

https://doi.org/10.48009/1_iis_2021_75-83

Global phenomenon of threats and risk management in management and information technologies

Dagmar Kopencova, *Ambis. University, Czech Republic, Dagmar.Kopencova@ambis.cz*

Roman Rak, *Ambis. University, Czech Republic, Roman.Rak@ambis.cz*

Vladimira Hudecova, *Police Presidium of Slovak Republic, Vladimira.Hudecova2@gmail.com*

Abstract

In the global world today, management is always associated with the security of the controlled object, including information security management. Information security, like any other security, always needs a quality risk analysis for its effective long-term fulfillment. The basic attributes of any risk analysis are the determination of a certain acceptable balance between the assets (the values we protect) and the potential, negative impacts of the threats on the objects we protect. Various phenomena can occur in the world around us. These always arise when certain conditions that are specific to them are met. So the phenomenon is what can theoretically happen. An event is then a realized phenomenon, that is, what happens or has already happened. The threat can therefore be defined as a phenomenon with negative effects on the protected object. Damage then occurs to the building. In risk analysis, it is often not easy to identify all the theoretical negative phenomena (threats) that may occur. In order to appreciate the risks well, on the one hand we must know the protected objects well, on the other hand we have practical experience, good theoretical knowledge, a certain imagination, and last but not least, good ideas and knowledge about various threats. The paper considers the theoretical, general level and division and action of various threats and brings their basic categorization.

Keywords: Threat, Source of threat, Threat characteristics, Risk, Management

Introduction

One of the fundamental values of life is safety. We live in a time of contradictions, in a globalized world of dynamic change. These changes may be positive, neutral or negative for each subject. In the latter case, they have an impact in the form of damage or injury. To avoid damage, we control safety. Security management also includes risk analysis, where we primarily identify threats and then categorize them according to the severity of their impacts.

The aim of this paper is to define the basic categories of threats so that they serve in the security analysis of any object or subject in various life situations. Knowledge of the basic categories of threats then helps security analysts to systemically, comprehensively analyze and exclude this possibility.

Threat

Threat is a terrible proximity to something bad, i.e. a phenomenon, event or process whose manifestations, factors, intensity and consequences limit, threaten, destroy, devastate, and destroy lives, health, property, the environment, and cultural values; in general, a threat threatens various, diverse objects. A threat always acts at a specific time, place and affects specific objects and entities.

Threat is a primary phenomenon that exists independently of us and that may or wishes to damage a particular object value (Odlerova, 2017) or assets.

Threat is a phenomenon that may turn into a negative event and cause damage or harm an object or interest. Threat is therefore, a phenomenon that may damage a protected object or interest.

In other words, threat (danger) is a non-activated phenomenon that has not yet turned into a negative event. Damage (harm) caused by a threat during its one action affecting a particular asset is called **threat impact**. Impact is the adverse effect (action) of a threat (negative event) at a given location and time, affecting protected interests. Impact is usually expressed as damage (financially quantifiable) or harm (difficult to quantify financially).

Threat (security threat) may be a speech, gesture, measure or action that reflects one's ability or even intention to cause damage to someone. Threat is a sign or foretaste of such an action that causes concerns on the threatened object's part. Every threat may cause damage and thus makes the endangered fearful. **Threat is an objective character phenomenon** (Hajdukova, Kissova, 2019), unlike risk, which is always subjective since it is assessed by people who may perceive various risks differently.

Threat seriousness is proportional to the nature of the value and how much we value the value of every object. The term **danger** is the synonym of the term threat.

Example:

In the winter period, on wet roads, there is the threat of icing. Consequently, the drivers face the danger of skidding.

Threat categories

A threat may be a natural or purely technological phenomenon, defined physically, chemically, biologically, etc. - such a threat is always called **a non-intentional (unintentional) threat**. The realisation of a non-intentional threat is of a stochastic nature. An unintentional threat may be a human as well (he does not know that he is infected by an infectious disease).

Of a completely different origin is a threat caused or intended by person with his will, intention (**intentional threat; therefore, intended threat**) – it is intended, prepared, triggered or realised by an individual or group of individuals.

Examples include aggression, terrorist attacks, economic sanctions, disruption of transport of strategic raw materials and energy sources, national oppression), sabotage, threatening, blackmailing, criminal threats, etc.

We call the intentional or unintentional threats caused by humans **anthropogenic threats**.

We also divide threats into **internal threats** and **external threats** from the perspective of the direction of their acting on the object (from the inside, from the outside). *Internal threats to the company may include disloyal employees, sharing know-how with the competition, and external threats may include thieves, threatening a safe with cash.*

Origin-wise, threats may be generally divided into these threats (Janicek, 2017), (Kopencova, Felcan & Rak, 2019):

Anthropogenic – caused by humans, their existence, activities, etc. This area also includes threats of the technological, social (societal) or economic character, as they are ultimately the result of human activities, people, and their various grouping forms.

Non-anthropogenic or **naturogenic** – not caused by humans, but by nature itself. Non-anthropogenic threats are further divided into **biotic threats** (caused by living organisms) and **abiotic threats**, caused by inanimate natural phenomena, events (drought, floods, flooding, torrential rains, tsunamis, earthquakes, volcano eruptions, etc.).

In terms of their action directness, threats may be divided into **direct threats** and **indirect threats (distant)**. If two objects interact directly, one object threatens the other, we find this case a direct threat. If there is some “mediator” transferring a threat during its action, then it is an indirect threat.

We speak of direct threats when our state is exposed to them, while indirect threats concern our allies or the regional or even global stability (Vlach, 2018).

Direct threats are those that imminently, directly threaten an asset (life, health, property - movable, real, intellectual). **Indirect threats** initially do not concern our security interests; however, they eventually may. Indirect threats may arise in response to our security measures, etc.

Depending on how easily threats may be identified over time, we may divide threats into **obvious threats** and **hidden threats**.

Obvious Threats. As a rule, this kind of threat may be identified simply or even with a greater effort, based on available information, knowledge, and practical experiences with their actual occurrence in the past.

Hidden Threats. We do not have available information, theoretical knowledge, or practical experiences to actually identify hidden threats (Hajdukova, Kissova, 2019). In other words - the knowledge of science, technology, social processes, etc. is not sufficient to identify this kind of threat. Hidden threats are usually encountered in activities that we have not yet performed as humanity, various organisational or social groups of people or individuals and have no experience with them (new technologies, medical treatments, processes, SW, artificial intelligence, etc.), and; therefore, we could not have tested them in any real environment.

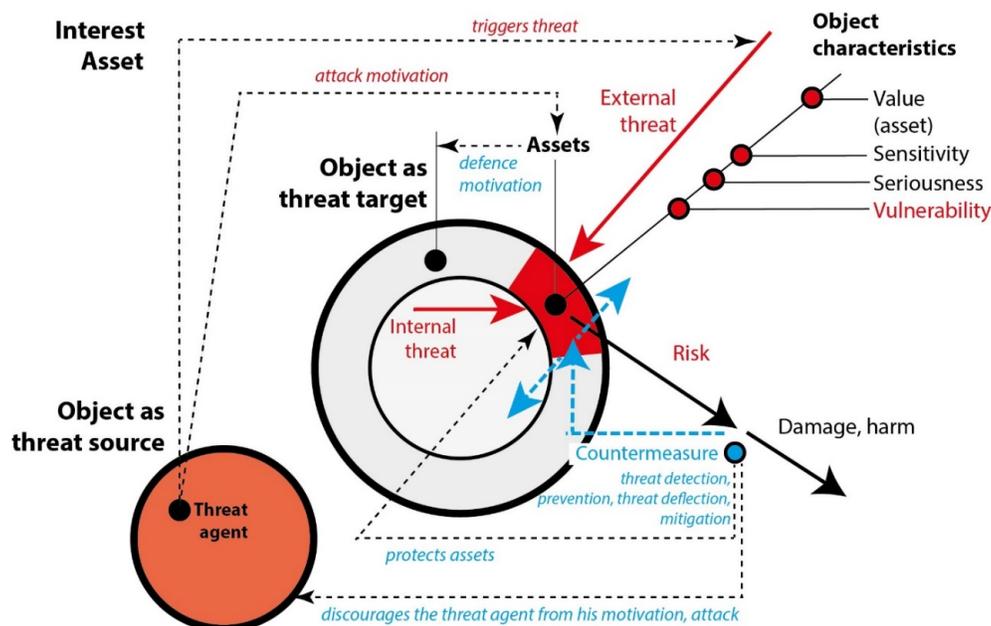


Figure 1. Threat and related terms. Demonstration of the mechanism of threat acting between the source and target objects

Hidden threats may also be encountered in the case of intentional threats, where the threat agent (originator, initiator) is so-called **hidden, ideological agent**. This threat agent carefully hides and conceals his interests and activities, which may be completely unexpected, unpredictable. In terms of criminalistics, we may speak, for example, of an offender who prepares a large-scale crime and purposefully conceals even his traces of preparation, so no one knows even the hints of the future threat's nature.

In terms of the threat handling speed, we may divide threats (dangers) into **acute (urgent)** and **chronic**. **Acute threat** is a threat requiring immediate response, as it may be triggered in a very short period of time (neighbouring house fire and the threat of fire propagation to any adjacent houses).

Chronic threats are threats we live with for a very long time, we are aware of them, and their activation is unclear in time, nothing has happened for a long time. We do not have to respond to them immediately since there is no immediate danger, but are aware of them, and based on the analysis of risks arising from the threat nature and their agents, we prepare corresponding measures that are usually focused on ensuring increased resistance of protected objects (e.g. design requirements for facilities capable of resisting to some degree of seismic activities in geologically unstable areas).

Symmetrical Threats (“Conventional”). A typical example is the classic war of two states that threaten each other with identical symmetrical threats. **Asymmetrical threats** (“unconventional”, “imbalanced”) are typical especially in modern conflicts, when one party uses unusual, non-standard threats, means that are often outside any regular norms, relations, international conventions etc. Asymmetrical threats include, for example, terrorist attacks.

Individual threats only threaten individual, specific objects, at a specific location and at a specific time. **Global threats** such as those that threaten humanity in general, everywhere, and constantly.

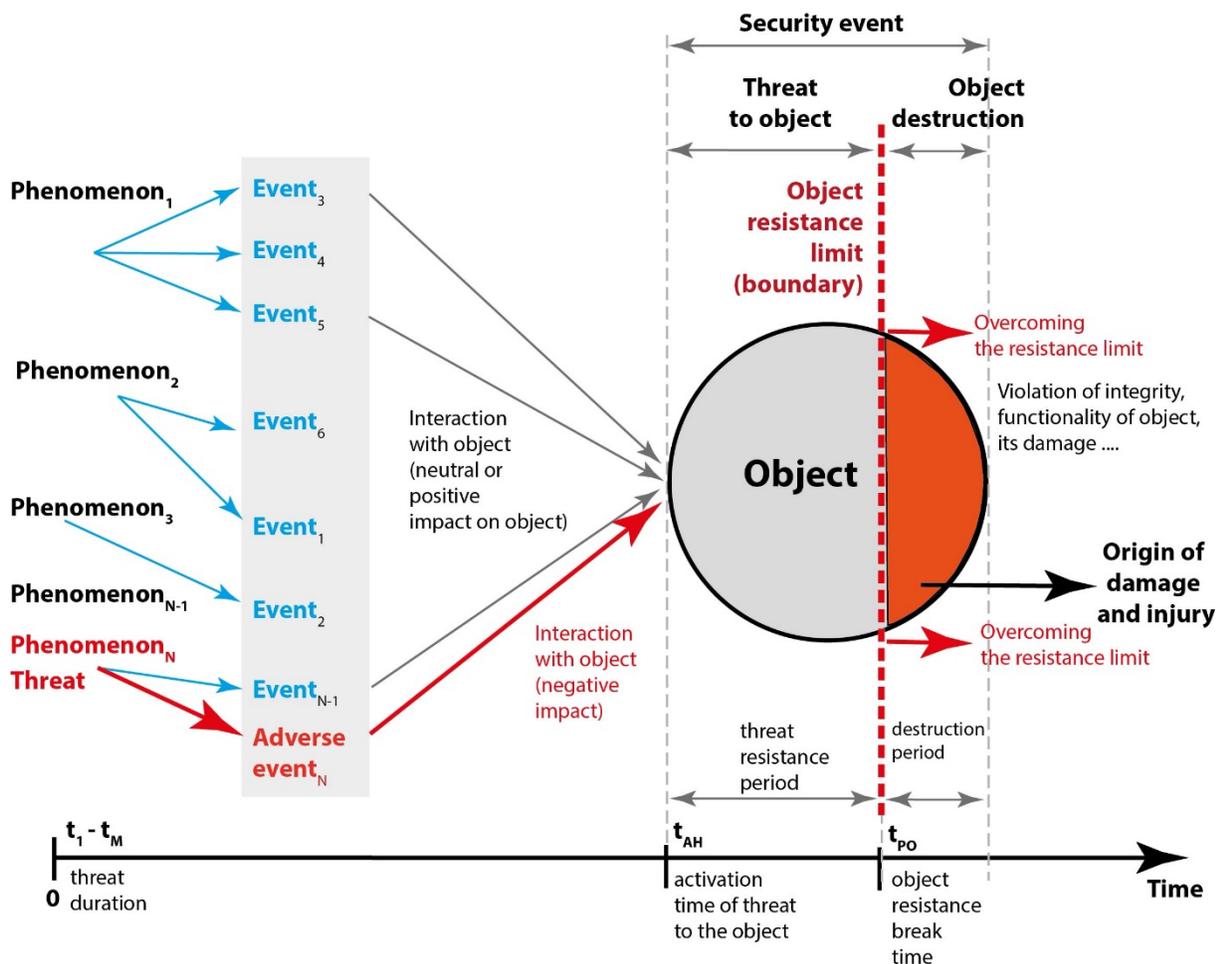


Figure 2. Relations among phenomena (threats), events (adverse events), threat to the object, object destruction, and security events

Systemic threats derive from the intrinsic nature of objects (systems), i.e. the internal structure, system's state, quality, and its behaviour. The system itself generates threats that threaten it and may threaten its immediate surroundings as well (Kubjatko, Görtz, Macurova & Ballay. 2018). **Non-systemic threats** act from outside of the system (object) (they are part of it) or inside the object (system) but as non-systemic, random elements, processes, or relationships.

Stable threats have a repeatable character and exist constantly (crime, hate, diseases, poverty, etc.).

Unstable threats occur sporadically, varyingly, at various times, with different intensities or directions of action (climate changes, accidents, epidemics, various crises, and terrorist attacks).

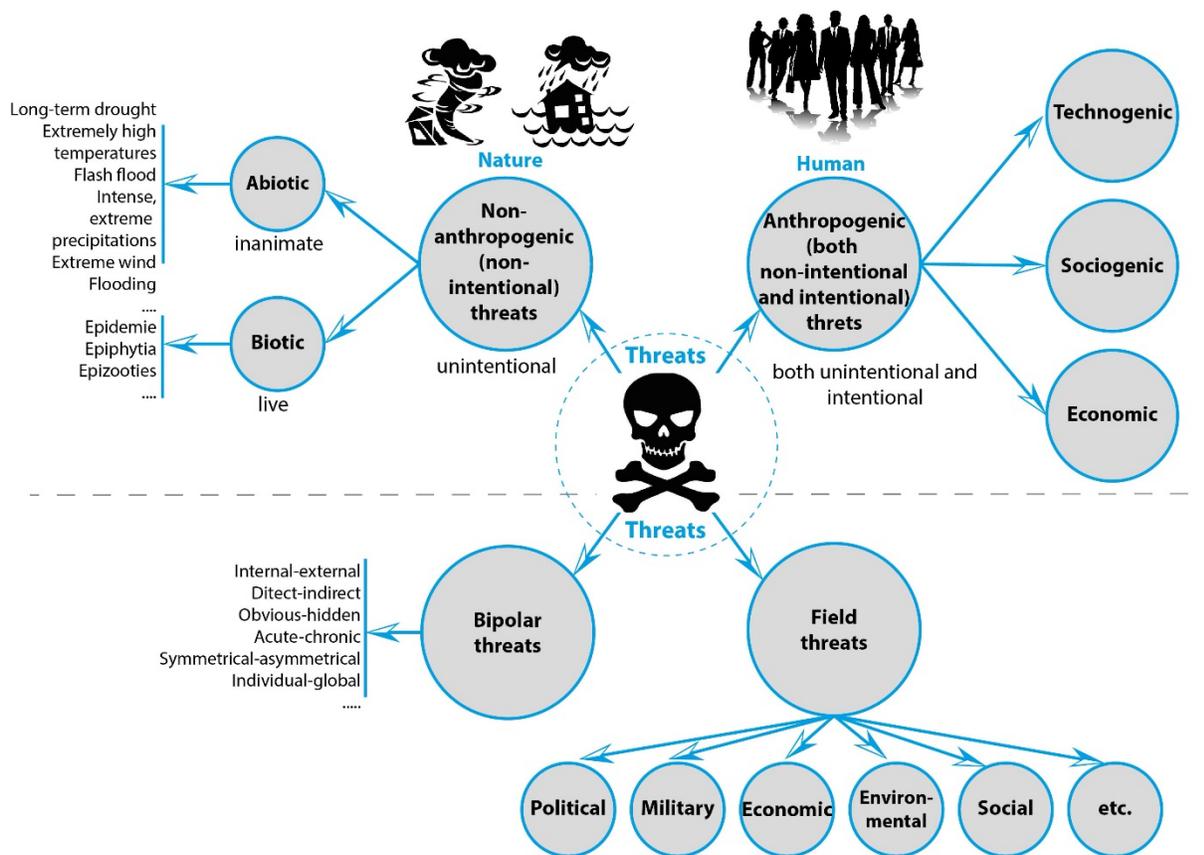


Figure 3. View of various threat categories. Field threats are subject to the interests of specific fields. Bipolar, pair threats are always presented by authors in pairs, e.g. direct vs. indirect threats and so defined.

The aforementioned breakdown of various types of threats (Blazek et al, 2016) may be supplemented by other pair threats, such as **natural/human threats**, **military or non-military threats**, etc.

In practise; however, some hidden threats that have never occurred in practise and are unlikely to occur may still be anticipated and expected. Such threats are **hypothetical threats**. With this type of threat, we usually face a situation when we decide on countermeasures, whether to implement them or not, since implementation may be very costly, and the probability of threat occurrence is low.

In terms of field threats, we may divide threats into **political, military, economic, criminal, and environmental** threats (Kotlan, 2019).

A threat is (consciously or unconsciously) targeted to a vulnerable (weak) spot the target object of interest. This creates the risk a threat turning into an adverse event, subsequent risk that will cause damage or harm to the target object. A threat always precedes the risk, which then causes damage, harm.

Table 1 Overview of unacceptable threats to the Czech Republic. Military threats are excluded from this overview because they are legally dealt with by other authorised institutions (Ministry of Defence). This table was produced by the Integrated Rescue System (IRS) staff CZ.

Threat Categories		Threats with unacceptable risk for the Czech Republic
Naturogenic ¹ (Non-anthropogenic)	abiotic ("inanimate")	Long-term drought
		Extremely high temperatures
		Flash flood
		Intense, extreme System precipitations
		Extreme wind
		Flood
	biotic ("inanimate")	Epidemic - mass infections of people
		Epiphytia - mass infections of field cultures
		Epizootics - mass infections of animals
Anthropogenic ²	Technogenic	Disruption of large-scale food supplies
		Disruption of the functionality of important electronic communication systems
		Breach of information security of a critical information infrastructure
		Special flood
		Leak of a hazardous chemical from stationary equipment
		Disruption of large-scale drinking water supplies
		Disruption of large-scale gas supplies
		Disruption of large-scale oil and petroleum products supplies
		Radiation accidents
		Disruption of large-scale electric power supplies
	Sociogenic	Large-scale migration waves
		Large-scale law violations (including terrorism)
	Economic	Disruption of a state's large-scale financial and foreign exchange economy

To prevent this, countermeasures are proposed based on risk analysis and their potential negative impacts. Their objective is two-fold: to protect vulnerable assets through various protection countermeasures against various threats, while at the same time discouraging all the threat agents from any further motivated attacks.

Obviously, we may only discourage intentional, intended threats of a human or other biological origin³; in particular, natural or technological threats (of non-intentional origin) cannot be discouraged or intimidated in any way since they do not "perceive" any prepared countermeasures.

¹ Caused by nature (both live and inanimate)

² Caused by humans, mankind as such.

³ An electric fence may prevent the entry of, for example, cattle herds on a highway, railway tracks, etc. The electric shock is then remembered by the animals as a conditional reflex, and in many cases, they are scared to repeat a similar experiment.

In their study, authors (Buzalka, Blazek, 2011), (Felcan, 2008) specified the following threats to the Czech Republic, which were classified as unacceptable. These threats are classified into their basic categories, see the Table 1.

In terms of external threats to the Czech Republic, we may find terrorism associated with the proliferation of weapons of mass destruction a very serious threat. It is a deliberate, pressing threat of a political and military nature. It has its two main agents. The first one includes the fanatical opponents of the West and its policies towards the Islamic world, and the second one includes the dictatorial and nationalist regimes that want to assure their invulnerability, i.e. staying as long as possible at their highest military positions (Odlerova, 2017), Zeman (2002). The currently intensively discussed threat is the immigration of people from Asia, North Africa to the EU countries, which at the time of writing did not have a uniform political solution across the EU countries.

Discussion

We live in a global world which, from the point of view of the economy, brings a number of economic benefit and, for many customers, in many respects better products, services, overall simplification of life, of our various activities. However, globalization also brings with it considerable negative effects, which can also have negative effects of a global nature. Many of these effects fall into the area of security, which can be understood in general as the continuity of existing, positive processes or states for us.

Security management falls into the area of threat analysis, risk management and implementation of appropriate measures. The basic, critical aspect is to analyse all potential threats and realistically consider their impacts. Only then can we prevent these threats. Threats in the global world are very diverse and therefore the analytical team must be represented by specialists from various fields, who are the only ones able to identify these threats and correctly assess the resulting risks. Otherwise, we may encounter a situation where we are unable to identify uncommon threats, let alone address them effectively. The categorization of general threats is presented in this paper. It can serve as a basic key to a comprehensive threat analysis so that no threat is overlooked. At first glance, the definitions of the threat categories listed here may seem too general. From the point of view of theory, however, this is perfectly fine, because nothing is left out. The basic directions in which threats and subsequently security must develop are defined. These directions must then be further specified by professional analysts in various fields. The final, output analyses are then submitted to the middle and top management for approval. However, it is important that the management is also an active participant in the analytical phase of defining threats, which are then crucial for the entire institution.

Summary

Our paper has explained all the basic threat relations that we need to know in order to understand threat and handle it meaningfully during our risk management process. It is important to know the threat activators (so-called agents). We often encounter engineering threats without even realising it. It is not that important whether it is the stage of drafting, design, production, operation or maintenance of a technical object or infrastructure. However, it is very important that we are able to identify risks associated with threats and consequently effectively manage risks or avoid risks in time.

References

- Blazek, V., Dworzecki, J., Buzalka, J. et al. (2016) *Crisis scenarios in public administration*. Bratislava Slovak Republic: Academy of the Police Force in Bratislava.
- Buzalka, J., Blazek, V. (2011). *Methodology and procedure of the analysis of the internal threat to the security of the Slovak Republic and its associated threats and risks*, Proceedings Methodology and Procedure of the Analysis of the Sources of Threats to the Internal Security of the Slovak Republic, Public Administration and Crisis management (p. 16-39), Slovakia, Bratislava Slovak Republic: Academy of the Police Force in Bratislava
- Felcan, M. (2008). Implementation of European Union legislation and regulations on road safety standards of the Slovak Republic *Security of transport on the road*, 2008, pp. 122-132
- Hajdukova, T., Kissova, M. (2019) *Prevention of human trafficking through the eyes of young people*. Bratislava, Slovak Republic: Police Academy.
- Janicek, P. (2007) *Systemic Conception of Selected Fields for technicians. Search for Relationships*. Vol. 1, 682 p., Brno, VUT, ISBN 978-80-724-555-6
- Kopencova, D., Felcan, M, Rak, R. (2019) *Objects and systems - Basic analytical security features*. Proceedings of the 14th International Symposium of 14.3. 2019 in *International Security expo*. Academy of Police force in Bratislava, (pp. 41-55), March 2019, Bratislava, Slovak Republic.
- Kotlan, P. (2019), The Seizure of Property in Criminal Proceedings. *Public prosecution*, 17(5), 52-57.
- Kubjatko, T., Görtz, M., Macurova, L., Ballay, M. (2018). Synergy of forensic and security engineering in relation to the model of deformation energies on vehicles after traffic accidents (Conference Paper) *Transport Means - Proceedings of the International Conference Volume 2018-October*, 2018, pp. 1342-1348, 22nd International Scientific on Conference Transport Means 2018; Trasalis - Trakai Resort and SPAGedimino str. 26, Trakai; Lithuania; 3 October 2018 through 5 October 2018; Code 140271,
- Odlerova, M. (2017). Information technology and operative-search activity. In: *Act on police corps: Application on practice*. (pp. 196-217), Bratislava, Slovak Republic: Police Academy.
- Vlach, F. (2018). *Evaluation of cooperation between educational institutions of the armed forces*. New trends in police training III. International conference. Holesov: Higher Police School and Secondary Police School of the Ministry of the Interior in Holesov, pp. 121 - 124.
- Zeman, P. et al. (2002). *Czech Security Terminology*, Institute of Strategic Studies of the University of Defence in Brno, Brno.