VÝCHODISKA HODNOCENÍ RESILIENCE PRVKŮ KRITICKÉ INFRASTRUKTURY

David Řehák[1]

ABSTRAKT
Resilienci v systému kritické infrastruktury lze chápat jako stav, který snižuje zranitelnost, minimalizuje následky působení hrozeb, urychluje reakci a obnovu a napomáhá adaptaci na danou nežádoucí událost. Na základě uvedeného článek prezentuje odborný pohled na problematiku hodnocení resilience prvků kritické infrastruktury. Pozornost je věnována zejména konceptu vnímání resilience v kontextu kritické infrastruktury. V souvislosti s hodnocením resilience prvků je představen rámec tohoto procesu a základní komponenty hodnocení, kterými jsou robustnost, obnovitelnost a adaptabilita. V závěru článku jsou přiblíženy nejen tyto komponenty, ale také jejich proměnné determinující resilienci prvků kritické infrastruktury.

Klíčová slova:
Kritická infrastruktura; Resilience; Robustnost; Obnovitelnost; Adaptabilita.

ABSTRACT
Critical Infrastructure Resilience can be seen as a condition that reduces vulnerability, minimizes the impact of threats, speeds up response and recovery, and helps adapt to the undesirable event. Based on the above, article presents an expert view on the issue of the of critical infrastructure elements resilience assessment. Attention is paid in particular to the concept of resilience perception in the context of critical infrastructure. In connection with the element resilience assessment, the framework of this process and the core components of the assessment are robustness, recovery and adaptability. At the end of the article, not only are these components, but also their variables determining the resilience of critical infrastructure are described.

Key words:
Critical infrastructure; Resilience; Robustness; Recoverability; Adaptability.

[1] Fakulta bezpečnostního inženýrství, VŠB – Technická univerzita Ostrava, Lumírova 13, 700 30 Ostrava – Výškovice, tel.: +420 597 322 816, email: david.rehak@vsb.cz

1 ÚVOD

Kritická infrastruktura (KI) představuje složitý a komplexní systém [1], jehož podstatou je permanentní poskytování služeb nezbytných pro fungování společnosti. Jedinečnost tohoto systému spočívá především v požadované vysoké spolehlivosti a dostupnosti služeb, zejména v oblastech s vysokou mírou urbanizace (koncentrovanost užití). Současně je však tento systém tvořen rozsáhlými systémy sítí infrastruktur, které jsou ze své podstaty, decentralizované a pokrývající značná území. Jednotlivé subsystémy kritické infrastruktury jsou proto neustále vystavovány působení různých hrozeb, které mají za následek vznik nežádoucích událostí. Ty pak mohou, v závislosti na své intenzitě, vést k narušení nebo dokonce selhání dodávky služeb jednotlivých subsystémů kritické infrastruktury.

Otázky ochrany kritické infrastruktury, stejně jako její vazba na dlouhodobý udržitelný rozvoj společnosti, jsou proto předmětem dlouhodobého zájmu z pohledu různých vědních disciplín. Lepší pochopení vazeb mezi jednotlivými subsystémy KI navzájem [2], ale také mezi systémem KI a společností jako takovou, je pak základem návrhu systému ochrany KI a jejích prvků. Z tohoto důvodu je věnována značná pozornost procesům a prostředkům ochrany kritické infrastruktury, přičemž za výchozí řešení může být považováno posilování resilience těchto subsystémů.

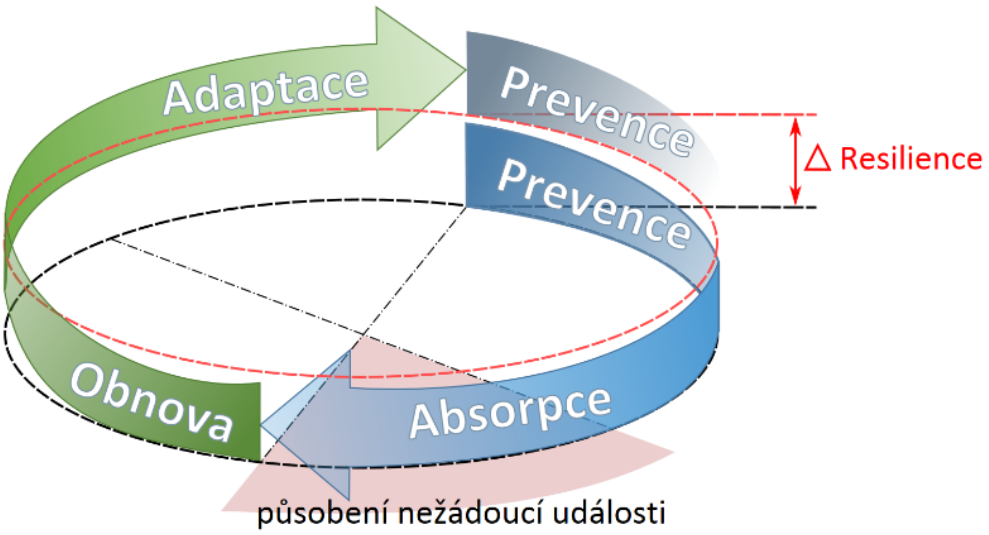
2 VNÍMÁNÍ RESILIENCE V KONTEXTU KRITICKÉ INFRASTRUKTURY

Termín resilience byl poprvé definován Hollingem [3], a to v souvislosti s rezistencí a stabilizací ekologických systémů (později také socio-ekologických systémů). Postupem času se pojem resilience začal promítat i do dalších vědních oborů jako sociologie, psychologie či ekonomie. Relativně nejmladší oborem, z pohledu zkoumání resilience systémů, je inženýrství. V kontextu kritické infrastruktury představuje resilience vnitřní připravenost subsystémů na nežádoucí události. Jedná se tak o schopnost těchto subsystémů zajistit a udržovat si své funkce při negativním působení vnitřních a/nebo vnějších faktorů. Resilienci lze tedy chápat jako opak zranitelnosti, resp. resilience a zranitelnost mají vůči sobě inverzní charakter. Zranitelné subsystémy postrádají resilienci a naopak resilientní subsystémy nejsou příliš zranitelné.

Resilience kritické infrastruktury byla poprvé komplexně definována v dokumentu Critical Infrastructure Resilience Final Report and Recommendations [4], ačkoliv úvahy o potřebě ochrany systému kritické infrastruktury jsou starší. Již v roce 1998 bylo vydáno Presidential Decision Directive PDD-63 [5] k ochraně kritické infrastruktury, avšak teprve Presidential Decision Directive PPD-21 [6] se extenzivněji zabývá kromě ochrany kritické infrastruktury také její resiliencí.

Základní funkční podmínkou utváření a posilování resilience subsystémů kritické infrastruktury je jednoznačné vymezení a vnímání faktorů, kterými je

determinována. V tomto kontextu je nutné vnímat resilienci v systému kritické infrastruktury jako cyklický proces neustálého zdokonalování prevence, absorpce, obnovy a adaptace systému (viz obrázek 1).



Obrázek 1 Cyklus resilience kritické infrastruktury [7]

První fází cyklu resilience subsystému kritické infrastruktury je prevence. Realizací preventivní činnosti vlastník/provozovatel připravuje subsystém na budoucí nežádoucí události. V okamžiku působení takovýchto událostí pak systém přechází z fáze prevence do fáze absorpce.

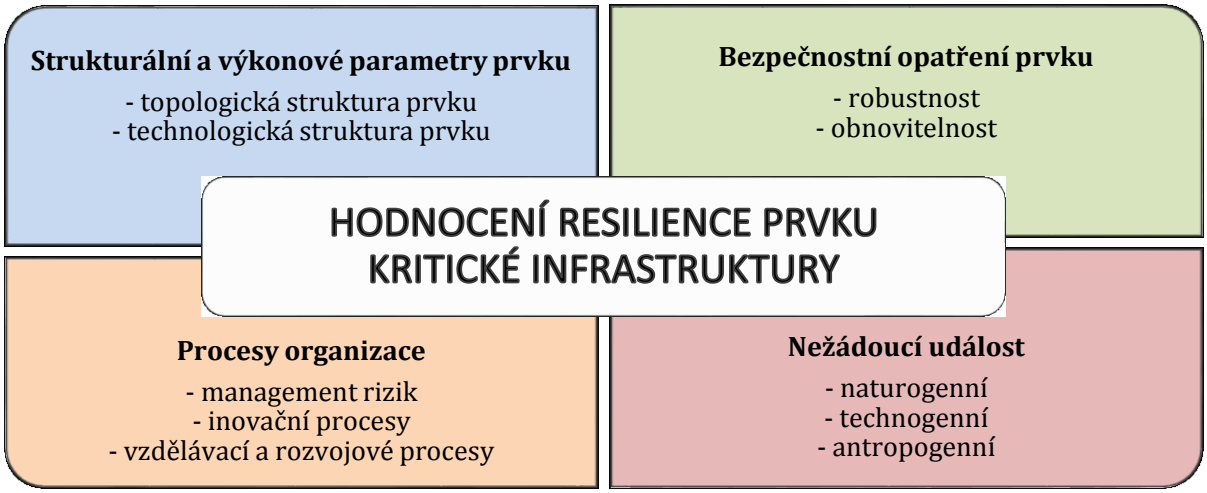
Absorpce je iniciována vlivem působení nežádoucí události a je determinována robustností subsystému kritické infrastruktury. Podstatou robustnosti je schopnost prvku kritické infrastruktury absorbovat působení nežádoucí události, aniž by došlo k výkyvům jím poskytovaných služeb.

Po ukončení působení nežádoucí události nastává fáze obnovy. Ta je charakterizována obnovitelností, tedy schopností subsystému obnovit svou činnost do původní, popř. požadované, úrovně výkonu. Délka fáze obnovy je determinována dostupnými zdroji a časem nutným pro realizaci jednotlivých procesů obnovy.

Poslední fází cyklu resilience kritické infrastruktury je adaptace. Jedná se o schopnost organizace adaptovat provozovaný subsystém na případné opakování již proběhlé nežádoucí události – tedy poučit se z v minulosti řešených nežádoucích událostí. Adaptace tak představuje dynamickou, dlouhodobě působící, schopnost organizace adaptovat se na změněnou situaci. Adaptace je determinována vnitřními procesy organizace směřujícími k posilování resilience, tj. management rizik, inovační procesy a vzdělávací a rozvojové procesy. K posilování resilience subsystémů ovšem může docházet již ve fázi obnovy např. formou výměny komponent nebo úpravy procesů jejich fungování.

3 RÁMEC HODNOCENÍ RESILIENCE PRVKŮ KRITICKÉ INFRASTRUKTURY

Hodnocení resilience prvků kritické infrastruktury představuje komplexní proces založený na jednoznačně definovaných postupech a dobré znalosti podkladových dat. K provedení hodnocení je totiž třeba znát základní strukturální a výkonové parametry hodnoceného prvku, stávající bezpečnostní opatření hodnoceného prvku, procesy organizaci podporující posilování resilience prvku a v neposlední řadě konkrétní nežádoucí událost, vůči které bude resilience prvku hodnocena (viz obrázek 2).



Obrázek 2 Rámec hodnocení resilience prvků kritické infrastruktury [7]

Znalost strukturálních a výkonových parametrů prvku je nezbytným podkladem pro hodnocení resilience. Jedná se zejména o schopnost provozovatele kategorizovat hodnocený prvek podle stanovených odvětvových kritérií [8], znalost topologické struktury prvku (tzn. zda se jedná o bodový, liniový nebo plošný prvek) a znalost technologické struktury prvku (např. počty a výkony klíčových technologií).

Dalším významným podkladem hodnocení resilience je znalost stávajících bezpečnostních opatření prvku se zaměřením na jeho robustnost a obnovitelnost prvku. Jedná se zejména o znalost úrovně krizové připravenosti, redundance, schopnosti detekce, reakceschopnosti, fyzické odolnosti (tj. technických prostředků a organizačních či režimových opatření), jakož i materiálních zdrojů, finančních zdrojů, lidských zdrojů či procesů obnovy prvku po nežádoucí události.

Procesy organizace jsou dalším významným zdrojem podkladových dat utvářejících rámec hodnocení resilience. Jejich znalost umožňuje hodnocení úrovně adaptability prvku na již proběhlé nežádoucí události. Jedná se zejména o znalost managementu rizik, inovačních procesů a vzdělávacích a rozvojových procesů.

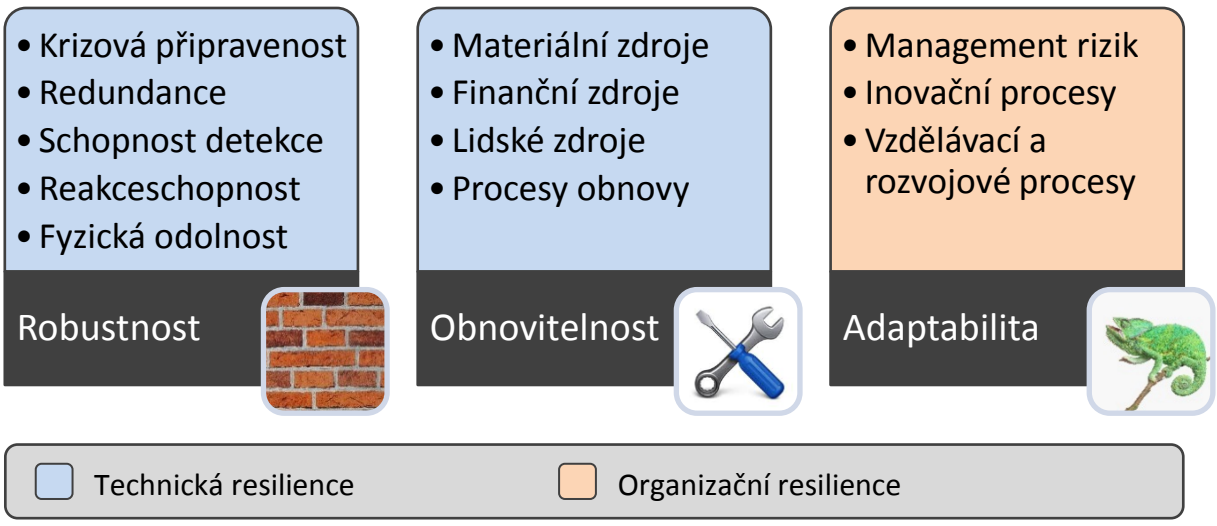
Posledním podkladem nezbytným pro hodnocení úrovně resilience prvku kritické infrastruktury je znalost konkrétní nežádoucí události. Specifikace nežádoucí

události primárně vychází ze znalosti konkrétní hrozby, vůči které je prvek hodnocen. Za tímto účelem bylo nadefinováno sedm základních skupin hrozeb, kterými jsou hrozby procesně-technologické a personální (tj. hrozby vnitřní) a hrozby geologické, meteorologické, kaskádní, kybernetické a fyzické (tj. hrozby vnější).

4 KOMPONENTY HODNOCENÍ RESILIENCE PRVKŮ KRITICKÉ INFRASTRUKTURY

Resilience prvků v systému kritické infrastruktury je determinována ve dvou základních oblastech, kterými jsou technologická a fyzická ochrana prvků a management organizace. První oblastí je technologická a fyzická ochrana jednotlivých prvků. Tento typ resilience je označován jako technická resilience a je determinován robustností a obnovitelností prvků. Posilování technické resilience je realizováno vždy výhradně ve vztahu ke konkrétnímu prvku nebo skupině stejných či velmi podobných prvků. Jako příklad může sloužit sektor elektroenergetiky, kde bude robustnost a obnovitelnost zajišťována odlišnými způsoby a prostředky u zařízení pro výrobu elektrické energie a u zařízení pro jeho přenos či distribuci.

Druhou oblastí je management organizace. Tento typ resilience je označován jako organizační resilience [9] a je determinován úrovní vnitřních procesů organizace, jejichž podstatou je vytváření co nejlepších podmínek pro adaptaci prvků kritické infrastruktury na nežádoucí události. Komponenty resilience a jejich proměnné jsou prezentovány na obrázku 3.



Obrázek 3 Komponenty a proměnné determinující resilienci prvků kritické infrastruktury [7]

Technická resilience je utvářena robustností a obnovitelností prvků kritické infrastruktury. Tyto dvě komponenty jsou u každého prvku determinovány či ovlivňovány třemi základními faktory, kterými jsou technologická struktura prvku, bezpečnostní opatření prvku a nežádoucí události, kterou je resilience ovlivňována.

Organizační resilience je utvářena společně pro všechny prvky kritické infrastruktury provozované danou organizací. Tento typ resilience je utvářen, hodnocen a posilován managementem organizace již ve fázi prevence a zohledňuje úroveň vnitřních procesů, které jsou nezbytné ve fázi adaptace prvků kritické infrastruktury s použitím zkušeností získaných při likvidačních a obnovovacích pracích v minulosti.

4.1 ROBUSTNOST PRVKŮ KRITICKÉ INFRASTRUKTURY

Robustnost je schopnost prvku absorbovat působení dopadů nežádoucí události. Tyto dopady mohou být absorbovány prostřednictvím strukturálních vlastností budov nebo použitých technologií (tj. strukturální robustnost) a/nebo prostřednictvím bezpečnostních opatření (tj. robustnost zabezpečení). Robustnost je determinována následujícími proměnnými [7]:

- krizová připravenost (soubor opatření ke zvýšení připravenosti prvku kritické infrastruktury na nežádoucí události);
- redundance (schopnost okamžité substituce výkonu narušené části prvku nebo posílení jeho kapacit);
- schopnost detekce (pravděpodobnost a/nebo čas rozpoznání nežádoucí události);
- reakceschopnost (pravděpodobnost a/nebo čas zásahu vedoucího k eliminaci příčin nežádoucí události nebo minimalizaci jejích následků);
- fyzická odolnost (soubor technických prostředků a organizačních či režimových opatření ke zvýšení fyzické odolnosti prvku kritické infrastruktury vůči nežádoucím událostem).

Dosáhne-li robustnost úrovně 100 %, pak se prvek stává proti dopadům dané nežádoucí události rezistentní. To znamená, že je schopen plně odolat jejím účinkům bez citelných negativních dopadů na prvkem poskytované služby.

4.2 OBNOVITELNOST PRVKŮ KRITICKÉ INFRASTRUKTURY

Obnovitelnost je schopnost prvku obnovit svou činnost do původní (požadované) úrovně poskytovaných služeb po ukončení působení dopadů nežádoucí události. Obnovitelnost je v oblasti kritické infrastruktury chápána jako opravitelnost; uvažována je tedy pouze oprava nebo náhrada poškozených nebo zničených komponent prvku. Obnovitelnost je determinována následujícími proměnnými [7]:

- materiální zdroje (dostupnost potřebných komponent k realizaci opravy nebo náhrady poškozených nebo zničených částí prvku);
- finanční zdroje (dostupnost finančních zdrojů, popř. rezerv, umožňujících financování rychlé obnovy prvku);
- lidské zdroje (dostupnost lidských zdrojů s potřebnou kvalifikací);
- procesy obnovy (procesy podporující rychlou obnovu požadovaného výkonu prvku).

Jsou-li výše uvedené zdroje dostatečné, může docházet k posilování resilience již v této fázi. Příkladem může být implementace modernějších technologií splňující vyšší bezpečnostní standardy a posilujících robustnost prvku.

4.3 ADAPTABILITA PRVKŮ KRITICKÉ INFRASTRUKTURY

Adaptabilita je schopnost subjektu kritické infrastruktury (tj. organizace) připravit prvek na opakované působení již proběhlé nežádoucí události. Představuje dynamickou (dlouhodobě působící) schopnost organizace přizpůsobit se na změněnou situaci. Adaptabilita je determinována vnitřními procesy organizace, jejichž podstatou je vytváření co nejlepších podmínek pro posilování technické resilience. Základními procesy posilujícími adaptabilitu prvků kritické infrastruktury na nežádoucí události jsou management rizik, inovační procesy a vzdělávací a rozvojové procesy.

Management rizik představuje významný vnitřní proces organizace, který je nezbytný pro zajišťování bezpečnosti a posilování resilience již ve fázi prevence. Management rizik spočívá v koordinaci činností pro vedení a řízení organizace s ohledem na rizika [10] a jeho úroveň ve vztahu k organizační resilienci je determinována čtyřmi kritérii, kterými jsou:

- úroveň managementu rizik,
- úroveň aplikované metodologie posuzování rizik,
- úroveň implementace bezpečnostních norem,
- úroveň specifikace scénářů nežádoucích událostí, které jsou stěžejním východiskem pro tvorbu nouzových plánů.

Dalšími vnitřními procesy, které významně přispívají k posilování resilience prvků kritické infrastruktury ve fázi prevence, jsou inovační procesy organizace. Z věcného hlediska se inovace člení na produktové, procesní, marketingové a organizační [11]. V případě posilování resilience jsou významné zejména inovace procesní a organizační, které jsou zaměřené na spolehlivost a vnější zabezpečení používaných technologií. Samotný inovační proces má tři základní fáze, kterými jsou invence, věda a výzkum a realizace. Úroveň inovačního procesu je determinována osmi kritérii, kterými jsou:

- pružnost organizační struktury,
- úroveň implementace systémů řízení,
- způsob řízení organizačních procesů,
- úroveň inovace procesů řízení,
- rozsah realizace technologických inovací,
- úroveň inovace bezpečnostních opatření,
- úroveň zapojení organizace do vědy a výzkumu,
- úroveň investic organizace do jednotlivých inovací.

Vzdělávací a rozvojové procesy jsou poslední skupinou procesů, které utvářejí a posilují organizační resilienci prvků kritické infrastruktury, čímž posilují schopnost organizace adaptovat tyto prvky na následné působení nežádoucí události. Vzdělávací a rozvojové procesy lze členit do tří základních kategorií [12], kterými jsou znalosti

(explicitní a tacitní), dovednosti (např. odborně-technické, manažerské, analytické, koncepční) a postoje (odrážejí hodnoty, které konkrétní osoba uznává). Mezi stěžejní formy vzdělávacích a rozvojových aktivit patří dlouhodobé vzdělávání, zahraniční studijní pobyty, rozvoj dovedností (soft skills), odborné školení (preventivního i represivního charakteru) a výcvik personálu. Úroveň vzdělávacího a rozvojového procesu je determinována třemi kritérii, kterými jsou:

- úroveň vzdělání, které je poskytováno a umožňováno pracovníkům organizace,
- úroveň výcviku a udržování praktických dovedností pracovníků,
- způsob hodnocení efektivnosti výcviku pracovníků.

5 ZÁVĚR

Resilience je v systému kritické infrastruktury definována jako schopnost absorbovat, přizpůsobit se, a/nebo se rychle zotavit z potenciálně nebezpečné události. V tomto kontextu ji lze chápat jako stav, který úzce souvisí s funkcí výkonu jednotlivých subsystémů. Resilientní subsystémy vykazují v průběhu působení nežádoucí události menší pokles výkonu a jeho návrat na požadovanou úroveň probíhá v kratším čase. Výchozím faktorem utváření a posilování resilience je definování funkčních podmínek, čímž dochází k jednoznačnému nastavení konceptu resilience těchto subsystémů v systému kritické infrastruktury.

Posilování resilience je založeno na kontinuálním zvyšování úrovně jednotlivých proměnných, kterými je determinována. Těmto proměnným musí být věnována pozornost nejen v oblasti technické resilience (tj. robustnosti a obnovitelnosti), ale také v oblasti resilience organizační (tj. adaptability). Současně je však nutné reflektovat také faktory limitující resilienci (tj. např. právní úprava provozu infrastruktur nebo úroveň disponibilních finančních zdrojů) a faktory, jež resilienci ovlivňují (tj. např. hrozby či nástroje posilování resilience).

VAZBA NA PROJEKT

Tento příspěvek vznikl za podpory grantového projektu VI20152019049 "RESILIENCE 2015: Dynamické hodnocení odolnosti souvztažných subsystémů kritické infrastruktury", podpořeného Ministerstvem vnitra České republiky v letech 2015-2019.

LITERATURA

[1] VAN DER LEI, T.E., BEKEBREDE, G., NIKOLIC, I. 2010. Critical infrastructures: a review from a complex adaptive systems perspective. In: *International Journal of Critical Infrastructures*. Vol. 6, pp. 380-401. DOI: 10.1504/IJCIS.2010.037454

[2] RINALDI, S.M., PEERENBOOM, J.P., KELLY, T.K. 2001. Identifying, understanding, and analyzing critical infrastructure interdependencies. In: *IEEE Control Systems.* Vol. 21, pp. 11-25. DOI: 10.1109/37.969131
[3] HOLLING, C.S. 1973. Resilience and Stability of Ecological Systems. In: *Annual Review of Ecology and Systematics*. Vol. 4, pp. 1-23. DOI: 10.1146/annurev.es.04.110173.000245
[4] National Infrastructure Advisory Council. 2009. Critical Infrastructure Resilience Final Report and Recommendations. U.S. Department of Homeland Security, Washington, D.C. 54 p.
[5] PPD-63. 1998. Presidential Decision Directive: Critical Infrastructure Protection. The White House, Washington, D.C.
[6] PPD-21. 2013. Presidential Decision Directive: Critical Infrastructure Security and Resilience. The White House, Washington, D.C.
[7] ŘEHÁK, D., ŠENOVSKÝ, P., HROMADA, M., PIDHANIUK, L., DVOŘÁK, Z., LOVEČEK, T., RISTVEJ, J., LEITNER, B., SVENTEKOVÁ, E., MARIŠ, L. 2018. Metodika hodnocení resilience prvků kritické infrastruktury. VŠB – Technická univerzita Ostrava, Ostrava. 90 s.
[8] Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, v platném znění.
[9] DENYER, D. 2017. Organizational Resilience: A summary of academic evidence, business insights and new thinking. BSI and Cranfield School of Management, Cranfield, United Kingdom. 55 p.
[10] ISO 31000:2018. Risk management – Guidelines.
[11] Oslo Manual. 2005. Guidelines for Collecting and Interpreting Innovation Data. 3rd edit. OECD, Paris, France. 162 p. DOI: 10.1787/9789264013100-en
[12] ARMSTRONG, M. 2017. Armstrong's Handbook of Human Resource Management Practice. 14th edit. Kogan Page, London, United Kingdom. 776 p.