JOURNAL OF SECURITY AND SUSTAINABILITY ISSUES
ISSN 2029-7017 print/ISSN 2029-7025 online
2019 December Volume 9 Number 2
http://doi.org/10.9770/jssi.2019.9.2(11)

THE PHYSICAL SECURITY OF BUILDINGS OF PUBLIC UNIVERSITIES

Radomír Ščurek[1], Věra Holubová[2]

[1]WSB University, Cieplaka 1c, 41-300 Dąbrowa Górnicza, Poland
[2]VŠB – Technical University of Ostrava, Faculty of Safety Engineering, Lumírova 630/13;
700 30 Ostrava – Výškovice; Czech Republic

E-mails: [1]radomir.scurek@gmail.com; [2]vera.holubova@vsb.cz

Received 18 February 2019; accepted 26 September 2019; published 30 December 2019

Abstract. The issues of terrorism, protection against crime, anti-social behaviour, and sociopathological phenomena are current topics in today's world. At present, there is no effective assessment in the Czech Republic of the physical security of buildings which could be the target of the threats. Within the security research of the Czech Republic, research was carried out whose main objective was to assess the existing level of physical security of public universities, with the subsequent determination of the minimum level of physical security of these buildings using new processes, practices, and technologies. In the Czech Republic, such research has not yet been realized. The main objective of the research was to thoroughly assess the current level of physical security of buildings at a representative sample of public universities, to create a security standard ensuring the minimum level of physical security of public universities against threats of terrorism, crime, anti-social behaviour, and also sociopathological phenomena. The contribution to the field of physical security in science is a rigorous assessment of the level of physical security measures of public universities, the analysis of criminal acts, security incidents, emergencies, risk designation, and the design of security measures. The benefit for practice is the creation of a security standard to ensure the minimum level of security of public buildings by physical security measures.

Keywords: physical security, public university, terrorism, crime, security standard, minimum level of physical security

Reference to this paper should be made as follows: Ščurek, R., Věra Holubová, V., 2019. The physical security of buildings of public universities, *Journal of Security and Sustainability Issues* 9(2): 505–516. http://doi.org/10.9770/jssi.2019.9.2(11)

JEL Classifications: O18

Additional disciplines: National Security; Economic Nationalism; National Security and War

1. Introduction

The subject of the research was the examination of the physical security issues of public universities as a whole. Physical security is a system of measures designed to prevent or hinder unauthorised access to a protected building, or to record his or her access or attempted access thereof (Reitšpís 2004). Schools and school facilities in the Czech Republic are called so-called soft targets. A soft target is a place with a high concentration of people and a low level of security against violent attacks, which are selected as a target for this type of attack due to the nature of the facility. The term attack is understood to mean terrorist, extremist, violent, arson, etc. (Fennelly 2004). The consequences of such attacks often affect a wider area, or require co-ordination when setting countermeasures. For the state, there is also a significant fact that soft targets are in great number. This greatly limits the practical possibilities of their security only on the part of the state or the public administration, and increases the importance of the security measures adopted by the soft targets themselves (Hofreiter 2015). The issue of physical security of public universities in the Czech Republic has not been given adequate attention for the long term. The research project focused on the area of security, with emphasis on the fight against terrorism, extremism, protection against crime, and sociopathological phenomena in connection with the situation in national and international security in order to enhance the safety of persons on the premises of public universities in the Czech Republic. Physical security as a security area is primarily aimed at protecting individuals, property, and information by implementing physical security measures against threats that are usually the result of an infringement (Fay 1993; Sitdikova., Starodumova 2019). The issue of physical security is, in Czech legislation, of fragmented design, and only generally, as a result of which the physical security measures are applied differently, and not always in the desired range, which is reflected in the level of security measures to ensure the physical security of public universities. The overall level of physical security is not sufficient, and can have a negative impact on emergencies and security incidents (Konečný, M. 2015).

2. Theoretical background

Within the Czech Republic, there are no comprehensive statistics of criminal acts, security incidents, and emergencies in public universities. Responsible representatives of individual public universities devote different attention to physical security issues, resulting in the level of protection achieved for each facility being at a different level. Often, individual levels of physical security are attained by responding to evolving security incidents, and not by the state of their system management. One of the causes of the described situation is the financial situation of public universities. Specific security designs are currently very often influenced by entities which carry out physical security as a business activity (Piwowarski 2012; Fabus et al. 2019). An employee responsible for physical security in a public university cannot rely on a professional opinion that would make it easier for him/her to make decisions in the physical security process. At the same time, a properly chosen and realized level of physical security contributes to the formation of the security consciousness of the entire population that passes through the education system. This security consciousness is part of the corporate responsibility of our own activities, which are reflected in the activities of businesses, organizations, and state and self-governing institutions. Another major issue that is not addressed by this article, but needs to be mentioned, is the unsatisfactory professional level of those responsible for physical security in public universities. The issue of physical security is analyzed by Coole, and emphasizes the expert security system established to diagnose a security issue in the physical security education process (Coole et. al. 2017, Coole et. al. 2012). National research has not yet addressed the issue of protecting the buildings of public universities. International research only focuses on the application of appropriate security technologies in the field of prevention of terrorism and other forms of unlawful conduct on the premises in the general sense, in which there are large numbers of people, with an emphasis on minimizing illegal entry and movement of persons in these buildings. Ensuring the physical security of public universities is a complex of technical and organizational measures aimed at minimizing risks to ensuring the safety of persons, and avoiding unauthorized manipulation of property by implementing appropriate safeguards (Fay 1993). Physical security of public universities must be treated in the same way as the physical security of any other public institution, however, taking into account certain specific conditions of the public university environment (Girdzijauskaite et al., 2019). Ensuring the physical security of public universities must respect the specific environmental conditions, as e.g. respecting academic freedoms and rights, organizing public events, concentration of residence and movement of persons at a certain time and period (day, academic year), variety of equipment and effects in multiple buildings, large areas or separate buildings situated between other purpose buildings, working in buildings not predisposed to college education, limited operating costs (Reitšpís 2004).

3. Research objective and methodology

The main objective of the research plan was to design a system of physical security for public universities. First, it was necessary to analyze the current level of physical security, to identify threats, risks, and to deal with the typology of potential offenders at the premises of public universities. In the next step, selected analytical methods were applied to assess security risks and threats in public universities. A suitable method for analyzing and managing safety incidents was then recommended to minimize the occurrence of a security incident and its impact on protected assets. The final step was to establish appropriate physical security measures in public universities in the form of a safety standard that would be applied in practice. The sequence of the individual steps of the research solution is illustrated in Figure 1.

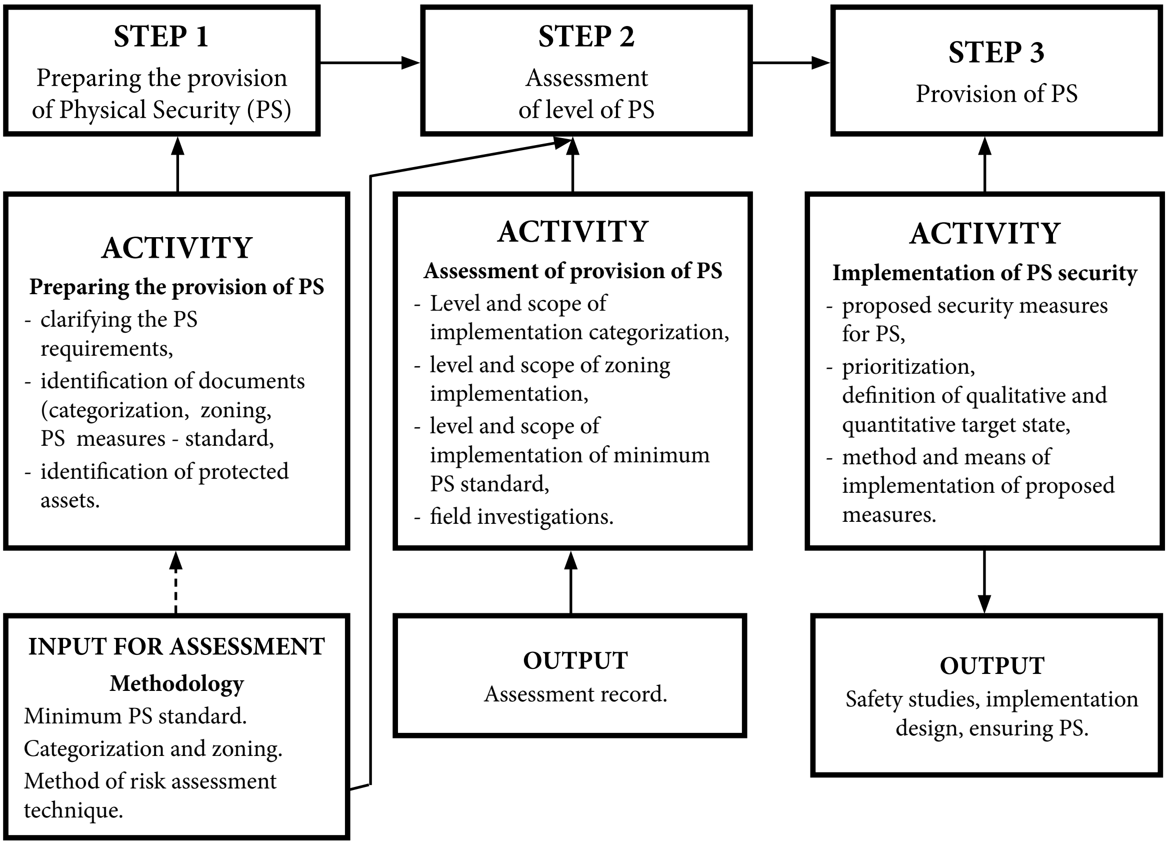
STEP 1
Preparing the provision of Physical Security (PS)
STEP 2
Assessment of level of PS
STEP 3
Provision of PS
ACTIVITY
Preparing the provision of PS
- clarifying the PS requirements,
- identification of documents (categorization, zoning, PS measures - standard,
- identification of protected assets.
ACTIVITY
Assessment of provision of PS
- Level and scope of implementation categorization,
- level and scope of zoning implementation,
- level and scope of implementation of minimum PS standard,
- field investigations.
ACTIVITY
Implementation of PS security
- proposed security measures for PS,
- prioritization, definition of qualitative and quantitative target state,
- method and means of implementation of proposed measures.
INPUT FOR ASSESSMENT
Methodology
Minimum PS standard.
Categorization and zoning.
Method of risk assessment technique.
OUTPUT
Assessment record.
OUTPUT
Safety studies, implementation design, ensuring PS.

Fig. 1. Sequence of research solution steps

Source: authors

3.1 Assessment of the status and level of physical security

The physical security system represents a conceptual system approach that defines effective physical security measures, including procedures and methods for the effective management of security risks in the university environment (Felson et. al. 1998). Implementation of a properly set up system will improve and unify the method of ensuring adequate physical security for persons and property, including the establishment of appropriate physical security measures. Universities in the Czech Republic under the Higher Education Act are divided into public, state, and private colleges and universities. In the Czech Republic, there are currently 26 public universities, 44 private universities, and 2 state universities. Funding of a public university is predominantly provided by subsidies from the state budget. The funding of a private university is predominantly provided by the own resources of the founder of the school, and the state universities do not have legal personality, and are the organizational components of the state with limited university autonomy. The basic prerequisite for solving the research intention was to obtain objective information about the state and level of physical security in a large population, so the research had to focus on the category of public universities. The public university as a system in itself was divided into smaller units, and the lower organizational wholes are faculties. Of the total number of 163 faculties of public universities, a representative sample was selected, which was the subject of the research. It was based on the assumption that individual faculties have common and comparable elements of physical security, despite their specific field differences. A representative sample of universities was determined by the relationship:

$$n = \frac{z^2 . N . r(1-r)}{(d^2 . N) + (z^2 . r\ (1-r))} \tag{1}$$

z the required degree of audit reliability (confidence coefficient 1.96)
N the size of the basic set (163 faculties)
d deviation tolerance rate (5% - 0.05)
r expected deviation rate (qualified estimate of 0.02).

By calculation, twenty-five faculties were found to be the minimum size of the representative sample. The criteria for selecting a representative sample of faculties were the number of students and academic staff, the extent, and method of ensuring physical security. The extent and method of ensuring the physical security of selected public universities was mapped out by field investigations, and evaluated as indicators in percentage terms. Table 1 lists the current level of physical security measures for the buildings under investigation. Attention was also paid to the issue of illumination of objects, with interesting information on the subject published by Deryol, and with the emphasis on crime prevention in the field of research on the effect of outdoor lighting and its impact on illegal behaviour (Deryol et al., 2017). The data in Table 1 is partially reduced due to the large amount of information, and was supplemented by statistical data from publicly available sources, especially from sources published by the Police of the Czech Republic (Konečný 2015).

Tab. 1. The existing level of physical security of selected public universities

Characteristics of the environment and buildings of public universities			**%**
Dislocation of a building in urban civil engineering			75
Building surroundings are freely accessible without boundaries			94
Easily accessible window construction holes			73
Main entrance from the building without barriers or other measures			75
Technical measures for physical security			**%**
Building entrances others	Mechanical barrier systems		90
	Camera systems		17
	Technical entry control systems		25
	Alarm intrusion and emergency system		31
Building entrance main	Mechanical barrier systems		98
	Camera systems		65
	Technical entry control systems		19
	Intrusion and emergency alarm system		31
	Infrared heater		2
Outer shell of building	VSS		67
	Security locks		10
	Safety grilles		35
Building surroundings	Camera system		62
	Fence	yes	87
	Fence	no	14
	Security lighting		100
Systems for technical protection in the interior areas			**%**
Entrance hall			73
Corridors (main routes)			77
Doors			52
Faculty management			69
Lecture halls			37
Classrooms			58
Offices			39
Guards			**%**
Professional physical security			30
Reception - guards			70

Source: Konečný 2015

3.2 Determination of the significance of protected assets

Identifying protected assets is an important step in designing adequate physical security measures in a university environment. The primary purpose of identifying assets is to determine the subject of protection. Individual assets must be broken down into categories according to predefined criteria, as shown in Table 2. Subsequently, the assets are assigned values, then they are compared, and the critical assets are selected from the point of view of physical security.

Tab. 2 Identifying tangible and intangible assets

Tangible asset	**Criterion of financial value**			**Criterion of replaceability**			**Criterion of misuse/abuse**	
	Low value €	Medium value €	Medium value €	Easily replaceable (within 1 month)	Hard to replace (max 1 year)	Cannot be replaced	Threats to life and health	Commission of a crime
1								
2								
Intangible asset	**Criterion of financial value**			**Criterion of replaceability**			**Criterion of misuse/abuse**	
	Low value €	Medium value €	Medium value €	Easily replaceable (within 1 month)	Hard to replace (max 1 year)	Cannot be replaced	Threats to life and health	Commission of a crime
1								
2								

Source: Konečný 2015

3.3 Risk assessment and minimization process

The process of risk assessment in a public university environment is crucial to meeting the main goal of the research plan. Risk identification and modelling have been carried out with a view to the process and structural approach and the determination of the acceptability limit with regard to the interdependence of individual risks. The risk assessment was carried out with respect to the priorities and purpose, based on the selected relevant data obtained through the field survey, including the typology of potential offender. The evaluation was compared in terms of acceptability. Risk assessments included characteristic implications, including synergy and the domino effect. The results were compared with several risk analysis methods. In assessing the physical security of public universities, the path of identifying the chain of danger - threats - damage - harm, the illegal activity was taken into account. On the basis of the analyses carried out, it was proposed to minimize them at an acceptable level for selected risks. The process of risk management in a public university environment is illustrated in Figure 2.

Identification of a source of risk risk search, recognition, description
Method selection Ishikawa, ETA, FTA, FMEA, CARVER
Risk assessment determining the level of risk: acceptable – unacceptable
Defining aims realistic, measurable, planned
Barriers preventing success primary, secondary, tertiary
Regulation of risks decision making, realization, monitoring

Fig. 2. Risk management process in public universities;

Source: authors

The risk management process is based on the systematic identification of sources and potential failures that could have a negative impact on the protected interest of a public university. The primary prerequisite for effective risk assessment is the choice of the appropriate method (Broder 2006). In the process of risk assessment in public universities, methods of observation and inductive thinking and techniques based on the description and comparison of evidence and verification of statistical data were used. Using the comparison, the outputs of the individual analyses were used for tertiary risk assessment. The resulting set of undesirable risks was subjected to a qualitative assessment. As part of this process, a panel discussion was carried out by investigators and practitioners over the evaluation of identified security risks, along with the proposal for physical security measures for public universities. The process of risk assessment in public universities was divided into three phases, as shown in Table 3.

Tab. 3 The process of risk assessment in public university environments

Phase 1 **Data collection**	**Phase 2** **Identification of risks and threats**	**Phase 3** **Clarification of results and verification**
Brainstorming, Check list, Delf method • Selection of the building under consideration. • Obtaining theoretical and practical starting points. • Data collection and processing. • Determining the appropriate risk analysis method.	**Ishikaw diagram, ETA, FTA, FMEA** • Consultation with experts from the area of physical security. • Application of selected methods of risk analysis. • Identification and assessment of significant risks in the environmentto public universities from procedural and structural points of view.	**FMEA + CARVER, Paret's principle, Lorentz curve, KARS method** • Clarification and verification of outputs of primary FMEA analysis. • Using Paret's principle with the Lorenz curve. • Correlation method.

Source: authors

The risk assessment process identified potential threats to the physical security of public universities. The threats have been assessed from a procedural point of view, the cause of which is human, and from structural, the cause of which is a system or technical error. The most significant risks are unauthorized access to the building, dangerous materials being brought into the building, explosive alarm system, insufficient area security or free space access, physical security failures, key mode failures, and asset theft. Assessing the state and the level of physical security of public universities has found that the state and level of physical security is insufficient, inefficient, and the security technology used does not meet the current security requirements. Serious findings have included the fact that public universities underestimate the importance of professional physical security.

3.4 Systematic method of analysis and management of security incidents

An innovative analytical method designed to assess and address an unexpected security incident from a physical security point of view was proposed. The aim of the method is to identify the root cause of the problem, and to establish corrective and preventive measures to minimize their recurrence. The method, with its repressive and preventive nature, is suitable for undesirable situations that need to be addressed quickly and efficiently. It represents a structured and documented process for the solution of the incident which, when properly implemented, helps solve the problem in a timely and complete manner (Garcia 2001). Determination of appropriate measures and their planning is based on data leading to the removal of the true causes of the problem itself, and not just its consequences. The principle of the method of managing security incidents lies in the systematic solution of the problem using a standardized form, consisting of eight consecutive phases, as shown in Table 4. This procedure defines the practical solution and application of the method of analysis and management of security incidents in the university environment. The primary objective is to minimize the recurrence of the adverse event, including the negative impact on the protected assets of the university. The condition is that a team of responsible and interested persons with the necessary expertise will be involved in the process, and will correctly identify the root cause of the problem and establish appropriate corrective and preventive measures. Thereby, the university gains a simple tool to manage incidents or emergencies that pose a significant risk to universities from a physical security point of view (Mach et al. 2013).

Tab. 4 Process of systematic analysis and management of security incidents

F0	**Initial phase**	- determination by the team - preparation and planning - initiate an inquiry according to a systematic form
F1	**Defining the problem**	- unambiguous definition of the problem - 5W/2H application
F2	**Comparison of risk of a similar nature**	- assess the risk of the occurrence of a similar problem in other university areas
F3	**Necessary corrective action**	- implementation of the necessary measures within 24 hours, in exceptional cases within 48 hours
F4 **F5**	**NO/OK analysis**	- finding the root cause of the problem - determine detection and occurrence factor + validation
F6	**Effective corrective and preventive measures**	- implementing the measures - the economic aspect and the expected efficiency
F7	**Efficiency monitoring set measures**	- monitoring detected factors and occurrence factors - monitoring from the onset of incidents
F8	**Evaluation of acquired data**	- lessons and experience from incident investigation - risk elimination declaration - distribution of outputs

Source: authors

3.5 Categorization through security zoning

The proposal for the categorization of individual buildings and premises is a prerequisite for setting appropriate physical security measures. In the specific environment of a university, security zoning involves preventive measures to minimize identified risks, and to determine the vulnerability of defined buildings or spaces. Such buildings and premises may remain accessible, however, while adhering to specified security measures that may be specific to individual groups of people, part of the day, or even period of the academic year. This is a regime measure that has a direct effect on the movement of persons in the security zone, which consists of defined technical measures or clearly defined boundaries. The principle of security zoning in the profiled conditions of universities is based on the division of individual areas into security zones (Ščurek et. al. 2014). The relationship between the asset categories and security zones in the university environment and the principle of the application are shown in Table 5.

Tab. 5 Relationship between asset categories and security zones

Asset category	**Security zone**	
I. Buildings and areas of considerable importance	**Non-public zone** area protected by increased security levels	**Secured zone** area with the highest level of security measures
II. Buildings and areas of usual importance		**Protected zone** area with medium-level security measures
III. Buildings and areas of low importance		**Controlled zone** area with a lower level of security measures
IV. Buildings and areas of special importance	**Public zone:** area protected by basic security levels	

Source: authors

3.6 Multi-criteria analysis of the choice of appropriate security technology

For practical implementation, it is necessary to determine which technology is best suited to the task at hand. The goal is to make a decision on which option is best, on the basis of the given criteria. The solution is to use multi-criteria analysis. Multi-criteria decision making is a marketing tool for mathematically calculating the right marketing strategy based on predetermined criteria, and assigning weight to these criteria (Ploch et.

al. 2016). The issue of ensuring an adequate level of physical security for public universities is specific and quite extensive. Because of the potential threats and risks in a public university environment, it is necessary to choose appropriate modern security technology, in particular Radio Frequency Identification (RFID) and biometric systems. In particular, RFID technology, as stated by Quan Qian, is also usable for building tracking and monitoring (Quan Qian et. al. 2016). For the correct assessment of the appropriate technology, a multi-criteria analysis was performed, the output of which is shown in Table 6.

Tab. 6 Multi-criteria matrix

				Assessed technologies				
Assessed values				**A**	**B**	**C**	**D**	**E**
Criteria K_i	**Unit**	**K_i**	**Weight V_i**	**Comparative criteria K_{ti}**				
K_1 Acquisition and operating costs	€	10	0167,	0,4	0,8	0,3	0,9	0,9
K_2 Difficulty of realization		8	0,133	0,5	0,6	0,4	0,9	0,8
K_3 Spectrum of application		7	0,117	0,3	0,9	0,2	0,6	0,2
K_4 Reliability of detection	%	9	0,150	0,2	0,1	0,4	0,3	0,3
K_5 Detection speed - passage	person/hour	10	0,167	0,4	0,6	0,2	0,4	0,3
K_6 Difficulty of evaluating data		6	0,100	0,3	0,5	0,3	0,4	0,4
K_7 Influence of human factor		5	0,083	0,4	0,1	0,4	0,6	0,7
K_8 Service, service life, maintenance		5	0,083	0,4	0,4	0,3	0,7	0,4
Total		**60**	**1**	**0,4**	**0,5**	**0,3**	**0,6**	**0,5**

Source: authors

This is a decision matrix with predefined criteria that, based on brainstorming, had been assigned the weight and degree of compliance with a given security technology. Criteria for the decision matrix were determined on the basis of empirical experience of security systems procurement in the physical security of public universities. Five technologies were assessed: A – biometric: fingerprint, B - biometric: eye scan, C - RFID: passive, D – RFID: active, E - video surveillance systems. Criterion K_i was marked as K_{1-8} and they were assigned to corresponding units. The criteria are rated by a score of 1 to 10, which indicates the relevance of each individual criterion. The first one represents the smallest value. According to the formula, the criterion weight was determined.

$$v_i = K_i / \sum K_i \tag{2}$$

For each technology, their compliance with the criteria was expressed. A zero value means that the technology meets the criteria without reservations, and the value one means that the technology does not meet the criteria. A suitable variant is determined by the relationship where the lower the value for V_i, the higher the consistency and potential of the effective implementation of the security technology (Konečný et. al. 2014).

$$K_i = \sum^{i=8} K_{ti} \cdot v_i \tag{3}$$

Through multi-criteria analysis, it was found that, given the cost, use spectrum, implementation difficulty, reliability, and speed of detection, the key criteria are $K_1, K_{4,} K_{5.}$ Criteria K_2, K_3 are also considered. A suitable security technology in a university environment is passive RFID and fingerprint biometrics. Video surveillance systems hold an irreplaceable position in security technology for the examined environment. Mutual integration of these security features is a prerequisite for ensuring an adequate level of security for persons and property against terrorism and other forms of illegal activity.

3.7 Effectiveness of the system for the protection of persons and property

In the next part of the research, it was necessary to deal with the issue of effectiveness of security systems for the protection of persons and property. In general, efficiency is defined as a measure of the positive deviation of the goal achieved from the desired goal or as a measure of success. An effective system of protection of persons and property requires a system that fulfils the basic condition that the time of attack T_N, or respectively the total time of breaking internal and external protection elements T_{PRL} is greater than the response time of the intervention unit T_{FO}. This means $T_N > T_{FO,}$ or respectively $T_{PRL} > T_{FO}$ (Korzeniowski 2008). Fulfilment of this condition may not always be sufficient, but the declaration of the safety system as effective is a necessary condition. An important parameter that describes the efficiency of a given system is the coefficient When this coefficient is is lower than one, then the effectiveness of safeguards is inadequate and the whole security system is ineffective. When the coefficient is greater than one, then the effectiveness of the security measures, and therefore the whole security system, is greater. If the intruder is detected by the active protection elements, then the coefficient is defined by the relationship (Loveček et. al. 2011):

$$Q_{ochr} = \frac{T_N}{T_{FO}} = \frac{T_P + T_{PRES} + T_{\acute{u}t} + T_{\acute{u}n}}{T_{pop} + T_{ver} + T_{pres} + T_{z\acute{a}s}} \text{ for } T_N > T_{FO} \tag{4}$$

$$Q_{ochr} = \frac{T_{PRL}}{T_{FO}} = \frac{T_P + T_{PRES}}{T_{pop} + T_{ver} + T_{pres} + T_{z\acute{a}s}} \text{ for } T_{PRL} > T_{FO} \tag{5}$$

If the intruder is detected by physical security, then Q_{ochr} is defined by the relationship:

$$Q_{ochr} = \frac{T_N}{T_{FO}} = \frac{T_P + T_{PRES} + T_{\acute{u}t} + T_{\acute{u}n}}{T_{HL} + + T_{pres} + T_{z\acute{a}s}} \text{ for } T_N > T_{FO} \tag{6}$$

$$Q_{ochr} = \frac{T_{PRL}}{T_{FO}} = \frac{T_P + T_{PRES}}{T_{HL} + T_{pres} + T_{z\acute{a}s}} \text{ for } T_{PRL} > T_{FO} \tag{7}$$

Q_{ochr} coefficient of effectiveness of protective measures, T_N total time of invasion by the intruder from the time of detection by the active elements of the protection until his leaving the guarded area, T_{PRL} total time to break through passive protection elements, T_{FO} total response time of the intervention unit, T_P time to break through all passive protection features, T_{pres} the total time required for the intruder to move to the protected interest until the moment of detection by the active elements of protection in time, $T_{\acute{u}t}$ time of intruder attack, $T_{\acute{u}n}$ time of intruder escape, T_{pop} time of alarm, T_{ver} time of attack verification, T_{pres} time of move to site, $T_{z\acute{a}s}$ time of intervention against the intruder, T_{HL} the interval between two physical security inspections or patrols.

Foreign literature, unlike coefficient Q_{ochr} shows the parameter characterizing the minimum delay time en route to the protected interest, which is defined by the relationship:

$$T_{MIN} = \sum_{i=1}^{n} \Delta t_i \tag{8}$$

Δt_i the delay time of the intruder in overcoming individual security measures of the security system, or overcoming the distance between individual zones.

The disadvantage of time T_{MIN} is that it does not even take into account the probability of intruder detection during his/her journey, or the time of the intervention unit. The problem of assessing the uncertainty of the security system is addressed by Szulim, who emphasizes efficiency coefficients in the application of mathematical models in five basic steps in relation to electronic security systems, using the Monte Carlo method (Szulim et. al. 2014). Another important parameter that relates to physical security, as a whole, is the probability of intruder detection P_1 . This parameter defines the probability that the intruder will be detected or eventually eliminated en route to a protected interest. This parameter, in contrast to the above, takes into account the probability of intrusion detection, the probability of a successful response of the physical security intervention unit, and the effect of stochastic phenomena. The probability *P* is based on the evaluation criterion of the physical security of the building's system, and that the total time of invasion T_N by the intruder from the moment of detection by the active protection elements until he/she leaves the guarded area or T_{PRL} the total break time of the passive protection elements must be greater than the reaction time Physical security intervention units T_{FO}. Tedy $T_N > T_{FO}$, respectively $T_{PRL} > T_{FO}$. The following conditions arise from the criteria shown:

$$T_N - T_{FO} > 0, \text{ respectively } T_{PRL} - T_{FO} > 0 \tag{9}$$

The likelihood of intruder detection is defined by the relationship:

$$P_1 = \frac{n!}{x!(n-x)!} p^x (1-p)^{n-x} \tag{10}$$

P_1 the probability of intrusion detection by a given detector, *n* number of detectors, *x x*-tý detection attempt, *p* probability that the intruder is not detected (Loveček et. al. 2011).

Results and discussion

This article focuses on the physical security of Czech public universities, with a focus on the protection of persons and property, especially against terrorism, various forms of crime, anti-social behaviour, and sociopathological phenomena. The prerequisite for launching security research was that the issue of protection of Czech public universities had not been given adequate attention. There is no comprehensive legal regulation or safety standard that regulates overall and conceptually this area of building protection. There is no recommendation to ensure a minimum level of physical security in the environment of Czech public universities. The overall level of physical security is inadequate, and can have a negative impact on the safety of persons and property in the event of emergencies and security incidents. Research data has been drawn from real practice, and the results of the research are implemented in practice.

Conclusions

The main objective of the research was to propose a system of physical security measures in Czech public universities which will ensure an adequate level of protection of persons and property against terrorism, other forms of crime, anti-social behaviour, and sociopathological phenomena. The main objective of the research was fulfilled by a thorough assessment of the existing level of ensuring the physical security of buildings at a representative sample of public universities, followed by the development of a security standard in the form of a certified methodology approved by the competent authorities of the Ministry of the Interior of the Czech Republic. Contribution to the practice is seen in the elaboration of a methodical procedure for designing the physical security of public universities, and putting them into practice. The methodology provides prerequisites for increasing the level of protection of persons and property in the environment of Czech public universities. The contribution of the research to the field of science is to obtain information about methods of ensuring the physical security of selected buildings of Czech public universities, an overview of criminal acts, security incidents, and extraordinary events in this environment. Such a range of information has not previously been gathered. A new analytical and systematic method has been developed in the field of risk prevention and repression to identify the root causes of the occurrence of undesirable events, and to establish immediate corrective and preventive measures. An innovative system of physical security for public universities has been designed. The prediction of further research in this area is directed towards exploration of possible models (pessimistic, realistic, pragmatic, and optimistic) in which the effectiveness of the system of protection of the buildings of Czech public universities is assessed. The article was prepared from the scientific outputs obtained within the Security Research Program of the Czech Republic, within the successfully defended project "Assessment and standardization of physical protection for public university buildings", on which the authors participated as co-investigators. The output of the project was a certified methodology for ensuring the physical protection of public universities in the Czech Republic.

References

Broder, J.F. 2006. *Risk Analysis and the Security Survey.* Elsevier, Amsterdam.

Coole, M. P., Brooks, D. J. & Minnaar, Secur, A. 2017. Educating the physical security professional: developing a science-based curriculum. *Security Journal*, 1-24. https://link.springer.com/article/10.1057/s41284-017-0114-1

Coole, M., Corkill, J., Woodward, A. 2012. *Defence in Depth, protection in Depth and Security in Depth: A Comparative Analysis towards a Common Usage Language*. In: Preceedings of the 5th Australian Security and Intelligence Conference, Perth.

Deryol, R., Payne, T. C. 2017. A method of identifying dark-time crime locations for street lighting purposes. *Crime Prevention & Community Safety,* 1-16. https://link.springer.com/article/10.1057/s41300-017-0035-2

Fabus, M., Dubrovina, N., Guryanova, L., Chernova, N., Zyma, O. 2019. Strengthening financial decentralization: driver or risk factor for sustainable socio-economic development of territories. *Entrepreneurship and Sustainability Issues,* 7(2), 875-890. http://doi.org/10.9770/jesi.2019.7.2(6)

Fay, J. 1993. *Encyklopedia of Security Management. Techniques and Technology*. Butterworth - Heinemann. Nextom, MA, USA.

Felson, M.; Clarke, R. V. 1998. *Opportunity Makes the Thief Practical theory for crime prevention*. PRC Unit, London.

Fennelly, L.J. 2004. *Effective Physical Security*. Elsevier, USA.

Garcia, M. L. 2001. *The Design and Evaluation of Physical Protection Systems*. Elsevier, USA.

Girdzijauskaite, E., Radzeviciene, A., Jakubavicius, A. 2019. Impact of international branch campus KPIs on the university competitiveness: FARE method. *Insights into Regional Development,* 1(2), 171-180. https://doi.org/10.9770/ird.2019.1.2(7)

Hofreiter, L.2015. *Manažment ochrany objektov.* [Building protection management]. Žilinská univerzita v Žiline - EDIS - vydavateľstvo Žilinskej univerzity.

Korzeniowski, L. F. 2008. *Securitologia. Nauka o bezpieczeństwie czlowieka i organizacji spolecznych*. [Securitology. The science of the safety of people and organizations]. EAS, Krakow.

Konečný, M. 2015. *Návrh fyzické bezpečnosti v prostředí vysokých škol.* [Design of physical security system for universities]. Disertační práce, VŠT-TU Ostrava.

Konečný, M., Stoniš, O., Maršálek, D., Ščurek, R. 2014. Exploring the impact on radio frequency signal of RFID technology related to physical protection of renewable resources, *Przeglad elektrotechniczny,* 90 (10), 188-191. https://doi.org/10.4028/www.scientific.net/amr.1001.149

Loveček, T., Reitšpís, J. 2011. *Projektovanie a hodnotenie systémov ochrany objektov*. [Design and evaluation of building protection systems]. Žilinská univerzita v Žiline - EDIS - vydavateľstvo Žilinskej univerzity.

Mach, V., Veľas, A. 2013. *Ujednotenie metodiky zisťovania prielomovej odolnosti mechanických zábranných prostriedkov obvodovej ochrany.* [Unification of methodology for determining the breakthrough resistance of mechanical protection devices for perimeter protection]. In: Krízový manažment: vedecko - odborný časopis Žilinská univerzita, Žilina, 12(2).

Piwowarski, J. 2012. *Trzy składowe kultury bezpieczeństwa*. [The three components of the security culture]. In: Kultura Bezpieczeństwa. Nauka - Praktyka - Refleksje. WSBPiA Apeiron, Kraków, 9, 3-8.

Ploch, J., Žihla, Z., 2016. Security and hidrance at airporst*. Journal of Security and Sustainability Issues*, 5(4), 481-488. http://dx.doi.org/10.9770/jssi.2016.5.4(3)

Reitšpís, J. 2004. *Manažérstvo bezpečnostných rizík.* [Security risk management]. Žilinská univerzita v Žiline - EDIS - vydavateľstvo Žilinskej univerzity.

Szulim, M., Ciosk, K., Kuchta, M.. Dukata, A. 2014. Niepewność oceny skuteczności systemu bezpieceństwa obiektu, [Uncertainty of measuring the effectiveness of the security system of buildings], *Przeglad elektrotechniczny,* 90(2), 182-185. http://dx.doi.org/10.12915/pe.2014.02.47

Ščurek, R., Maršálek, D., Konečný, M., Stoniš, O. 2014. System of management of uncertainty and risk renewable resources. Advanced Materials Research, 1001, 492-497. https://doi.org/10.4028/www.scientific.net/amr.1001.492

Sitdikova, L.B., Starodumova, S.J. 2019. Corporate agreement as a means of providing security in the course of entrepreneurship development. *Entrepreneurship and Sustainability Issues,* 7(1), 324-335. http://doi.org/10.9770/jesi.2019.7.1(24)

Quan Qian, Yan-Long Jia, Rui Zhang. 2016. A Lightweight RFID Security Protocol Based on Elliptic Curve Crypotography. International Journal of Network Security, 18(2), 354-361. https://doi.org/10.6633/IJNS.201603.18(2).17

Radomír ŠČUREK, Associate Professor, MEng, MSc, Ph.D.**,** specialises in the security of persons and property, protection of companies, current security threats, criminology, and national security of the state. Solver and co-solver of several security research projects, author of a number of articles and monographs on security issues**.**
https://orcid.org/0000-0002-2971-9313

Věra HOLUBOVÁ, Ing., Ph.D., specialises in security of persons and property, protection of buildings and internal security of the state. Founder and co-researcher on several security research projects, author of articles on security issues.
https://orcid.org/0000-0001-8198-3157