	0.3	0.2	0.3	0.4
I_5	0.3	0.4	0.5	0.3	0.4	0.5	0.3	0.4	0.5	0.1	0.2	0.3	0.1	0.2	0.3
Indirect losses sub-criterion															
I_1	0.8	0.9	1	0.7	0.8	0.9	0.6	0.7	0.8	0.7	0.8	0.9	0.8	0.9	1
I_2	0.6	0.7	0.8	0.6	0.7	0.8	0.6	0.7	0.8	0.7	0.8	0.9	0.7	0.8	0.9
I_3	0.3	0.4	0.5	0.5	0.6	0.7	0.3	0.4	0.5	0.7	0.8	0.9	0.3	0.4	0.5
I_4	0.3	0.4	0.5	0.4	0.5	0.6	0.1	0.2	0.3	0.3	0.4	0.5	0.2	0.3	0.4
I_5	0.5	0.6	0.7	0.3	0.4	0.5	0.5	0.6	0.7	0.3	0.4	0.5	0.3	0.4	0.5
Criticality sub-criterion															
I_1	0.9	1	1	0.9	1	1	0.9	1	1	0.8	0.9	1	0.9	1	1
I_2	0.8	0.9	1	0.8	0.9	1	0.9	1	1	0.8	0.9	1	0.8	0.9	1
I_3	0.7	0.8	0.9	0.7	0.8	0.9	0.7	0.8	0.9	0.7	0.8	0.9	0.7	0.8	0.9
I_4	0.3	0.4	0.5	0.4	0.5	0.6	0.5	0.6	0.7	0.3	0.4	0.5	0.5	0.6	0.7
I_5	0.7	0.8	0.9	0.6	0.7	0.8	0.5	0.6	0.7	0.4	0.5	0.6	0.4	0.5	0.6

4. Results and Discussions

As a result of the calculations, components that are necessary to calculate risk were obtained (Fig. 10).

AHP approach was used to compare each criteria taking into account the sub-criteria. As mentioned above, the Likert-type scale was used. Also, the questionnaire about expert's evaluation level toward threat choice was applied. It consists of 10 various levels.

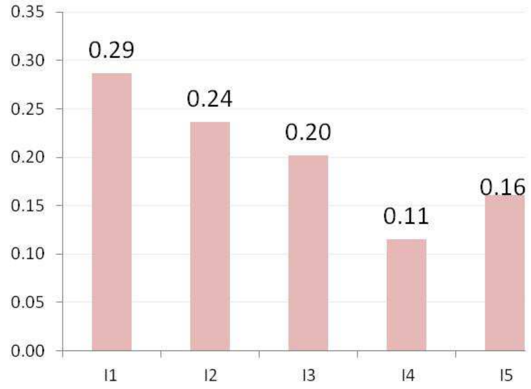

Fig. 5. Assessment of the threat impact on CII.

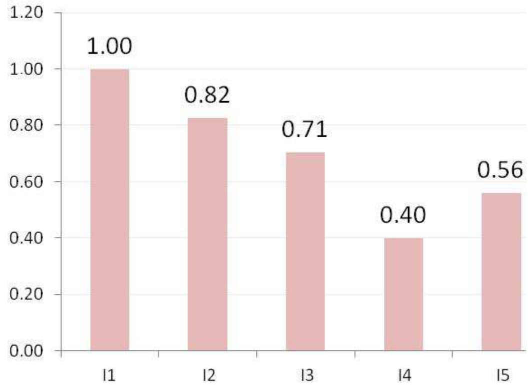

Fig. 6. RI-relative importance of the threat impact on CII.

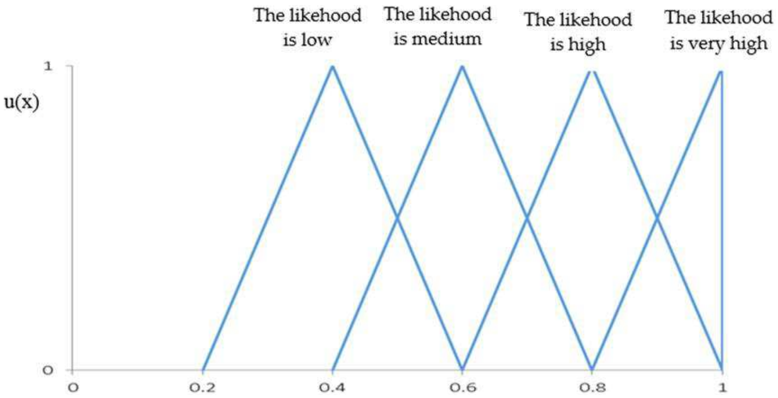

Fig. 7. Likert-type scale to determine the probability of the threats.

Table 5
Weight ranking scale for the probability of the threats.

Rating	Description	Definition
4	The probability is very high	Incidents were previously registered, and measures to prevent them have not been taken. Statistical data, the experience of other organizations, and world practice show the growth trend of these threats and their relevance for a given period. There is a great interest in the realization of this threat among intruders or competitors. There are a lot of critical vulnerabilities to implement the threats, or there is no check for vulnerabilities.
3	The probability is high	Incidents were previously registered, and measures to prevent them have not been fully implemented. Statistical data, the experience of other organizations, and world practice show the growth trend of these threats. There is an interest in the realization of this threat from intruders or competitors. There are critical vulnerabilities to implement the threat, or a vulnerability check has not been carried out.
2	The probability is medium	Incidents were previously registered, but measures to prevent them have been taken in full. Statistical data, the experience of other organizations, and world practice show no significant increase in the trend of the threats. There is little interest in the realization of this threat among intruders or competitors. There are no critical vulnerabilities to implement the threat.
1	The probability is low	Preventive incident prevention measures are taken regularly. Statistics, the experience of other organizations, and world practice shows a low growth trend of the threats. The interest in realizing this threat among intruders or competitors is low. There are minor vulnerabilities to the threat.

Table 6
Weight ranking scale for the probability of the threats.

Threat probability	Value	Probability level	Fuzzy triangular numbers		
abbreviation			α	β	γ
VH	4	The probability is very high	0.8	1	1
H	3	The probability is high	0.6	0.8	1
M	2	The probability is medium	0.4	0.6	0.8
L	1	The probability is low	0.2	0.4	0.6

The experts determine criteria weights. Table 9 presents the experts' integrated results for sub-criterion "Loss of availability". The priority weight vector describes the significance level of the criteria in the decision matrix. After getting the significance level of criteria, next calculations were used to assess the risk index of information infrastructures.

Thus, other matrices were created for all sub-criteria by five experts. (Table 10).

The probability level of threat implementation was also determined by the AHP method (Table 11).

Thus, other matrices were created according to the results of the five experts' answers (Table 12).

Normalized weight for impact and probability indexes is presented in Table 13.

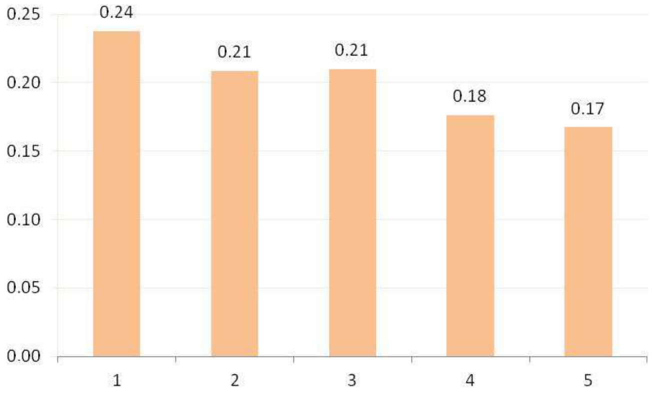

Fig. 8. Assessment of the threat probability values.

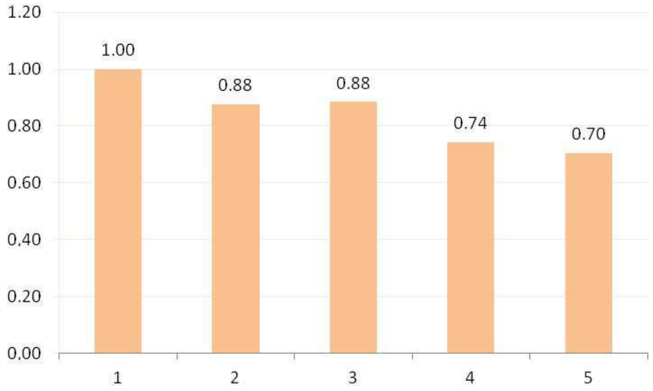

Fig. 9. Relative probability values.

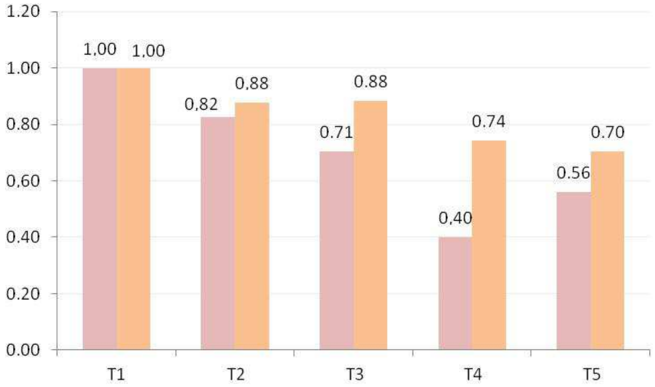

Fig. 10. Assessment of the threat impact on CII and probability of threat values.

Table 7
Probability of the threats lexical evaluation based on Likert-type scale.

Probability of	Experts				
threats on CII	E_1	E_2	E_3	E_4	E_5
P_1	H	M	M	M	M
P_2	H	M	M	L	M
P_3	M	M	M	M	M
P_4	L	L	M	M	M
P_5	L	L	L	M	L

Table 8
Probability level expressed by triangular fuzzy numbers corresponding to the linguistic scale.

	E_1			E_2			E_3			E_4			E_5		
	α	β	γ	α	β	γ	α	β	γ	α	β	γ	α	β	γ
P_1	0.6	0.8	1	0.4	0.6	0.8	0.4	0.6	0.8	0.4	0.6	0.8	0.4	0.6	0.8
P_2	0.6	0.8	1	0.4	0.6	0.8	0.4	0.6	0.8	0.2	0.4	0.6	0.4	0.6	0.8
P_3	0.4	0.6	0.8	0.4	0.6	0.8	0.4	0.6	0.8	0.4	0.6	0.8	0.4	0.6	0.8
P_4	0.2	0.4	0.6	0.2	0.4	0.6	0.4	0.6	0.8	0.4	0.6	0.8	0.4	0.6	0.8
P_5	0.2	0.4	0.6	0.2	0.4	0.6	0.2	0.4	0.6	0.4	0.6	0.8	0.2	0.4	0.6

Table 9
Pairwise comparisons of criteria weight.

		x_1	x_2	x_3	x_4	x_5	w
Health and safety threat	x_1	1	3	2	5	2	0.38
Technology threat	x_2	1/3	1	3	4	3	0.28
Information security threat	x_3	1/2	1/3	1	2	2	0.16
Legal and regulatory compliance threat	x_4	1/5	1/4	1/2	1	1	0.08
Climate and weather threat	x_5	1/2	1/3	1/2	1	1	0.10

Table 10
The results of the comparison of criteria weights.

	Loss of availability					…	Criticality					Result
	E_1	E_2	E_3	E_4	E_5	…	E_1	E_2	E_3	E_4	E_5	
T_1	0.38	0.38	0.31	0.44	0.33	…	0.39	0.41	0.35	0.43	0.33	0.34
T_2	0.28	0.25	0.32	0.18	0.30	…	0.24	0.20	0.25	0.21	0.30	0.25
T_3	0.16	0.17	0.16	0.18	0.15	…	0.20	0.20	0.22	0.16	0.16	0.19
T_4	0.08	0.09	0.10	0.10	0.11	…	0.08	0.10	0.08	0.10	0.11	0.11
T_5	0.10	0.11	0.11	0.10	0.11	…	0.10	0.10	0.10	0.10	0.10	0.11

Table 11
Pairwise comparisons of probability level.

		x_1	x_2	x_3	x_4	x_5	w
Health and safety threat	x_1	1	2	1	4	5	1
Technology threat	x_2	1/2	1	1	4	4	0.50
Information security threat	x_3	1	1	1	3	3	1.00
Legal and regulatory compliance threat	x_4	1/4	1/4	1/3	1	2	0.25
Climate and weather threat	x_5	1/5	1/4	1/3	1/2	1	0.20

Table 12
Weight comparison results.

	E_1	E_2	E_3	E_4	E_5	w
T_1	0.34	0.26	0.27	0.41	0.35	0.33
T_2	0.25	0.25	0.30	0.22	0.28	0.26
T_3	0.26	0.34	0.28	0.20	0.20	0.25
T_4	0.09	0.06	0.08	0.11	0.10	0.09
T_5	0.06	0.09	0.07	0.06	0.08	0.07

Table 13
Normalized weight for impact and probability indexes.

	For impact		For probability	
	w_{Eck}	w_{AHP}	w_{Eck}	w_{AHP}
Health and safety threat	0.29	0.34	0.24	0.33
Technology threat	0.24	0.25	0.21	0.26
Information security threat	0.20	0.19	0.21	0.25
Legal and regulatory compliance threat	0.11	0.11	0.18	0.09
Climate and weather threat	0.16	0.11	0.17	0.07

Table 14
The normalized integrated weight.

	The normalized integrated weight for impact index	The normalized integrated weight for probability index
Health and safety threat	0.31	0.29
Technology threat	0.25	0.24
Information security threat	0.20	0.24
Legal and regulatory compliance threat	0.11	0.12
Climate and weather threat	0.13	0.11

Integrating two methods.

The previously normalized results of the weights of the criteria and the threat probability were integrated according to Hwang and Yoon (1981):

$$w_j = \frac{w_{AHP}^{j} w_{Eck}^{j}}{\sum_{j=1}^{n}(w_{AHP}^{j} w_{Eck}^{j})}. \tag{6}$$

where $j = \overline{1, n}$.

The results of calculations by the equation (6) are given in Table 14.

According to OHSAS 18001, the risk for information infrastructure R is calculated as:

$$R = I \times P, \tag{7}$$

where I – impact of the threat implementation on information infrastructure, P – probability of implementation of the threats.

Table 15
Risks indicators and their ranking.

The threats	Risk value	Rank
Health and safety threat	0.399	1
Technology threat	0.265	2
Information security threat	0.213	3
Legal and regulatory compliance threat	0.060	5
Climate and weather threat	0.063	4

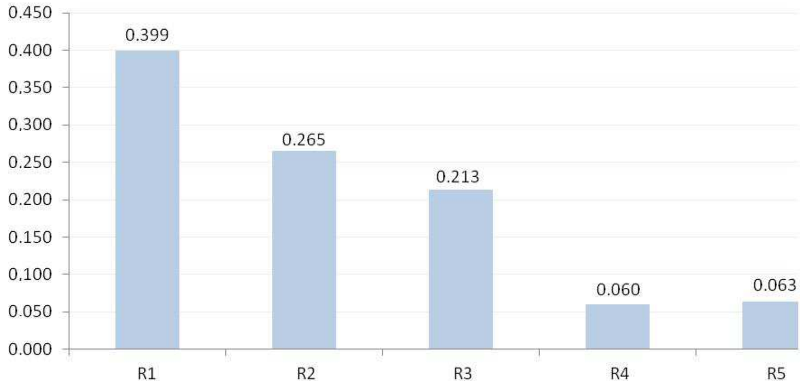

Fig. 11. Relative assessment of risk indicators for the proposed threats.

The risk was calculated according to equation (7), and the following results were obtained (Table 15, Fig. 11).

Thus, the most dangerous risk for CII is Health and safety risk. Technology as well as Information security risks are less significant risks. The lowest risks are Climate and weather as well as Legal and regulatory compliance risks.

The results of the study show what risks of threat realization must be mitigated initially.

5. Conclusions

This article describes a new model developed to analyse the risks of critical information infrastructures.

As described above, any failure in the information infrastructure, especially in the critical infrastructure, can lead not only to the disruption or termination of its functioning, but also to more global consequences in the form of large-scale monetary loss, its irreversible harmful destruction or a significant decrease in the level of public safety for an extended period of time. The possibility of disruption of such the infrastructures raises the risks that are associated with these technologies. In turn, the existence of risks leads to the need to find effective methods for evaluating them.

An important issue for each country is to prevent accidents and the suspension of production at CII. The introduction of the necessary measures to prevent the most probable and dangerous risks begins with their identification. However, risk identification is only one of the first steps in the risk management process. It is necessary to determine the importance of risks and their probability to start mitigating the most dangerous ones.

The best solutions to solve the issue can be achieved by applying scientific methods involving a large amount of information and calculations.

Experts present the initial data in similar group decision-making approaches in words. Each of the experts has his/her own opinion about criteria values. The significance of expert estimations was assessed with the help of the modified fuzzy group Eckenrode's rating method and the AHP method. The proposed approach is superior to conventional techniques because the proposed method can make group decisions in two environments. Therefore, it is a powerful tool to solve such problems.

Regular checking for risks using effective MCDM methods allows to prevent consequences that could suspend or damage the system. Risk assessment should be based on expert knowledge, which makes it possible to determine the frequency of occurrences of failures and their consequences to predict potential failures in the information infrastructures. Information about the risks realized, and the incidents that have occurred should be correctly collected, as inaccurate information can lead to severe losses. Thus, it is a very important and relevant topic for both Lithuania and other countries of the world.

The proposed model is aimed to solve the problem of calculating risks of the information infrastructures by applying the MCDM approach. Six main criteria were defined: "Loss of availability" and "Loss of confidentiality"; "Loss of integrity", "Direct losses", "Indirect losses" and "Criticality".

The study shows that the most important and possible risks rank as follows: Health and safety threat (rates as 0.4), Technology threat and Information security threat (rates from 0.21 to 0.27), Legal and regulatory compliance threat and Climate and weather threat (rates 0.06 and 0.063, respectively). The model presented in this study is suitable for determining the probability of risk and its impact, or for determining the importance of criteria in the multi-criteria utility function.

This model is proposed to be used further to calculate the risks of critical information infrastructures.

References

Allen, D.E., McAleer, M., Singh, A.K. (2017). Risk measurement and risk modelling using applications of Vine copulas. *Sustainability*, 9(10), 1762.

Allesch, A., Brunner, P.H. (2014). Assessment methods for solid waste management: a literature review. *Waste Management & Research*, 32(6), 461–473.

Ananda, J., Herath, G. (2009). A critical review of multi-criteria decision making methods with special reference to forest management and planning. *Ecological Economics*, 68(10), 2535–2548.

Aloini, D., Dulmin, R., Mininno, V. (2012). Risk assessment in ERP projects. *Information Systems*, 37(3), 183–199.

Akbari, M., Afshar, A., Mousavi, S.J. (2014). Multi-objective reservoir operation under emergency condition: abbaspour reservoir case study with non-functional spillways. *Journal of Flood Risk Management*, 7(4), 374–384.

Bamakan, S.M.H., Dehghanimohammadabadi, M. (2015). A weighted Monte Carlo simulation approach to risk assessment of information security management system. *International Journal of Enterprise Information Systems (IJEIS)*, 11(4), 63–78.

Bannerman, P.L. (2008). Risk and risk management in software projects: A reassessment. *Journal of Systems and Software*, 81(12), 2118–2133.

Bates, M.E., Sparrevik, M., De Lichy, N., Linkov, I. (2014). The value of information for managing contaminated sediments. *Environmental Science & Technology*, 48(16), 9478–9485.

Baynal, K., Sari, T., Akpinar, B. (2018). Risk management in automotive manufacturing process based on FMEA and grey relational analysis: a case study. *Advances In Production Engineering & Management*, 13(1), 69–80.

Bell, T.E. (1989). Managing Murphy's law: engineering a minimum-risk system. *IEEE Spectrum*, 26(6), 24–27.

Boehm, B.W. (1991). Software risk management: principles and practices. *IEEE Software*, 8(1), 32–41.

Boranbayev, A., Boranbayev, S., Nurusheva, A., Yersakhanov, K. (2018a). The modern state and the further development prospects of information security in the Republic of Kazakhstan. In: *Information Technology – New Generations*. Springer, Cham, pp. 33–38.

Boranbayev, A., Boranbayev, S., Nurusheva A., Yersakhanov K. (2018b). Development of a software system to ensure the reliability and fault tolerance in information systems. *Journal of Engineering and Applied Sciences*, 13(23), 10080–10085.

Boranbayev, A., Boranbayev, S., Yersakhanov, Y., Nurusheva, A., Taberkhan, R. (2018c). Methods of ensuring the reliability and fault tolerance of information systems. In: *Information Technology – New Generations*. Springer, Cham, pp. 729–730.

Boranbayev, S., Goranin, N., Nurusheva, A. (2018d). The methods and technologies of reliability and security of information systems and information and communication infrastructures. *Journal of Theoretical and Applied Information Technology*, 96(18), 6172–6188.

Cagliano, A.C., Grimaldi, S., Rafele, C. (2015). Choosing project risk management techniques. A theoretical framework. *Journal of Risk Research*, 18(2), 232–248.

Can, G.F. (2018). An intuitionistic approach based on failure mode and effect analysis for prioritizing corrective and preventive strategies. *Human Factors and Ergonomics in Manufacturing & Service Industries*, 28(3), 130–147.

Caplinskas, A., Dzemyda, G., Kiss, F., Lupeikiene, A. (2012). Processing of undesirable business events in advanced production planning systems. *Informatica*, 23(4), 563–579.

de Almeida, A.T., Ferreira, R.J.P., Cavalcante, C.A.V. (2015). A review of the use of multicriteria and multi-objective models in maintenance and reliability. *IMA Journal of Management Mathematics*, 26(3), 249–271.

Dubois, D., Prade, H. (1978). Operations on fuzzy numbers. *International Journal of Systems Science*, 9(6), 613–626.

Eckenrode, R.T. (1965). Weighting multiple criteria. *Management Science*, 12(3), 180–192.

Garcez, T.V., de Almeida, A.T. (2014). Multidimensional risk assessment of manhole events as a decision tool for ranking the vaults of an underground electricity distribution system. *IEEE Transactions on Power Delivery*, 29(2), 624–632.

Garcia, M.N.M., Roman, I., Garcia, Penalvo, F., Bonilla M. (2008). An association rule mining method for estimating the impact of project management policies on software quality, development time and effort. *Expert Systems with Applications*, 34(1), 522–529.

Ginevicius, R. (2011). A new determining method for the criteria weights in multicriteria evaluation, *International Journal of Information Technology & Decision Making*, 10(6), 1067–1095.

Giraud, L., Galy, B. (2018). Fault tree analysis and risk mitigation strategies for mine hoists. *Safety Science*, 110, 222–234.

Govindan, K., Chaudhuri, A. (2016). Interrelationships of risks faced by third party logistics service providers: a DEMATEL based approach. *Transportation Research Part E: Logistics and Transportation Review*, 90, 177–195.

Grabauskyte, I., Tamosiunas, A., Kavaliauskas, M., Radisauskas, R., Bernotiene, G., Janilionis, V. (2018). A comparison of decision tree induction with binary logistic regression for the prediction of the risk of cardiovascular diseases in adult men. *Informatica*, 29(4), 675–692.

Jin, F., Pei, L., Chen, H., Zhou, L. (2014). Interval-valued intuitionistic fuzzy continuous weighted entropy and its application to multi-criteria fuzzy group decision making. *Knowledge-Based Systems*, 59, 132–141.

Jozi, S.A., Majd, N.M. (2014). Health, safety, and environmental risk assessment of steel production complex in central Iran using TOPSIS. *Environmental Monitoring and Assessment*, 186(10), 6969–6983.

Haimes, Y.Y. (1991). Total risk management. *Risk Analysis*, 11(2), 169–171.

Han, W.M. (2015). Discriminating risky software project using neural networks. *Computer Standards & Interfaces*, 40, 15–22.

Hwang, C.L., Yoon, K. (1981). *Multiple Attribute Decision Making: Methods and Applications*. Springer-Verlag, Berlin, pp. 15–22.

Hu, K.H., Jianguo, W., Tzeng, G.H. (2017). Risk factor assessment improvement for China's cloud computing auditing using a new hybrid MADM model. *International Journal of Information Technology & Decision Making*, 16(03), 737–777.

Ijadi Maghsoodi, A., Hafezalkotob, A., Azizi Ari, I., Ijadi Maghsoodi, S., Hafezalkotob, A. (2018). Selection of waste lubricant oil regenerative technology using entropy-weighted risk-based fuzzy axiomatic design approach. *Informatica*, 29(1), 41–74.

Immawan, T., Sutrisno, W., Rachman, A.K. (2018). Operational risk analysis with fuzzy FMEA (Failure Mode and Effect Analysis) approach (case study: optimus creative bandung). In: *MATEC Web Conference*, Vol. 154, 01084. EDP Sciences.

Kaklauskas, A., Dzemyda, G., Tupenaite, L., Voitau, I., Kurasova, O., Naimaviciene, J., Rassokha, Y., Kanapeckiene, L. (2018). Artificial neural network-based decision support system for development of an energy-efficient built environment. *Energies*, 11(8).

Kersuliene, V., Zavadskas, E.K., Turskis, Z. (2010). Selection of rational dispute resolution method by applying new step?wise weight assessment ratio analysis (SWARA). *Journal of Business Economics and Management*, 11(2), 243–258.

Keshavarz-Ghorabaee, M., Amiri, M., Zavadskas, E.K., Turskis, Z., Antucheviciene, J. (2018). An extended step-wise weight assessment ratio analysis with symmetric interval type-2 fuzzy sets for determining the subjective weights of criteria in multi-criteria decision-making problems. *Symmetry*, 10(4), 91.

Kosseff, J. (2018). Cybersecurity of the Person. *Law Review*. 103(3), 985–1031.

Linkov, I., Satterstrom, F.K., Kiker, G., Batchelor, C., Bridges, T., Ferguson, E. (2006). From comparative risk assessment to multi-criteria decision analysis and adaptive management: Recent developments and applications. *Environment International*, 32(8), 1072–1093.

Linstone, H.A., Turoff, M. (2002). *The Delphi Method: Techniques and Applications*. Addison-Wesley Publishing Company: Advanced Book Program, 18.

Lo, H.W., Liou, J.J.H. (2018). A novel multiple-criteria decision-making-based FMEA model for risk assessment. *Applied Soft Computing*, 73, 684–696.

Lough, K.G., Stone, R.B., Tumer, I. (2008). Implementation procedures for the risk in early design (red) method. *Journal of Industrial and Systems Engineering (JISE)*, 2(2), 126–143.

Ma, J., Bai, Y., Shen, J., Zhou, F. (2013). Examining the impact of adverse weather on urban rail transit facilities on the basis of fault tree analysis and fuzzy synthetic evaluation. *Journal of Transportation Engineering*, 140(3), 04013011.

Macary, F., Dias, J.A., Figueira, J.R., Roy, B. (2014). A multiple criteria decision analysis model based on ELECTRE TRI-C for erosion risk assessment in agricultural areas. *Environmental Modeling & Assessment*, 19(3), 221–242.

Medineckiene, M., Zavadskas, E.K., Bjork, F., Turskis, Z. (2015). Multi-criteria decision-making system for sustainable building assessment/certification. *Archives of Civil and Mechanical Engineering*, 15, 11–18.

Mena, D.M., Papapanagiotou, I., Yang, B.J. (2018). Internet of things: survey on security. *Information Security Journal*, 27(3), 162–182.

Miao, X., Yu, B., Xi, B., Tangd, Y.H. (2010). Modeling of bilevel games and incentives for a sustainable critical infrastructure system. *Technological and Economic Development of Economy*, 16(3), 365–379.

Muniz, M.V.P., Lima, G.B.A., Caiado, R.G.G., Quelhas, O.L.G. (2018). Bow tie to improve risk management of natural gas pipelines. *Process Safety Progress*, 37(2), 169–175.

Navickiene, O., Sprindys, J., Siaulys, J. (2018). The Gerber–Shiu discounted penalty function for the bi-seasonal discrete time risk model. *Informatica*, 29(4), 733–756.

Olifer, D., Goranin, N., Janulevicius, J., Kaceniauskas, A., Cenys, A. (2017). Improvement of security costs evaluation process by using data automatically captured from BPMN and EPC models. In: *International Conference on Business Process Management*. Springer, Cham, pp. 698–709.

Papamichail, K.N., French, S. (2012). 25 years of MCDA in nuclear emergency management. *IMA Journal of Management Mathematics*, 24(4), 481–503.

Pfeifer, J., Barker, K., Ramirez-Marquez, J.E., Morshedlou, N. (2015). Quantifying the risk of project delays with a genetic algorithm. *International Journal of Production Economics*, 170, 34–44.

Saaty, T.L., Erdener, E. (1979). A new approach to performance measurement the analytic hierarchy process. *Design Methods and Theories*, 13(2), 62–68.

Saaty, T.L., Ergu, D. (2015). When is a decision-making method trustworthy? Criteria for evaluating multi-criteria decision-making methods. *International Journal of Information Technology & Decision Making*, 14(06), 1171–1187.

Safari, H., Faraji, Z., Majidian, S. (2016). Identifying and evaluating enterprise architecture risks using FMEA and fuzzy VIKOR. *Journal of Intelligent Manufacturing*, 27(2), 475–486.

Sangaiah, A.K., Samuel, O.W., Li, X., Abdel-Basset, M., Wang, H. (2018). Towards an efficient risk assessment in software projects – fuzzy reinforcement paradigm. *Computers & Electrical Engineering*, 71, 833–846.

Saparauskas, J., Zavadskas, E.K., Turskis, Z. (2011). Selection of facade's alternatives of commercial and public buildings based on multiple criteria. *International Journal of Strategic Property Management*, 15(2), 189–203.

Sherman, A.T., DeLatte, D., Neary, M., Oliva, L., Phatak, D., Scheponik, T., Herman, G.L., Thompson J. (2018). Cybersecurity: exploring core concepts through six scenarios. *Cryptologia*, 42(4), 337–377.

Sherwood, J., Clark, A., Lynas, D. (2005). *Enterprise Security Architecture: A Business-Driven Approach*. Computer Security Institute, CMPBooks, CA, USA, Gail Saari.

Sivilevicius, H., Zavadskas, E.K., Turskis, Z. (2008). Quality attributes and complex assessment methodology of the asphalt mixing plant. *Baltic Journal of Road & Bridge Engineering*, 3(3), 161–166.

Tamilselvi, J.J. (2018). Fuzzy multi-criteria random seed and cutoff point approach for credit risk assessment. *Journal of Theoretical and Applied Information Technology*, 96(4), 1150–1163.

Tavana, M., Khalili-Damghani, K., Abtahi, A.R. (2013). A hybrid fuzzy group decision support framework for advanced-technology prioritization at NASA. *Expert Systems Applications*, 40(2), 480–491.

Taylor, J.R. (2017). Automated HAZOP revisited. *Process Safety and Environmental Protection*, 111, 635–651.

Turskis, Z., Lazauskas, M., Zavadskas, E.K. (2012). Fuzzy multiple criteria assessment of construction site alternatives for non-hazardous waste incineration plant in Vilnius city, applying ARAS-F and AHP methods. *Journal of Environmental Engineering and Landscape Management*, 20(2), 110–120.

Turskis, Z., Zavadskas, E.K., Antucheviciene, J., Kosareva, N.A. (2015). Hybrid model based on fuzzy AHP and fuzzy WASPAS for construction site selection. *International Journal of Computers Communications & Control*, 10(6), 873–888.

Turskis, Z., Dzitac, S., Stankiuviene, A., Sukys, R. (2019). A fuzzy group decision-making model for determining the most influential persons in the sustainable prevention of accidents in the construction SMEs. *International Journal of Computers, Communications & Control*, 14(1), 90–106. doi:10.15837/ijccc.2019.1.3364.

Vrhovec, S.L., Hovelja, T., Vavpotic, D., Krisper, M. (2015). Diagnosing organizational risks in software projects: Stakeholder resistance. *International Journal of Project Management*, 33(6), 1262–1273.

Woodward, M., Kapelan, Z., Gouldby, B. (2014). Adaptive flood risk management under climate change uncertainty using real options and optimization. *Risk Analysis*, 34(1), 75–92.

Yan, F., Xu, K. (2018). A set pair analysis based layer of protection analysis and its application in quantitative risk assessment. *Journal of Loss Prevention in the Process Industries*, 55, 313–319.

Yasseri, S., Mahani, R. (2013). *Quantitative Risk Assessment for Oil and Gas Facilities*. Smart Petroleum Ltd., Manchester, UK.

Yusta, J.M., Correa, G.J., Lacal-Arántegui, R. (2011). Methodologies and applications for critical infrastructure protection: state-of-the-art. *Energy Policy*, 39(10), 6100–6119.

Zadeh, L.A. (1965). Fuzzy sets. *Information and Control*, 8(3), 338–353.

Zavadskas, E.K., Antucheviciene, J., Saparauskas, J., Turskis, Z. (2013). MCDM methods WASPAS and MULTIMOORA: verification of robustness of methods when assessing alternative solutions. *Economic Computation and Economic Cybernetics Studies and Research*, 47(2), 5–20.

Zavadskas, E.K., Antucheviciene, J., Turskis, Z., Adeli, H. (2016a). Hybrid multiple-criteria decision-making methods: A review of applications in engineering. *Scientia Iranica. Transaction A, Civil Engineering*, 23(1), 1–20.

Zavadskas, E.K., Govindan, K., Antucheviciene, J., Turskis, Z. (2016b). Hybrid multiple criteria decision-making methods: A review of applications for sustainability issues. *Economic Research-Ekonomska Istraživanja*, 29(1), 857–887.

Zavadskas, E.K., Kaklauskas, A., Turskis, Z., Kalibatas, D. (2009). An approach to multi-attribute assessment of indoor environment before and after refurbishment of dwellings. *Journal of Environmental Engineering and Landscape Management*, 17(1), 5–11.

Zavadskas, E.K., Turskis, Z., Antucheviciene, J., Zakarevicius, A. (2012). Optimization of weighted aggregated sum product assessment. *Elektronika ir Elektrotechnika*, 122(6), 3–6.

Zavadskas, E.K., Turskis, Z., Antucheviciene, J. (2015a). Selecting a contractor by using a novel method for multiple attribute analysis: weighted aggregated sum product assessment with grey values (WASPAS-G). *Studies in Informatics and Control*, 24(2), 141–150.

Zavadskas, E.K., Turskis, Z., Bagocius, V. (2015b). Multi-criteria selection of a deep-water port in the Eastern Baltic Sea. *Applied Soft Computing*, 26, 180–192.

Zolfani, S.H., Zavadskas, E.K., Turskis, Z. (2013). Design of products with both International and Local perspectives based on Yin-Yang balance theory and SWARA method. *Economic Research-Ekonomska Istrazivanja*, 26(2), 153–166.

Zhao, H., You, J.X., Liu, H.C. (2017). Failure mode and effect analysis using MULTIMOORA method with continuous weighted entropy under interval-valued intuitionistic fuzzy environment. *Soft Computing*, 21(18), 5355–5367.

Zhou, Q., Thai, V.V. (2016). Fuzzy and grey theories in failure mode and effect analysis for tanker equipment failure prediction. *Safety Science*, 83, 74–79.

Z. Turskis is prof. dr. of technical sciences, professor at the Department of Construction Management and Real Estate, chief research fellow at the Laboratory of Operational Research, Research Institute of Sustainable Construction, Vilnius Gediminas Technical University, Lithuania. Research interests: building technology and management, decision-making theory, computer-aided automation in design, expert systems. He is the author of more than 120 research papers, which are referred in the Web of Science database.

N. Goranin, PhD, associated professor at the Department of Information Systems, vice-dean for research and international relations at Faculty of Fundamental Sciences at Vilnius Gediminas Technical University. Has job experience as a system administrator, FP6 and EU structural funds project coordinator. Member of ISACA Lithuania Board. Keeps the position of Chief Information Security Officer at Level 1 (VISA classification) service provider (responsible for PCI DSS compliance and certification). Keeps the CISM and CISA certificates. Has published over 30 papers. Research interests: information security technologies, information security management, artificial intelligence in information security, information security process modelling.

A. Nurusheva is a PhD student at the Department of Information Systems, Gumilyov Eurasian National University, Astana, Kazakhstan. Research interests: information technologies, risk management, reliability, decision-making theory, computer-aided automation in design, expert systems.

S. Boranbayev is prof. dr. of technical sciences, professor at the Department of Information Systems, Gumilyov Eurasian National University, Astana, Kazakhstan. Member of American Mathematical Society (2006), academician of the International Academy of Informatization (2009). The author and co-author of more than 100 papers and monographs. Scientific interests: information and computer technologies, reliability and security of information and computer systems, mathematical cybernetics, mathematical and computer modelling, system analysis, artificial intelligence.