NOVÝ ŠTUDIJNÝ PROGRAM „BEZPEČNOSŤ A OCHRANA KRITICKEJ INFRAŠTRUKTÚRY“ – CHARAKTERISTIKA PROGRAMU A AKTUÁLNE VÝZVY

Bohuš Leitner [1], Zdeněk Dvořák [2], Eva Sventeková [3]

ABSTRAKT
V roku 2014 začal proces komplexnej akreditácie vysokých škôl pôsobiacich v SR. V rámci tohto procesu vedenie Fakulty bezpečnostného inžinierstva ŽU v Žiline rozhodlo o podaní žiadosti o akreditáciu nového študijného programu s názvom „Bezpečnosť a ochrana kritickej infraštruktúry“. Cieľom príspevku je prezentácia dôvodov pre zavedenie nového programu, zdôvodnenie potreby vzdelávania v oblasti bezpečnosti kritickej infraštruktúry, charakteristika profilu absolventa a študijného plánu, ale aj poukázanie na aktuálne problémy s realizáciou študijného programu.

Kľúčové slová: kritická infraštruktúra, sektor energetika, sektor doprava, bezpečnosť, ochrana, nový študijný program

ABSTRACT
In 2014 began the process of comprehensive accreditation of universities operating in Slovakia. In this process, the Faculty of Safety Engineering University of Žlina decided to accredit new study program named "Security and protection of critical infrastructure." The aim of the paper is to present the main reasons for the introduction of a new program, justification for the need of education in the field of critical infrastructure, characteristics of the graduate profile and content of the curriculum, but also point out the current issues related to the implementation of the study program.

Key words: critical infrastructure, sector of energetics, sector of transportation, safety, protection, new study program.

[1] Bohuš Leitner, doc. Ing., PhD., Žilinská univerzita, Fakulta bezpečnostného inžinierstva, 1.mája 32, 010 26, Žilina, +421-41-513 6863, fax: +421-41-513 6620, Bohus.Leitner@fbi.uniza.sk

[2] Zdeněk Dvořák, prof. Ing., PhD., Žilinská univerzita, Fakulta bezpečnostného inžinierstva, 1.mája 32, 010 26, Žilina, +421-41-513 6600, fax: +421-41-513 6620, Zdenek.Dvorak@fbi.uniza.sk

[3] Eva Sventeková, doc. Ing., PhD., Žilinská univerzita, Fakulta bezpečnostného inžinierstva, 1.mája 32, 010 26, Žilina, +421-41-513 6862, fax: +421-41-513 6620, Eva.Sventekova@fbi.uniza.sk

1 ÚVOD

Z výsledkov komplexnej akreditácie činnosti Žilinskej univerzity v Žiline (ďalej iba ŽU v Žiline) za hodnotené obdobie 2002 – 2007 vyplynulo, že ŽU v Žiline je vysokoškolskou vzdelávacou a vedecko-výskumnou inštitúciou s výrazne širokým záberom. Ako jedna zo slabších stránok v činnosti univerzity bola uvedená roztrieštenosť výskumných a vzdelávacích kapacít v niektorých profilových odboroch (napr. manažment, dopravné služby). Na základe odporúčaní bolo na Fakulte bezpečnostného inžinierstva Žilinskej univerzity v Žiline (ďalej FBI ŽU) prijaté rozhodnutie, že realizovaný študijný program „Doprava v krízových situáciách“, zaradený v rámci oblasti výskumu 22 - Dopravné služby bude postupne utlmený a fakulta sa bude uchádzať o akreditáciu nového študijného programu v oblasti výskumu 23 - Bezpečnostné služby. Uvedená aktivita bola úspešne ukončená v auguste 2013, kedy bol Akreditačnou komisiou, ako poradným orgánom Vlády SR, akreditovaný nový študijný program s názvom „Bezpečnosť a ochrana kritickej infraštruktúry“. Cieľom príspevku je uvedenie základných pojmov z oblasti bezpečnosti kritickej infraštruktúry a jej ochrany, zdôvodnenie potreby vzdelávania v oblasti riadenia bezpečnosti a ochrany kritickej infraštruktúry a prezentácia obsahu študijného programu, ale aj aktuálnych výziev pre ďalší rozvoj a skvalitnenie obsahu a prínosov študijného programu pre spoločnosť.

2 RIADENIE BEZPEČNOSTI KRITICKEJ INFRAŠTRUKTÚRY A ZDÔVODNENIE POTREBY VZDELÁVANIA V TEJTO OBLASTI

Nové ohrozenia, dynamický rozvoj technológie, politické a ekonomické zmeny vo svete prinášajú potrebu hľadať nové spôsoby ako ochrániť (t.j. zaistiť požadovanú mieru bezpečnosti) ľudí, majetok alebo určité územie ako celok. Otázky bezpečnosti a ochrany tzv. *kritickej infraštruktúry* (ďalej KI) je potrebné vnímať a riešiť komplexne, najmä kvôli vzájomnej prepojenosti jednotlivých infraštruktúr. Snahou Európskej únie (ďalej iba EÚ) v tejto strategickej oblasti je predovšetkým zlepšenie spolupráce medzi jednotlivými krajinami a vytvorenie jednotného prístup k zásadným problémom riadenia bezpečnosti dôležitej európskej infraštruktúry. Slovenská republika (ďalej SR) už dávnejšie prijala niektoré zákonné normy [1] a opatrenia, vedúce k zvýrazneniu významu problematiky KI a zaisteniu požadovanej úrovne jej bezpečnosti a ochrany.

Kritickou infraštruktúrou rozumieme časť národnej infraštruktúry (vybrané systémy, služby a organizácie a ich dôležité objekty a zariadenia), ktorej zničenie alebo znefunkčnenie v dôsledku pôsobenia rizikového činiteľa spôsobí ohrozenie alebo narušenie fungovania spoločnosti alebo ohrozenie života a zdravia obyvateľstva. Kritická infraštruktúra je súčasťou bezpečnostného systému štátu. Pre správne pochopenie celej šírky oblastí kritickej infraštruktúry je potrebné uviesť zoznam tzv. *sektorov kritickej infraštruktúry*. Vo väčšine krajín sú sektormi KI najmä – *energetika* (hlavne jadrová energetika a prenos elektrickej energie), *doprava* (cestná, železničná, letecká, a vodná), *informačné a komunikačné technológie* (siete, dátové centrá, nosiče dôležitých informácií a pod.) prípadne ďalšie oblasti, ako vodné hospodárstvo, potravinová bezpečnosť, finančný sektor, sieť zdravotníckych zariadení a ďalšie.

Smernicou Rady Európy 2008/114/ES [2] bol definovaný pojem tzv. *Európskej kritickej infraštruktúry* (ďalej EKI). Pre identifikáciu prvkov a riadenie bezpečnosti EKI je nevyhnutné zadefinovať najpravdepodobnejšie typy útokov, pričom medzi najpravdepodobnejšie typy antropogénnych ohrození je možné zaradiť najmä:

- *„priamu akciu – priamy ozbrojený fyzický útok na cieľ uskutočnený ozbrojenými teroristickými skupinami,*
- *bombový útok – útok, ktorý je spravidla vykonaný jednotlivcom alebo malou skupinou s využitím napr. nekonvenčných náloží,*
- *tzv. CBRN útok – útok s použitím CBRN (chemických, biologických, bakteriologických alebo rádioaktívnych) látok,*
- *kybernetický útok – útok, ktorý je zameraný na zničenie alebo ovládnutie informácií a údajov, prípadne na narušenie počítačových systémov a programov (spravidla prostredníctvom internetovej siete),*
- *informačné operácie – útoky, ktoré majú za cieľ získať alebo zneužiť informácie, ovplyvniť procesy založené na informáciách (napr. ovplyvniť systém tak, že sa javí ako plne funkčný, ale v skutočnosti pracuje so „zmanipulovanými“ údajmi)“* a pod.

Z pohľadu aktuálneho chápania problematiky, vychádzajúceho z európskeho alebo národného právneho rámca [3], je nutné mať zadefinované určité minimálne požiadavky (bezpečnosť, spoľahlivosť), konkretizované pre jednotlivé systémy a objekty vybraných prvkov KI. V podmienkach SR zatiaľ však chýba všeobecne akceptovaná metodika pre jednoznačné zaradenie prvkov jednotlivých infraštruktúr (najmä energetickej, dopravnej a informačno-komunikačných technológií) do množiny prvkov KI, ako aj objektívnejšia metodika pre hodnotenie ich kritickosti a citlivosti na zlyhanie ďalších dôležitých infraštruktúr. Okrem identifikácie prvkov KI je aktuálnou úlohou aj overovanie toho, či prevádzkovatelia jednotlivých systémov KI majú realizovaný proces posúdenia rizík ich technológií (identifikácia hrozieb, analýza a hodnotenie rizík, určenie zraniteľných miest, ...) a či majú dostatočne kvalitne spracované základné dokumenty v oblasti ochrany, najmä tzv. *bezpečnostné plány [4]*.

Vo všeobecnosti, pod pojmom ochrana kritickej infraštruktúry [5] rozumieme súbor opatrení, ktoré vlastník, prevádzkovateľ objektu, ale aj súkromné bezpečnostné služby a určené jednotky integrovaného záchranného systému musia zabezpečiť s cieľom zaistiť požadovanú funkčnosť a výkonnosť dôležitej infraštruktúry. Je zrejmé, že ochrana ako proces musí prebiehať nepretržite, nielen počas trvania krízového javu. Z uvedeného je zrejmé, že ochrana kritickej infraštruktúry je proces, ktorý má za cieľ zabezpečiť fungovanie subjektov a objektov KI, aby sa minimalizovalo riziko ich zlyhania pri zohľadnení všetkých možných podmienok a hrozieb.

Cieľom systému ochrany kritickej infraštruktúry by mala byť predovšetkým minimalizácia vplyvu jej znefunkčnenia tak, že vyradenie funkcie, činnosti alebo služby bude krátke, zvládnuteľné (aj keď iba provizórnym spôsobom) a priestorovo obmedzené na minimálny počet ovplyvnených obyvateľov [8]. Procesy riadenia bezpečnosti by preto nemali byť zamerané iba na záverečnú fázu – samotnú ochranu - prvkov kritickej infraštruktúry, ale vo väčšej miere predovšetkým na možnosti minimalizácie vzniku nežiaducich negatívnych javov a ich potenciálnych následkov.

Je preto nutné objektívne definovať celý proces riadenia bezpečnosti - začínajúci identifikáciou možných prvkov KI, cez analýzu ich ohrození, posudzovanie rizík a ich vplyvu na výkonnosť, zraniteľnosť a funkčnosť potenciálnych prvkov KI pri

určitých obmedzujúcich podmienkach a končiaci možnosťou definovania a uplatňovania efektívnych ochranných opatrení na zaistenie ich fungovania.

Z uvedeného je možné definovať ciele ochrany KI:

- *zamedziť prieniku do objektu a zabrániť činnosti nepovolaným osobám či skupinám,*
- *znížiť alebo zabrániť vzniku bezpečnostného rizika (teroristického útoku, sabotáže, krádeže, a iné),*
- *zabezpečiť funkčnosť technológií a využiteľnosť uskladnených zásob,*
- *zabezpečiť bezpečnosť prevádzky a z nej vplývajúcu bezpečnosť pobytu obyvateľstva alebo ozbrojených síl v okolí objektov. Upravené podľa [5].*

Z vyššie uvedených zdrojov [1,2,3,4,5] a ďalších vybraných publikovaných informácií o kritickej infraštruktúre [6,7,8,10] vyplýva, že určitý významný objekt infraštruktúry bude zaradený ako prvok KI zvyčajne vtedy, ak je dôležitý pre niektorý zo sektorov významne ovplyvňujúcich bezpečnosť štátu.

Z pojmov a teoretických úvah o riešení problémov KI je zrejmé, že pre

- **definovanie exaktne podložených kritérií pre identifikáciu a kategorizáciu objektov významných infraštruktúr** za účelom objektívneho vymedzenia množiny prvkov kritickej infraštruktúry,
- **realizáciu procesu posudzovania rizík a kvantifikácie ich zraniteľnosti**, parametrov ich obmedzenej výkonnosti, citlivosti na zlyhanie iných infraštruktúr,
- **návrh postupov pre zaistenie ich funkčnosti, spoľahlivosti a ochrany** a pod.,

je nevyhnutné mať k dispozícii špecificky zameraných odborníkov s manažérskymi schopnosťami a technickými znalosťami v konkrétnom sektore KI. Takto vyškolení odborníci musia poznať problematiku KI v celej jej šírke a musia byť schopní navrhovať, realizovať a riadiť všetky procesy pre zaistenie bezpečnosti a ochrany určených prvkov KI. Za týmto účelom bol na FBI ŽU akreditovaný nový študijný program „Bezpečnosť a ochrana kritickej infraštruktúry“, ktorý je zameraný najmä na sektory energetika a doprava, ale obsahuje aj predmety zamerané na ďalšie sektory KI – najmä informačné a komunikačné technológie, voda, zdravotníctvo a pod., z ktorých vyplývajú dôležité povinnosti pre jednotlivé systémy krízového manažmentu.

3 CHARAKTERISTIKA A OBSAH ŠTUDIJNÉHO PROGRAMU

Jednou z oblastí vysokoškolského vzdelávania je aj oblasť bezpečnosti, resp. ochrany obyvateľstva a krízového riadenia. Je potrebné si uvedomiť, že ochrana obyvateľstva je mimo iného založená aj na princípe zaistenia bezpečnosti jednotlivca, komunity a zabezpečenie funkcie spoločnosti. [9]. V lete 2013 Akreditačná komisia – poradný orgán Vlády SR, potvrdila akreditáciu pre denné aj externé bakalárske a inžinierske študijné programy, zamerané na oblasť bezpečnosti a ochrany KI. V nadväznosti na to začal proces propagácie študijných programov a nasledujúcom v akademickom roku 2014/2015 bolo štúdium v bakalárskom programe otvorené. Predpokladá sa, že štúdium v inžinierskom stupni bude otvorené až od AR 2016/2017.

3.1 CHARAKTERISTIKA ODBORNÉHO PROFILU ABSOLVENTA

Na preukázanie predpokladaných znalostí a zručností absolventov študijného programu uvádzame podstatné časti z profilu absolventa inžinierskeho stupňa.

Absolventi 2. stupňa budú schopní identifikovať ohrozenia a zdroje rizík v spoločenských, hospodárskych, prírodných, technických a technologických procesoch, dokážu ich analyzovať a komplexne hodnotiť, ako aj navrhovať postupy, využitie a aplikáciu metód a spôsobov minimalizácie rizík. Majú vedomosti z teórie ochrany kritickej infraštruktúry s dôrazom na energetiku, dopravu a nutné základy z oblasti informačných a komunikačných technológií. Sú spôsobilí navrhovať a uskutočňovať preventívne opatrenia, monitorovať a analyzovať vývoj rizikových a krízových činiteľov, prípravu adekvátnej reakcie na vznikajúci krízový jav, riadenie kontinuity fungovania prvku KI a uskutočňovanie efektívnej obnovy systémov vo fáze ex post. Absolventi budú schopní prognózovať vývoj na konkrétnom úseku spoločenských, hospodárskych, prírodných alebo technických procesov, využívať optimalizačné metódy a ďalšie nástroje riadenia na zvýšenie účinnosti svojej práce. Budú zoznámení so štruktúrou verejnej správy, systémom riadenia bezpečnosti štátu a územných celkov vrátane územnej samosprávy.

Výber teoretických vedomostí = absolvent dokáže [11]

- hľadať nové riešenia a tvorivo ich uplatniť v praxi, účelne prispôsobovať zahraničné najlepšie skúsenosti na vlastné podmienky,
- pripraviť a realizovať tréningy osôb v pôsobnosti prvku kritickej infraštruktúry,
- uplatniť vlastné metodické postupy a využiť vlastnú tvorivú invenciu pri identifikovaní zdrojov rizík a ohrození v konkrétnom prostredí určeného prvku (príp. celého sektoru) kritickej infraštruktúry,
- vypracovať bezpečnostné plány a návrhy na organizačné a legislatívne oparenia pre konkrétny druh potenciálnych prvkov kritickej infraštruktúry.

Výber praktických schopností a zručností = absolvent je schopný [11]

- uplatňovať exaktné metódy riadenia v procesoch ochrany KI,
- využívať techniky a zaužívané metodické postupy na získavanie zodpovedajúcich informácií o stave bezpečnosti prvku kritickej infraštruktúry,
- riadiť podriadených s dôrazom na zložité podmienky riešenia krízových javov,
- pochopiť vývoj kontrolovaných dejov, procesov a činností a vyvodzovať závery,
- koncepčne navrhovať a riadiť preventívne opatrenia a minimalizovať predpoklady možných ohrození a zdrojov rizík.

2.2 ŠTRUKTÚRA A OBSAH ODPORÚČANÉHO ŠTUDIJNÉHO PLÁNU

Na zdokumentovanie obsahu 1. aj 2. stupňa študijného programu „Bezpečnosť a ochrana kritickej infraštruktúry“ uvádzame obsah tzv. *odporúčaného študijného plánu* pre denný bakalárky a denný inžiniersky stupeň štúdia.

Odporúčaný študijný plán pre bakalársky stupeň štúdia, denná forma [11]:

1. akademický rok

Predmet	Rozsah	Samostatná práca /h/	Typ	Katedra	Kredity
Zimný semester					
Povinné predmety					
9BD001 Inžinierska geometria	1 - 3 - 0	108	S	Mat	6
9BD002 Ekonómia	2 - 2 - 0	90	S	KM	5
9BD003 Matematika 1	2 - 3 - 0	126	S	Mat	7
9BD005 Informatika 1	1 - 0 - 1	54	S	TVI	3
Letný semester					
Povinné predmety					
9BD013 Fyzika	2 - 1 - 1	90	S	F	5
9BD014 Logistika	2 - 2 - 0	90	S	TVI	5
9BD015 Matematika 2	2 - 3 - 0	126	S	Mat	7
9BD016 Podniková ekonomika	2 - 2 - 0	90	S	KM	5
9BD017 Informatika 2	1 - 0 - 1	54	S	TVI	3
Celkové zaťaženie v akademickom roku 1674 h.					

2. akademický rok

Predmet	Rozsah	Samostatná práca /h/	Typ	Katedra	Kredity
Zimný semester					
Povinné predmety					
9BD023 Manažment	2 - 2 - 0	90	S	KM	5
9BD024 Základy mechaniky pevných telies	2 - 2 - 0	90	S	TVI	5
9BD025 Bezpečnosť a ochrana zdravia pri práci	2 - 2 - 0	90	S	TVI	5
9BD300 Energetická infraštruktúra	2 - 2 - 0	90	S	TVI	5
Letný semester					
Povinné predmety					
9BD035 Manažérska štatistika	2 - 2 - 0	90	S	KM	5
9BD034 Operačná analýza	2 - 2 - 0	90	S	TVI	5
9BD042 Dopravná infraštruktúra	2 - 2 - 0	72	S	TVI	4
9BD036 Manažment rizík	2 - 2 - 0	90	S	KM	5
9BD301 Výrobné zariadenia a technológie v energetike	2 - 2 - 0	90	S	TVI	5
Celkové zaťaženie v akademickom roku 1774 h.					

3. akademický rok

Predmet	Rozsah	Samostatná práca /h/	Typ	Katedra	Kredity
Zimný semester					
Povinné predmety					
9BD047 Právo	2 - 2 - 0	90	S	BM	5
9BD049 Základy mechaniky kvapalín a plynov	2 - 2 - 0	90	S	PI	5
9BD048 Krízový manažment vo verejnej správe	2 - 2 - 0	108	S	KM	6
9BD050 Ochrana kritickej infraštruktúry	2 - 2 - 0	90	S	TVI	5
9BD052 Dopravná technika a technológie	2 - 2 - 0	72	S	TVI	4
Letný semester					
Povinné predmety					
9BD303 Špeciálne prepravy	2 - 2 - 0	90	S	TVI	5
9BD304 Ochrana objektov kritickej infraštruktúry v sektore dopravy a energetiky	2 - 4 - 0	108	S	TVI	6
9BD306 Seminár k bakalárskej práci	0 - 1 - 0	36	H	TVI	2
9BD307 Obhajoba bakalárskej práce		144	S	TVI	8
9BD305 Odborná prax	40	36	H	TVI	2
Celkové zaťaženie v akademickom roku 1642 h.					

Odporúčaný študijný plán pre inžiniersky stupeň štúdia, denná forma [11]:

1. akademický rok

Predmet	Rozsah	Samostatná práca /h/	Typ	Katedra	Kredity
Zimný semester					
Povinné predmety					
9ID001 Stochastické metódy operačnej analýzy	2 - 2 - 0	90	S	TVI	5
9ID002 Psychológia	2 - 2 - 0	90	S	KM	5
9ID003 Manažérske informačné systémy	2 - 0 - 2	90	S	TVI	5
9ID005 Doprava v krízových situáciách	2 - 1 - 0	72	S	TVI	4
9ID007 Pozemné stavby	2 - 1 - 0	54	S	TVI	3
Letný semester					
Povinné predmety					
9ID012 Manažérske metódy a techniky	2 - 2 - 0	90	S	KM	5
9ID011 Krízový manažment	2 - 2 - 0	90	S	KM	5
9ID016 Dopravné stavby	2 - 2 - 0	90	S	TVI	5
9ID700 Evakuácia osôb, zvierat a vecí	2 - 2 - 0	72	S	TVI	4
9ID701 Riadiace a informačné systémy v kritickej infraštruktúre	2 - 1 - 0	72	S	TVI	4
9ID702 Odborná prax	40	36	H	TVI	2
Celkové zaťaženie v akademickom roku 1731 h.					

2. akademický rok

Predmet	Rozsah	Samostatná práca /h/	Typ	Katedra	Kredity
Zimný semester					
Povinné predmety					
9ID020 Prognózovanie a plánovanie	2 - 2 - 0	90	S	KM	5
9ID023 Riziká priemyselných procesov	2 - 2 - 0	90	S	KM	5
9ID705 Plánovanie ochrany kritickej infrašt.	2 - 1 - 1	90	S	KM	5
9ID706 Obnova pozemných stavieb	2 - 2 - 0	90	S	TVI	5
9ID707 Núdzové zásobovanie	2 - 2 - 0	90	S	TVI	5
Letný semester					
Povinné predmety					
9ID709 Manažment rizík kritickej infraštruk.	2 - 0 - 2	90	S	KM	5
9ID710 Projekt ochrany prvku kritickej infraštruktúry	1 - 0 - 2	72	S	TVI	4
9ID029 Manažment kvality	2 - 2 - 0	90	S	KM	5
9ID711 Seminár k diplomovej práci	0 - 1 - 0	36	H	TVI	2
9ID712 Obhajoba diplomovej práce		180	ŠS	TVI	10
Celkové zaťaženie v akademickom roku 1587 h.					

Medzi aktuálne problémy nového študijného programu je možné zaradiť najmä:

- dôsledky demografickej krízy (menej záujemcov o štúdium na VŠ),
- neznalosť pojmu kritická infraštruktúra a jeho obsahu v spoločnosti, dôsledkom ktorého je názov študijného programu pre záujemcov o štúdium veľkou neznámou,
- prvý študijný program so zameraním na problematiku KI v strednej a východnej Európe a preto chýbajú možnosti výmeny skúseností a odborníkov v tejto oblasti,
- potrebu budovania obsahu a formy nových profilových predmetov, najmä pre dôležité oblasti energetiky a IKT,
- chýbajúca odborná a praktická spolupráca s významnými energetickými subjektmi a ich odborníkmi pre otázky bezpečnosti a ochrany ich podnikovej infraštruktúry.

3 ZÁVER

Energetický a dopravný systém regiónu, štátu resp. celého európskeho priestoru je komplexná, vzájomne previazaná štruktúra, pozostávajúca z veľkého množstva infraštruktúr (energetické zariadenia, dopravné cesty, informačné systémy, terminály, prenosové sústavy apod.), ktorá má zásadný význam pre zabezpečenie životne dôležitých funkcií spoločnosti. Oblasti energetiky a dopravy sú preto považované za najvýznamnejšie sektory kritickej infraštruktúry vo väčšine vyspelých krajín sveta.

LITERATÚRA

[1] Zákon č.45/2011 Z. z. o kritickej infraštruktúre

[2] Smernica rady 2008/114/ES, z 8.12.2008 o identifikácii a označení európskych kritických infraštruktúr a zhodnotení potreby zlepšiť ich ochranu, In: Úradný vestník Európskej únie, L 345/75-82, zo dňa 23.12.2008.

[3] Council Decision on a Critical Infrastructure Warning Information Network (CIWIN). Dostupné na: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri= COM:2008: 0676: FIN:EN:PDF

[4] Boc, K., Vidriková, D., Figuli, L.: Security plan as a part of critical infrastructure protection. In: MEST journal [elektronický zdroj]. ISSN 2334-7058. Vol. 1, no. 2 (2013), s. 136-145. Dostupné na: http://mest.meste.org/MEST_2_2013/_13.pdf

[5] Hofreiter, L. a kol.: Ochrana objektov kritickej dopravnej infraštruktúry. 1.vyd., EDIS – vydavateľstvo ŽU v Žiline 2013. 238 s., ISBN 978-80-554-0803-3.

[6] Lusková, M.: Critical infrastructure protection in the European security research. In: Riešenie krízových situácií v špecifickom prostredí: 18. medzinárodná vedecká konferencia: 5.-6.6.2013, Žilina. ISBN 978-80-554-0700-5. s. 333-339.

[7] Sventeková, E., Čičmancová, S.: Risk assessment of rail transport. In: Transport means 2013 : proceedings of the 17th international conference : October 24-25, 2013, Kaunas University of Technology, Lithuania. ISSN 1822-296X. Kaunas: Kaunas University of Technology, 2013. S. 228-231.

[8] Šimák, L. a kol.: Ochrana kritickej infraštruktúry v sektore doprava. 1.vyd., EDIS - vydavateľstvo ŽU v Žiline, 2012, 180 s. ISBN 978-80-554-0625-1.

[9] Tomek, M.: Vybrané problémy vysokoškolské přípravy ochrany obyvatelstva a krizového řízení ve Slovenské republice. Mezinárodní workshop, Inovace a rozvoj výuky bezpečnosti se zaměřením na krizové řízení, Zlín: UTB, FLKŘ. 2014. ISBN 978-80-7454-336-4.

[10] Vidriková D., Boc, K.: Ochrana kritickej infraštruktúry. EDIS – vydavateľstvo Žilinskej univerzity v Žiline, 2013. ISBN 978-80-554-0654-1.

[11] Dokumentácia: študijný program Bezpečnosť a ochrana kritickej infraštruktúry, 2013, Fakulta špeciálneho inžinierstva, Žilinská univerzita v Žiline.

Príspevok vznikol za podpory grantovej agentúry VEGA prostredníctvom projektu VEGA č. 1/0240/15 a agentúry APVV na základe Zmluvy č. APVV-0471-10.

Článok recenzovali dvaja nezávislí recenzenti.