Scientific Journal of Silesian University of Technology. Series Transport
Zeszyty Naukowe Politechniki Śląskiej. Seria Transport

Volume 108 **2020**

p-ISSN: 0209-3324

e-ISSN: 2450-1549

DOI: https://doi.org/10.20858/sjsutst.2020.108.9

Journal homepage: http://sjsutst.polsl.pl

Article citation information:
Korecki, Z., Adámková, B. Multi-criteria evaluation of critical infrastructure resilience and economic impacts in selected airports in the Czech Republic. *Scientific Journal of Silesian University of Technology. Series Transport*. 2020, **108**, 95-106. ISSN: 0209-3324.
DOI: https://doi.org/10.20858/sjsutst.2020.108.9.

Zbyšek KORECKI[1], Blanka ADÁMKOVÁ[2]

MULTI-CRITERIA EVALUATION OF CRITICAL INFRASTRUCTURE RESILIENCE AND ECONOMIC IMPACTS IN SELECTED AIRPORTS IN THE CZECH REPUBLIC

Summary. A region's economic development stability is directly linked to the level of services provided and the transport and communication infrastructure available to it. Airport security in the context of transport infrastructure development and the further development of regional logistics facilities is an important factor affecting both the public and private sectors. The causes and consequences investigation, which are the basic means for finding solutions in the safety area of the selected critical infrastructure subject was solved using the Ishikawa diagram. The search for causation based on the principle where each result has its own cause or combination of causes.

We can use the 6M approach (staff, methods, machines, materials, measurement, and mother-nature), or 8M, which is supplemented by management and maintenance. In the process of elaborating this article, the consequences defined and the causes underlying the proposed solutions were examined in a successive way. This paper points out possible directions of development in the field of airport security within the context of the public logistics centre development. Obviously, there is no totally secure system and an increase in the

[1] Faculty of Military Technology. University of Defence, Kounicova 65, 662 10 Brno, Czech Republic, Email: zbysek.korecki@unob.cz
[2] Ministry of Defence, Tychonova 221/1, 160 00 Praha, Czech Republic, Email: blanka.adamkova@email.cz

level of security can be ensured by correlating all systems used to increase of the critical infrastructure elements resilience.

Keywords: airport infrastructure, critical infrastructure, resilience of critical infrastructure, airport expansion, stability

1. INTRODUCTION

The present dynamically developing world is constantly exposed to security threats and risks, prompting the issue of company protection to be discussed and addressed at national and international levels. The security threats require continuity and a comprehensive approach to security. In order to ensure safety as a whole, it is necessary to address specific areas of securing functional infrastructure, a system serving to protect human lives, health, property and the environment [1].

Critical infrastructure defined as "a critical infrastructure element or critical infrastructure element system whose disruption of function would have a serious impact on national security, the essential living needs of the population provision, human health or the economy of the State" [2].

An airport is a defined area of land or water, including buildings, facilities and equipment, intended either wholly or in part for the arrivals, departures and ground movements of aircraft. Airport security is a set of organisational, technical, economic, environmental and other measures for ensuring the serviceability of airfields and airport facilities for air traffic. These measures achieved through the aerodrome for air operations preparation, its maintenance and repairs [3,4].

Aerodrome preparation for air traffic is a set of measures designed to enforce the working limits of the movement area and airport facilities. Aerodrome portability is the area movement condition and aerodrome equipment, which is determined by values meeting the limits for aircraft operation.

Airport portability is based on data from the following areas:

- condition and operating limits of the movement area,
- bearing capacity of paved and unpaved movement surface,
- friction and braking characteristics on a paved runway (RWY),
- the state of restraint systems.

The term security is defined as “a state where a system is able to withstand known and predictable (and unexpected) external and internal threats that can negatively affect each element (or the system) to keep up the system structure, stability and reliability and targeted behaviour” [5,6,7].

The key issues in the field of security are aimed at protecting the fundamental values of life, health, property rights of the population, the environment, etc., and expressing areas of protected interest. Threats and implied risks are reasons efforts are made to protect our values.

The level of safety reflects the likelihood of an incident occurring, which will very much affect protected interest. This is a hazard or event that can or will cause damage or harm to a particular value [8].

A threat is defined as the cause of a negative event that causes the most harmful effects, expressed most likely by chance. The Czech Republic in the document, Threat Analysis for the Czech Republic [9,1,11], defined 22 out of a total of 72 identified types of hazards threatening the territory of the Czech Republic, which need increased attention. The identified hazard types are autogenic (abiotic, biotic) or anthropogenic (technologic, economic).

2. RISK ANALYSIS

Risk analysis allows one analyse risks for a specifically defined asset area based on the classification. Evaluated threats and vulnerabilities allow defining the relationship to a selected critical infrastructure area according to the formula:

$$R=A \times T \times V \tag{1}$$

Where: R – Risk, A – Asset, T – Threat, V – Vulnerability.

Using the method of multitude quantitative risk analysis alongside mutual correlation, the dependency of the management structure of the selected critical infrastructure area is then determined, which is expressed by the mutual relation of identified risks. The outputs are thereafter reflected in the process of determining the requirements of critical infrastructure protection management in the areas [12,13,14] of physical security, information security, administrative and people security and crisis management and planning.

Risk analysis is an essential building block for risk management [15]. It serves to find undesirable phenomena, assesses the level of risks in preparation for dealing with emergencies and crisis. The process of risk analysis processing aims to get the basis for risk assessment and identification of threats to the entity. Subsequent outputs from risk analysis propose a coherent framework applicable to the implementation of the measures in the framework of preventive action, in the process of preparing for an emergency or carrying out activities during an emergency.

There are several basic approaches to risk analysis processing: quantitative risk analysis, checklist analysis, safety audit, what-if analysis, preliminary hazard analysis, failure mode and effect analysis.

The authors of this paper used the Ishikawa diagram (cause and effect diagram), which is based on the proposition that each result or problem has its cause or a combination thereof. It is the best-known team method of problem analysis, which aims to decide the most likely cause of the question. Based on the hierarchical factors that influence each other in the process, the causes are gradually generated, and thus, analysed [16,17].

The whole process of creating a diagram comprises of the basic steps consisting of identifying the analysed problem, defining the root causes of the problem. The main and secondary causes are further plotted on the side branches of the diagram, giving the possibility to decide the subgroups of causes to the main causes. Subsequently, the weighting factors assigned to the causes, where the need to take measures to cut the risk arises according to the weight of the cause.

The Ishikawa diagram creation is based on defining the problem with the basic areas being labelled “8M”. It is presented thus:

- manpower – qualification, training, responsibility,
- methods – technological, manufacturing and service procedures,
- machines – transport and handling equipment, warehouses, information and communication means,

- materials – documents, information sources and energy sources, raw materials,
- measurement – standards, regulations,
- mother-nature – environment and environmental impacts,
- management - causes initiated by incorrect management,
- maintenance - causes due to improper maintenance [18].

In the next step, smaller branches expressing groups of possible causes assigned to the basic areas are represented by the branches of the graph, according to the division “6M”. When creating groups of causes, other possible causes are described based on different aspects of the problem being solved until all possibilities are exhausted. From a practical point of view, the second level is recommended.

2.1. Probability - consequences and evaluator's opinion method

The semi-quantitative PNH method is used to check the Ishikawa diagram for an independent point evaluation of causes. It is a simple method of risk assessment using three components:

- probability (P),
- consequences (C),
- evaluator's opinion (E).

The rate of risk determination is then calculated using the formula:

$$RR = A \times T \times V \tag{2}$$

Where: RR – Rate of risk, P – Probability, C – Consequences, E – Evaluator's opinion.

The risk elimination process continues by identifying tasks to cut the causes and implementing control mechanisms to verify that the cause persists in the process or is eliminated [19,20].

3. ANALYSIS OF OBJECT PROTECTION LEVEL

The terminal and most of the area is situated in the cadastral area of the Brno district of Tuřany, part of the airport area extends into the cadastral area of the town of Šlapanice and in the cadastral area of the Brno district of Dvorska.

The airport terminal is located 1.6 km from the D1 motorway, close to exit 201 Brno-Slatina and a public logistics centre built around the terminal.

In the neighbourhood, a solar photovoltaic power plant is ready on the airport grounds. Railway Modernisation of the Brno - Přerov line is prepared by Infrastructure Administration to a line speed of 200 km/h and a new stop arise at the airport, which should improve the transport accessibility of the airport.

In the spring of 2009, the South Moravian Regional Authority published development plans for the next five-year period [21], which includes, inter alia:

- complete airport security including CCTV installation,
- reconstruction of the guidance system for zero visibility conditions (ILS CAT IIIc),

- construction of cargo terminal, and thereafter, the logistic centre with connection to motorway and railway network.

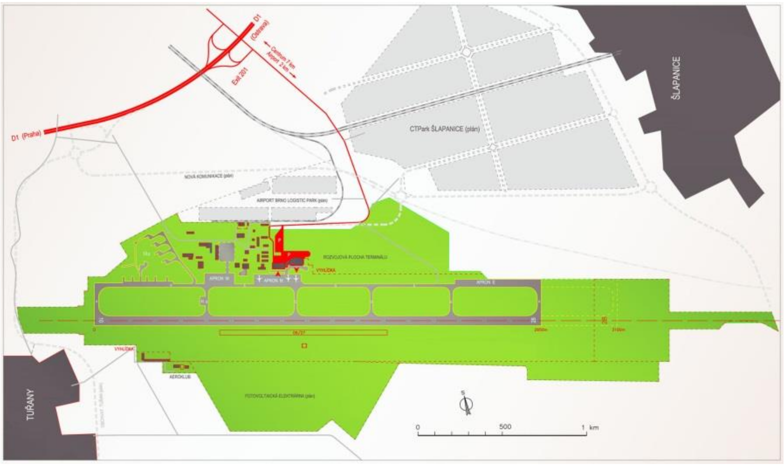

Fig. 1. Graphic scheme of the public airport Brno-Tuřany

Within the extensive issue of risk analysis, the object is assessed at several levels for the purposes of the basic evaluation. In the first level, the risks to the object from the external and internal environment are evaluated.

The airport complex itself has a lot of buildings, parking areas, garage parking for heavy machinery, tempered garage parking, workshops, warehouses, chemical plants and other technical operating facilities, including an office building.

The main aim of object protection is to set a standard of security to ensure the required level of physical security, which is primarily to:

- avoid damage, theft and unauthorised use of tangible property,
- prevent theft and misuse of intangible assets (for example, intellectual property, know-how, etc.).

The building level security and the protection elements application met by the requirements of the Czech state standard ČSN P 73 4450-1 Physical protection of a critical infrastructure element. It specifies general requirements for a system of physical protection of elements to decrease the impact of anthropogenic threats, including a terrorist attack. The standard clearly covers the process of designing a physical protection system and areas of technical, regime measures, physical surveillance depending on the group of the building, including the system the implementation [22,23].

3.1. Physical protection

Physical protection means a concrete guarding of an object by live force. Security of the building provided by a specialised body, security service, which performs the following tasks:

- prevent unauthorised persons from entering the facility, non-public areas and areas with special modes of entry and movement of persons,
- identify potential threats and take immediate action to stop them,
- protection of external and internal perimeter,
- operation of technical protection equipment,

- checking entry and exit vehicles,
- immediate intervention in the disruption event of the building, signalling of security devices,
- application of necessary defence and extreme emergency, eventually detention of a person,
- keeping the necessary documentation.

3.2. Technical means

The technical means are electronic and mechanical devices recording or preventing unauthorised entry into buildings.

Tab. 1

Technical means

Enclosure	Gates	Lighting	Locks
Walls	Barriers	Doors	Safety glass and foil
Fences	Blinds	Grilles	

The area is closed all around its perimeter. In a part of the area, the intrusion protection consists of fencing. The area entered through the main entrance or entrance to the area, which is equipped with a remote-controlled barrier.

3.3. Signal security devices

Signalling and early warning devices in the fire event or other event serve to detect and show disruption of buildings; create conditions for the transmission of alarm and related information to prevent large-scale damage to property and human health.

- closed-circuit television (CCTV),
- alarm security and distress system (ASDS),
- electronic fire alarm (EFA),
- access control system (ACS).

A camera system is installed in the area monitoring the external and internal perimeter with recording equipment. The system consists of eighteen cameras with a technical specification, allowing good resolution with reduced visibility due to changing day and night times and adverse weather. Image recording is automatically stored in the recording equipment for inspection inan emergency event.

3.4. Regime measures

It lays down rules and principles for employees' movement and for other persons in specific areas, the entry of vehicles, the way of handling, rules for carrying out security controls, etc. or specifications to fulfil specific tasks. Entry and movement are only allowed for designated employees or escorts. The regime measures are implemented in the following areas:

- entry and movement of employees,

- entry of visits, external subjects and persons with free admission,
- special assess regimes (restricted access to specific buildings or premises),
- key modes,
- security systems (physical protection, construction and technical protection).

4. THREAT AND RISK ANALYSIS

The cause and effect diagram method used in six basic areas where specific threats were identified that could cause disruption to the airport's functionality. The six main areas include:

Tab. 2

Six main areas

Building	Attack	People
Areal	Technology	Systems

The assessment of areas has taken into account events involving external and internal influences that are directly related to the threat. Specific consequences are then defined in each area to decide the causes.

The semi-quantitative “PNH” point method was used to assess the risk sources. A simple point method made it possible to assess the risk according to the chance of a possible result.

- probability of occurrence (P),
- possible consequences of danger (PC),
- evaluator's opinion (EO),
- determining the degree of risk (D = P x PC x EO).

Individual levels of risk chance, the severity of consequences and assessor assessment defined in particular areas are based on the criteria set out above and through scoring between 1 and 5. Responsibility for risk management spread across the organisation. Naturally, the greatest responsibility lies with the owner, the statutory body and the company's top management. Usually, risk management is associated with the role of the Chief Financial Officer as the impacts of risk and countermeasures is expressed financially and has an impact on financial planning. In identifying risks, management must adopt proposed measures, including later changes in internal and external conditions. Given the possible economic demands of the measures taken, the creditworthiness aspects of clients to the financial market developments are considered. Risk management is also linked to monitoring compliance with established risk management practices as well as risk prevention.

Risk prevention aimed at increasing system resilience is determined by the system's ability to withstand threats while maintaining its functionality, which is presented by the entity's durability, persistence, and sustainability. An important need is also the ability to cut the severity or duration of a destructive event. The risks definition is based on the resilience concept, which is defined as reducing the risk to communities, increasing recovery capacity and ensuring essential services continuity and activities. In this perspective, we can speak of the need to give a broad base of infrastructure resilience. Ensuring the resilience of air transport elements represents an increase in critical infrastructure system ability, networks and activities to keep up the functionality and adaptation of changes caused by external agents, as well as rapid damage recovery.

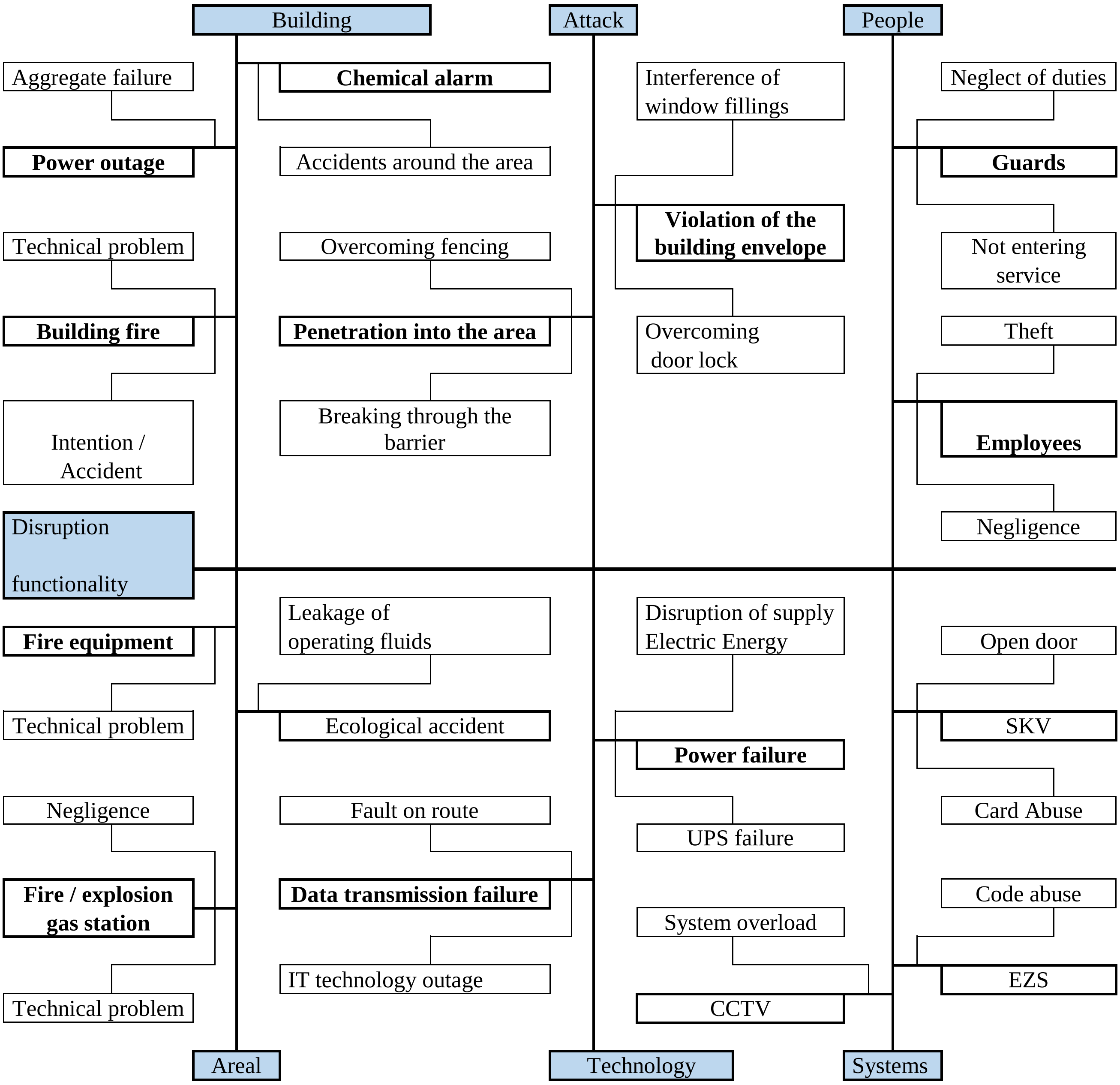

Fig. 2. Cause and effect diagram

Tab. 3

Degree and level of risk

Degree of risk	Value R	Level of risk
I.	>50	Unacceptable
II.	20 ÷ 50	Undesirable
III.	11 ÷ 20	Mild
IV.	3 ÷ 10	Acceptable
V.	< 3	Insignificant

Tab. 4

Risk assessment

Threat	Hazard identification	Risk assessment			
		P	PC	EO	D
Building					
Chemical alarm	Accidents around the area	4	3	4	48
Building fire	Intention	3	2	4	24
	Accident	1	3	4	12
	EPS technical fault	1	3	4	12
Power outage	Motor generator failure	3	3	4	36
Areal					
Gas station fire	Technical problem	3	2	4	24
	Negligence	1	3	4	12
Gas station explosion	Technical problem	1	3	4	12
	Negligence	3	2	4	24
Fire equipment	Technical problem	2	2	2	8
Ecological accident	Leakage of operating fluids	4	2	2	16
Technology					
Data transmission failure	Outage on route	1	3	3	9
	Fault on route	1	3	4	12
Power failure	Power supply interruption	2	3	2	12
	UPS failure	2	3	2	12
Systems					
CCTV	System overload	2	1	1	2
	Blind spot	3	5	3	45
EZS	Code abuse	1	1	1	1
SKV	Open door	3	4	3	36
	Card abuse	1	4	4	16
People					
Employees	Theft	3	1	1	3
	Negligence	2	3	2	12
Guards	Neglect of duties	4	3	4	48
	Not entering service	3	3	4	36
Attack					
Violation of the building envelope	Interference of window fillings	3	4	4	48
	Overcoming door lock	1	1	1	1
Penetration into the area	Overcoming fencing	4	3	3	36
	Breaking through the barrier	2	2	2	8

The evaluation of the performed PNH analysis shows that the existing level of protection of the building was solved comprehensively. None of the risk areas considered falls into the class of unacceptable. The undesirable and mild risks were treated by internal normative acts and corrective action rules, which in the event of a hazard, can cut impacts and keep up the desired level of functionality and make sure the airport is operational.

4. CONCLUSIONS

Proposed measures to increase protection of Brno-Tuřany International Airport reflects on the outputs from the analytical part. Based on each analysis of the degree of security protection, areas were identified in which it is possible to make changes so as to increase the current protection of the airport.

The proposed measures to increase the level of object security is aimed at:

4.1. Increase the number of guards

Increasing the number of guards due to the size and working nature of the airport complex will improve the distribution of tasks related to its security. In the unlikely event in the building or in its immediate vicinity, the security forces can be distributed without reducing the level of security in the premises. The economic costs of increasing security post are not inefficiently spent by the owner, given the role of the airport.

4.2. Extra fencing construction

It would be suitable to use modern 3D fencing suitable for industrial sites and military buildings. The 3D fencing system consists of each panel with horizontal 3D embodiments and fence posts with several attachments to form a compact unit with high resistance. Fence panels composed of horizontal and vertically folded wires with a diameter of 4 or 5 mm.

The advantage of 3D panels is the variability of design with overlapping vertical wires to create spines in the upper part. To increase the effectiveness of protection, it would be proper to use 3D fencing variant with the smallest end height of the panel 210 cm from the ground level, this does not need a building permit or notification, zoning permission or zoning permit.

4.3. Complementing CCTV

Complementing the CCTV system with an end element in the blind spot will increase the awareness of those guarding the premises to detect perimeter disruption and complete coverage of the premises by the CCTV system will be achieved. By increasing the CCTV terminal element, it will help to detect the breach in a timely manner, thus ensuring the required level of protection. Critical infrastructure protection is an essential element in ensuring human lives protection, health, and property of citizens, without which the vital needs of the population of the Czech Republic cannot be met.

This article analyses the issue of ensuring protection in the field of air transport with the aim to propose applicable solutions to increase international airport protection situation in the context of regional development.

The authors identified the elements of critical infrastructure and elements in the risk management system; the air terminal was described, making it possible to propose some measures for aviation critical infrastructure. Describing the processes of the airport security management system and follow-up analysis of ensuring airport security using the Ishikawa cause and effect diagram, the current level of object security of the airport complex was analysed. The analysis results made it possible to propose measures to increase the resilience of Tuřany International Airport.

References

1. Ishutkina A.M., R.J. Hansman. 2008. "Analysis of interaction between air transportation and economic activity". *8th AIAA Aviation Technology, Integration and Operations (ATIO) Conference*: 1-18. DOI: 10.2514/6.2008-8888. Available at: https://pdfs.semanticscholar.org/7537/e16087a7fa863e5afbf94e43411d94a36984.pdf.
2. Zákon č. 240/2000 Sb., ze dne 28. června 2000, o krizovém řízení a o změně některých zákonů (krizový zákon). [In Czech: Act No. 240/2000 Coll., Of 28 June 2000, on Crisis Management and on Amendments to Certain Acts (Crisis Act)].
3. Bröcker J., P. Rietveld. 2009. "Infrastructure and regional development". Capello R., P. Nijkamp (Eds.). *Handbook of Regional Growth and Development Theories*. Edward Elgar, Cheltenham, UK. P. 149-181.
4. Gherman L. 2017. "Defense architecture based on information age OODA loop". *Review of Air Force Academy "Henri Coandă"* 3. Braşov. ISSN: 1842-9238.
5. Korecki Z., et al. 2016. *Procesy a subjekty krizového řízení*. [In Czech: *Crisis management processes and subjects*]. Brno: Mendel University in Brno. ISBN: 978-80-7509-389-9.
6. Adámková B., M. Fukala. 2017. "Security consequences of development in Georgia in the year 19991-2015 with impact on economic development". *Security forum 2017 Conference Proceedings*: 6-19. Banská Bystrica, Slovakia, Interpolis. ISBN: 978-80-972673-2-2.
7. Commission of the European Communities. Green Paper on a European Program for Critical Infrastructure Protection. Available at: http://eurlex.europa.eu/LexUriServ/site/cs/com/2005/com2005_0576cs01.pdf.
8. Paulus F., A. Krömer, J. Petr, J. Černý. 2015. *Analýza hrozeb pro Českou republiku*. Praha: Hasičský záchranný sbor České republiky Generální ředitelství Hasičského záchranného sboru ČR. [In Czech: *Threat analysis for the Czech Republic*. Prague: Fire and Rescue Service of the Czech Republic General Directorate of the Fire and Rescue Service of the Czech Republic]. Available at: https://www.hzscr.cz/soubor/analyza-hrozeb-zaverecna-zprava-pdf.aspx.
9. Deloitte ČR. 2019. *Metodika zajištění ochrany kritické infrastruktury v oblasti výroby, přenosu a distribuce elektrické energie*. Praha: Ministerstvo vnitra České republiky. [In Czech: *Methodology for ensuring the protection of critical infrastructure in the field of production, transmission and distribution of electricity*. Prague: Ministry of the Interior of the Czech Republic]. Available at: https://www.mvcr.cz/cthh/clanek/ochrana-kriticke-infrastruktury-ochrana-kriticke-infrastruktury.aspx.
10. Čičmanec L., J. Nevrlý. 2012. "Capabilities and applications of fuzzy logic in airport operations". *ICMT'12 – International Conference on Military Technologies*: 382-386. Bratislava: Alexander Dubček University of Trenčín. ISBN: 978-80-8075-525-6.
11. Školník M., L. Belan. 2015. *Obranné plánovanie - Základy plánovania a projektovania v systéme obrany a bezpečnosti SR*. [In Czech: *Defense planning - Basics of planning and design in the system of defense and security of the Slovak Republic*]. GMRŠ Armed Forces Academy in Liptovský Mikuláš. University textbook. ISBN: 978-80-8040-522-9.
12. Benjamin H.S., L.M. Lahr. 1988. *Regional economic multipliers: definition, measurement, and application*.
13. Transport Infrastructure Development, Public Performance and Long-Run Economic Growth: A Case Study for the Eu-28 Countries. 2014. Available at: http://www.hrpub.org/download/20140105/AEB6-11802008.pdf.

14. Brizgalová L., Z. Vránová. 2016. "Economic security from point of view of raw material sufficiency and defence force". *Economics and Management* 1: 7-17. ISSN: 1802-3975.
15. Badenhorst-Weiss J.A., B.J. Waugh. 2015. "A logistics sector's perspective of factors and risks within the business environment that influence supply chains' effectiveness: An explorative mixed method study". *Journal of Transport and Supply Chain Management* 9(1) (a177). DOI: https://doi.org/10.4102/jtscm.v9i1.177.
16. Kraftová I., M. Maštálka, Z. Matějka, O. Svobora, P. Zdražil. 2016. *Bezpečný rozvoj regionu: základní koncept*. [In Czech: *Safe development of the region: basic concept*]. Praha: Wolters Kluwer. ISBN: 978-80-7552-261-0.
17. Procházková D. 2008. *Kritická infrastruktura a její problémy*. [In Czech: *Critical infrastructure and its problems*]. Ostrava: VŠB, SPBI. ISBN: 978-80-7385-034-0.
18. Ishikawa diagram – 8M. Available at: https://zsf.cz/show/ishikawa-diagram-rybi-kosti-8m.
19. Koudelka C., V. Vrána. 2006. *Rizika a jejich analýza*. [In Czech: *Risks and their analysis*]. VŠB TU Ostrava: Faculty of Electrical Engineering and Computer Science. Available at: http://fei1.vsb.cz/kat420/vyuka/Magisterske%20nav/prednasky/web/RIZIKA.pdf.
20. Dukiewicz T. 2014. „Security and information in the military environment". *Security Forum* I: 97-109. Jaroslav Ušiak, Jana Lasicová, Dávid Kollár (Eds.). ISBN 978-80-557-0677-1.
21. South-Moravian region. Portal of the South Moravian Region. South-Moravian region.
22. ČSN P 73 4450-1. *F*yzická ochrana prvku kritické infrastruktury - Část 1: Obecné požadavky. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. 2013. [In Czech: ČSN P 73 4450-1. Physical protection of a critical infrastructure element - Part 1: General requirements Prague: Office for Technical Standardization, Metrology and State Testing. 2013].
23. Kozuba J., M. Kelemen, V. Polishchuk, B. Gavurová, St. Szabo, R. Rozenberg, M. Gera, J. Hospodka, R. Andoga, A. Divoková, P. Bliš'an. 2019. "Fuzzy model for quantitative assessment of environmental start-up projects in air transport". *Int. J. Environ. Res. Public Health* 16(3572). ISSN: 1660-4601. DOI: 10.3390/ijerph16193573.

Received 28.02.2020; accepted in revised form 29.05.2020