VÝSKUM NÁSTROJOV PRE RIADENIE BEZPEČNOSTI A OCHRANY KRITICKEJ INFRAŠTRUKTÚRY V SEKTORE DOPRAVY

Bohuš Leitner[1], Eva Sventeková [2]

ABSTRAKT

Neustále nové bezpečnostné hrozby, politické a ekonomické zmeny vo svete, ale aj dynamický rozvoj technológií prinášajú neustále nové formy bezpečnostných rizík. Problematiku bezpečnosti a ochrany tzv. kritickej infraštruktúry je nutné vnímať a riešiť komplexne, najmä kvôli vzájomnej prepojenosti významných infraštruktúrnych systémov. Rozvoj poznania v oblastiach manažérstva bezpečnosti najdôležitejších systémov a služieb modernej spoločnosti je stále aktuálny. Cieľom príspevku je stručná prezentácia chápania problematiky bezpečnosti dôležitých infraštruktúrnych sietí a charakteristika projektu s názvom „Procesný model riadenia bezpečnosti a ochrany kritickej infraštruktúry v sektore dopravy“, riešeného na FBI UNIZA.

Kľúčové slová: kritická infraštruktúra, bezpečnosť, ochrana, sektor dopravy, vedecký projekt.

ABSTRACT

New security threats, political and economic changes in the world, but also the dynamic development of technologies still bring new forms of security risks. Problems of critical infrastructure safety and protection should be viewed and solved in a complex, mainly due to the interconnectedness of major infrastructure systems. The development of knowledge in the areas of modern society systems and services safety management most important is still current. The aim of the paper is short presentation of the security issues of major infrastructure networks understanding and a short description of the project called "Process model of safety and protection of critical infrastructure in the transport sector", currently solved on the FBI UNIZA.

Key words: critical infrastructure, safety/security, protection, transportation, scientific project.

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. 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

ÚVOD

Bezpečnosť a adekvátna ochrana objektov a služieb tzv. kritickej infraštruktúry (KI) je neoddeliteľnou súčasťou zaistenia požadovanej úrovne bezpečnosti ľudskej spoločnosti a jej trvalo udržateľného rozvoja. Riešenie problematiky riadenia bezpečnosti a optimálnej ochrany KI je plne v kompetencii subjektov vlastniacich, príp. prevádzkujúcich jej jednotlivé prvky, ale aj určených inštitúcií verejného sektora a zložiek integrovaného záchranného systému.

V článku prezentovaný projekt VEGA je zameraný na výskum nástrojov a riešení pre zefektívnenie procesov riadenia bezpečnosti a ochrany KI, so špecifickým zameraním na sektor dopravy. Vychádza sa z toho, že vývojom nových, ale aj efektívnou modifikáciou už známych postupov, nástrojov a metód riadenia, je možné formulovať konzistentný a objektívny návod na aplikáciu manažmentu rizík pri realizácii efektívnych spôsobov riadenia bezpečnosti a ochrany potenciálnych prvkov KI v sektore dopravy. Hlavným výstupom projektu bude procesný model určený pre objektívne riadenie úrovne bezpečnosti a efektívnej ochrany prvkov dopravnej infraštruktúry. Model bude integrovať nástroje a procesy posudzovania a riadenia rizík ohrozujúcich funkčnosť a odolnosť určeného infraštruktúrneho systému s činnosťami a kompetenciami verejnej správy, ako aj vlastníkov / prevádzkovateľov prvkov systému.

1 RIADENIE BEZPEČNOSTI KRITICKEJ INFRAŠTRUKTÚRY

Otázky ochrany kritickej infraštruktúry sa začali významnejšie riešiť v roku 2001, kedy udalosti v USA poukázali na zraniteľnosť prvkov kritickej infraštruktúry a významnosť možných následkov ich narušenia na fungovanie spoločnosti. Začali sa formulovať prvé sofistikované návrhy pre určovanie množiny potenciálnych prvkov kritickej infraštruktúry (KI), zvýšenie úrovne ich odolnosti, skúmanie ich citlivosti na negatívne javy v iných sektoroch, ako aj opatrenia na zefektívnenie ich ochrany. Ohrozenie kľúčových objektov KI v dôsledku možných teroristických útokov, veľkých prírodných katastrof, technologických havárií, prípadne zastaranosti alebo nízkej miery ich inherentnej spoľahlivosti je vždy spojené s narušením zaužívaných postupov a štandardov v organizácii a stability fungovania spoločnosti (napr. straty na životoch a majetku, morálne škody, rozsiahle narušenie životného prostredia a pod.).

Snahou Európskej únie (ďalej iba EÚ) v strategickej oblasti zameranej na ochranu KI je predovšetkým zlepšenie spolupráce medzi krajinami európskeho priestoru a vytvorenie jednotného prístup k zásadným otázkam riadenia bezpečnosti dôležitej európskej infraštruktúry. Smernicou Rady Európy 2008/114/ES [1] bol definovaný pojem tzv. *Európskej kritickej infraštruktúry* (ďalej EKI), kde boli definované pravidlá pre identifikáciu a určovanie prvkov EKI a zaistenie ochrany najdôležitejších systémov a služieb európskeho významu .

Slovenská republika (ďalej SR) prijala zákonné normy [2] a opatrenia, vedúce k zvýrazneniu významu problematiky KI a zaisteniu požadovanej úrovne jej bezpečnosti

a ochrany. Podľa [2] je kritická infraštruktúra systém, ktorý sa člení na sektory a prvky. Prvky systému kritickej infraštruktúry (KI) tvoria objekty, zariadenia, služby a informačné systémy, ktorých narušenie alebo zničenie by malo závažné nepriaznivé dôsledky na uskutočňovanie hospodárskej a sociálnej funkcie štátu.

Pre správne pochopenie celej šírky oblastí kritickej infraštruktúry je vhodné uviesť zoznam tzv. **sektorov kritickej infraštruktúry**. Vo väčšine vyspelých krajín sú za hlavné sektory KI uvažované – ***energetika*** (výroba, prenos a distribúcia elektrickej energie, preprava a distribúcia zemného plynu, preprava a spracovanie ropy, výroba tepla a ťažba významných surovín), ***doprava*** (cestná, železničná, letecká, vodná), ***informačné a komunikačné technológie*** (siete, dátové centrá, riadiace a informačné systémy, nosiče dôležitých informácií a pod.). Medzi ďalšie životne dôležité oblasti patria *vodné hospodárstvo, potravinová bezpečnosť, zdravotníctvo finančný sektor* a ďalšie významné systémy a služby v spoločnosti.

Pre identifikáciu prvkov a efektívne riadenie bezpečnosti KI je nutné definovať nielen typy útokov aj s odhadom miery pravdepodobnosti ich vzniku, ale hlavne odhad (kvantifikácia) očakávaných dôsledkov. Vo všeobecnosti sa jedná o vplyvy:

- **Antropogénne** – negatívne javy vyvolané v dôsledku činnosti človeka (napr. teroristické útoky, hackerské útoky, priemyselné havárie, zlyhanie personálu a pod.

Medzi najpravdepodobnejšie antropogénne ohrozenia je možné zaradiť najmä priamy ozbrojený fyzický útok na cieľ uskutočnený ozbrojenými teroristickými skupinami, bombový útok – spravidla vykonaný jednotlivcom alebo malou skupinou. Ďalšou možnosťou je kybernetický útok, ktorý je zameraný na zničenie alebo ovládnutie počítačových systémov. Významným rizikom sú tzv. *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)“. Riešením ochrany voči vyššie uvedeným typom útokov a z nich vyplývajúcich bezpečnostných rizík sa autori článku zaoberali ako riešitelia výskumného projektu *APVV č.0471-10 s názvom „Ochrana kritickej infraštruktúry v sektore doprava“* [3].

- **Prírodné** – negatívne javy vyvolané v dôsledku prírodných procesov (napr. vplyvy tektonického charakteru, meteorologické riziká spojené s extrémnymi vplyvmi počasia, riziká spojené so svahovými pohybmi a pod.).

Medzi najpravdepodobnejšie typy prírodných ohrození je možné podľa [4] v podmienkach Európy zaradiť 14 prejavov extrémov počasia. Medzi najvýznamnejšie meteorologické vplyvy a ich dôsledky v podmienkach strednej Európy zaraďujeme: *extrémne zrážky, víchrice, riečne povodne, búrky z tepla, búrky s nadmerným výskytom bleskov, výdatné sneženie, snehové búrky, mrznúci dážď, extrémne vysoké teploty, lesné požiare, extrémne vysoké teploty.* Riešením bezpečnostných rizík a dopadov na spoločnosť vyplývajúcich z negatívneho vplyvu extrémnych meteorologických podmienok na fungovanie systémov a služieb KI sa na FBI UNIZA aktuálne zaoberá

skupina riešiteľov v rámci riešenia výskumného projektu FP7 – RAIN s názvom *„Analýza rizík infraštruktúrnych sietí vyvolaných extrémnym počasím“ [4]*.

V podmienkach SR nebola zatiaľ vytvorená všeobecne akceptovaná metodika pre objektivizáciu zaradenia prvkov jednotlivých infraštruktúrnych systémov (najmä v energetike, doprave a sektore informačno-komunikačných technológií) do množiny tzv. potenciálnych prvkov KI. Na riešení uvedenej problematiky autori aktuálne pracujú, a to prostredníctvom výskumných aktivít realizovaných v rámci projektu VEGA č.1/0240/15 s názvom *„Procesný model riadenia bezpečnosti a ochrany kritickej infraštruktúry v sektore dopravy“* [5].

Aktuálne v podmienkach SR absentuje aj exaktne definovaná metodika pre hodnotenie kritickosti dôležitých prvkov infraštruktúry a ich citlivosti na zlyhanie ďalších významných infraštruktúrnych systémov. Na riešení problematiky sa autori aktuálne podieľajú v rámci projektu „*RESILIENCE 2015 Dynamické hodnocení odolnosti souvztažných subsystémů kritické infrastruktury*“, riešeného v rámci Grantovej agentúry MV ČR [7].

Pojem **ochrana kritickej infraštruktúry** [2] predstavuje súbor opatrení, ktoré vlastník, alebo prevádzkovateľ objektu a určené jednotky integrovaného záchranného systému musia zabezpečiť s cieľom zaistiť požadovanú funkčnosť a výkonnosť dôležitej infraštruktúry. Cieľom systému ochrany kritickej infraštruktúry by mala byť predovšetkým minimalizácia vyradenia funkcie, činnosti alebo služby chráneného systému [3]. Základnými cieľmi ochrany objektov a služieb KI je hlavne:

- zamedziť prieniku do objektu a zabrániť činnosti nepovolaným osobám,
- znížiť alebo zabrániť vzniku bezpečnostného rizika (teroristického útoku, sabotáže, obmedzenie vplyvu extrémov počasia 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 pohľadu aktuálneho chápania problematiky, vychádzajúceho z európskeho [1] alebo národného právneho rámca [2], je nutné mať zadefinované určité minimálne požiadavky (bezpečnosť, spoľahlivosť, zraniteľnosť / odolnosť), konkretizované pre jednotlivé systémy a objekty vybraných prvkov KI.

Aby bol systém správy a ochrany KI uplatňovaný v podmienkach SR dostatočne účinný a efektívny musí akceptovať podmienky koncepcie Európskeho programu pre ochranu kritickej infraštruktúry a Smernice rady 2008/114/ES o určovaní a označovaní európskych kritických infraštruktúr a o posúdení potreby zvýšiť ich ochranu. Je pritom však nutné rešpektovať aj všetky právne, ekonomické, technické a technologické, prírodné a ďalšie špecifiká každej krajiny. Zodpovednosť za ochranu KI majú jednotlivé členské štáty a vlastníci / prevádzkovatelia systému alebo zariadenia každého významného infraštruktúrneho systému.

2 CHARAKTERISTIKA PROJEKTU VEGA Č.1/0240/15

Problematika kritickej infraštruktúry je v podmienkach SR aktuálne kodifikovaná v Zákone č.45/2011 Z.z. o kritickej infraštruktúre. Súčasné postupy uplatňované orgánmi verejnej správy SR, ako aj vlastníkmi a prevádzkovateľmi pri spravovaní a ochrane kritickej infraštruktúry sa ukazujú ako menej objektívne a efektívne. Je preto nutné permanentne hľadať efektívnejšie a účinnejšie opatrenia, ktoré zaistia nižšiu pravdepodobnosť vzniku krízových javov v infraštruktúrnom systéme a v prípade ich vzniku umožňujú minimalizovať negatívne dôsledky.

Riešitelia majú ambíciu riešiť predkladaný projekt v súlade s potrebami spoločnosti, využitím svojho odborného zamerania a výskumného potenciálu, ako aj s ohľadom na budovanie a rozvoj znalostnej základne pre akreditovaný študijný program „Bezpečnosť a ochrana kritickej infraštruktúry“. Zámyslom riešiteľov je rozšírenie oblasti výskumu spôsobov identifikácie, analýzy a hodnotenia relevantných aspektov v oblasti kritickej infraštruktúry, a to najmä posudzovania rizík, zaisťovania bezpečnosti a ochrany systémov a zariadení KI, optimalizáciu riadiacich a výkonných procesov pri zaisťovaní systému riadenia bezpečnosti KI a jej ochrany, ako aj informačnej podpory počas riešenia mimoriadnych a krízových situácií.

Riešený projekt má za cieľ integrovať poznanie z uvedených oblastí za účelom zvýšenia úrovne bezpečnosti a ochrany kritickej infraštruktúry, so špecifickým zameraním na sektor dopravy.

2.1 CIELE A PRÍNOSY PROJEKTU

Hlavný cieľ projektu: návrh štruktúry a vytvorenie hierarchického modelu riadiacich a výkonných procesov, realizovaných v rámci prevencie a ochrany dôležitých prvkov dopravnej infraštruktúry a overenie jeho objektívnosti. Model bude integrovať procesy posudzovania a riadenia rizík ohrozujúcich funkčnosť dôležitých objektov a služieb v sektore dopravy a procesy pre zaistenie optimálnej úrovne a efektívnosti ich ochrany.

Uvedený hlavný cieľ projektu bude postupne plnený realizáciou úloh:

- Stanovenie potrebných kritérií na výber a definovanie množiny relevantných prvkov KI pre jednotlivé podsektory v rámci sektora dopravy.
- Rámcový návrh štruktúry a spracovanie všeobecného procesného modelu, určeného na objektívne riadenie rizík v KI v sektore dopravy.
- Vytvorenie všeobecného hierarchického procesného modelu určeného pre objektívne riadenie úrovne bezpečnosti a ochrany prvkov KI, jeho aplikácia na vybrané objekty alebo služby v jednotlivých podsektoroch dopravy.

Očakávané výsledky projektu: rozšírenie základne teoretických poznatkov využiteľných pre tvorbu strategických a koncepčných materiálov na úseku zaistenia

bezpečnosti kritickej infraštruktúry na území SR, so špecifickým zameraním na problematiku riadenia bezpečnosti a ochrany najdôležitejšej dopravnej infraštruktúry.

Medzi najvýznamnejšie výstupy projektu patrí navrhnutý hierarchický model procesov realizovaných v rámci prevencie a ochrany najdôležitejších prvkov KI v sektore dopravy, ktorý bude integrovať procesy posudzovania a riadenia rizík, ohrozujúcich funkčnosť a výkonnosť potenciálnych prvkov KI s činnosťou a priradením kompetencií pre jednotlivé zložky verejnej správy, ale predovšetkým vlastníkov a prevádzkovateľov potenciálnych prvkov kritickej dopravnej infraštruktúry (ďalej iba KDI). Ďalšie očakávané teoretické výstupy z riešenia projektu budú tvorené údajmi, znalosťami a súvislosťami nevyhnutnými pre spracovanie relevantných plánovacích a riadiacich dokumentov, podporujúcich účinnú a efektívnu ochranu KI v riešených sektoroch.

Výstupy projektu budú prínosom pri rozvoji znalostného manažmentu v oblasti ochrane KI a vytvoria základy pre výskum a vývoj expertných systémov na podporu rozhodovania z hľadiska maximálnej efektívnosti prvej reakcie na narušenie funkčnosti KI spôsobené činnosťou človeka alebo prírodnými živlami.

Medzinárodná vedecká spolupráca: bude smerovaná predovšetkým na partnerské univerzitné a výskumné pracoviská, ako sú napr. Trinity College Dublin (Írsko), TU Delft (Holandsko), Freie Universitat Berlín (Nemecko), Univerzita dopravy Sofia (Bulharsko), Politechnika Swietokryzska Kielce (Poľsko), Vilnius Gediminas University (Litva), Kaunas University of Technology (Litva), ako aj ďalší partneri ako Jan Kochanowski University Kielce (Poľsko), Univerzita Pardubice (ČR), VŠB – TU Ostrava (ČR), Univerzita T. Bati Zlín (ČR) a Univerzita obrany Brno (ČR).

Očakávané výstupy projektu:

- Vytvorenie metodiky posudzovania zraniteľnosti kritickej infraštruktúry a posudzovania rizík vybraných subsystémov a služieb KI,
- Tvorbu modelov riadenia rizík a definovanie postupov vytvárania scenárov možných narušení prevádzkyschopnosti najdôležitejších prvkov KI v sektoroch energetika a doprava,
- Definovanie zásad a spôsobov ochrany prvkov kritickej infraštruktúry a postupov odstraňovania následkov narušenia jej funkčnosti vo vybraných typoch objektov KI v sektoroch dopravy a energetiky.

Používaný teoretický aparát:

Realizácia základného výskumu smeruje najmä k využitiu metód a princípov matematického aparátu viackriteriálneho rozhodovania (určovanie množiny prvkov KI), teórie grafov (charakteristika a optimalizácia náhrady líniových stavieb v doprave), sieťovej analýzy (pri tvorbe logických nadväzností v rámci procesného modelu riadenia bezpečnosti), systémovej analýzy (synergia pôsobenia rizikových činiteľov, citlivosť prvkov na zmeny v iných sektoroch KI, hodnotenie odolnosti KI a pod.), stochastické procesy a určovanie pravdepodobnosti / dôsledkov negatívneho

javu, teóriu stochastických dynamických systémov (stabilita systému, dynamika šírenia degradácie prvku, Domimo efekt a pod.).

2.2 PLÁNOVANÝ ČASOVÝ HARMONOGRAM RIEŠENIA

Pre úspešné splnenie hlavného cieľa projektu bude potrebné realizovať činnosti, metodicky a logicky, rozdelené do štyroch nadväzujúcich etáp:

1.etapa: 01/2015–12/2015 - vytvorenie predpokladov pre riešenie problému

Vymedzenie a špecifikácia riešeného problému a posúdenie aktuálneho stavu bezpečnosti spoločnosti vo vzťahu k ochrane kritickej infraštruktúry v sektore dopravy. Nosným výstupom aktivity je štúdia zameraná na posúdenie bezpečnostného prostredia vo vzťahu k ochrane KI. Realizované úlohy:

- Zmeny bezpečnostného prostredia v EÚ a SR a ich vplyv na funkčnosť KI.
- Požiadavky EÚ na funkčnosť a ochranu jednotlivých systémov, zariadení a služieb KI v rámci jednotlivých členských štátov.
- Analýza aktuálneho stavu v oblasti bezpečnosti a ochrany KI v SR.
- Význam a úloha kritickej infraštruktúry v sektore dopravy a definovanie základných požiadaviek na jej funkčnosť, odolnosť a efektívnu ochranu.
- Stanovenie kritérií na definovanie množiny potenciálnych prvkov KI v sektore dopravy.
- Spracovanie štúdie „Posúdenie aktuálnych problémov bezpečnosti a ochrany kritickej infraštruktúry“.

2.etapa: 1/2016–12/2016 - objektivizácia všeobecného modelu riadenia rizík v KI

Posudzovanie a riadenie rizík vybraných typov objektov KI v sektore doprava. Objektívne definovať ohrozenia, spôsoby pre posudzovanie rizík, ale najmä zásadné predpoklady pre tvorbu procesného modelu riadenia rizík KDI. Plánované úlohy:

- Návrh všeobecného modelu riadenia rizík v oblasti ochrany kritickej infraštruktúry v sektore doprava.
- Identifikácia rizík ohrozujúcich funkčnosť KI v sektore dopravy a jej jednotlivých subsystémov / prvkov.
- Postupy, metódy a techniky pre posudzovanie rizík, ohrozujúcich funkčnosť KDI.
- Návrh vhodných postupov a techník pre objektivizáciu procesov riadenia rizík pre najdôležitejšie druhy objektov KDI.

3.etapa 1/2017 – 12/2017 – pôsobnosť a väzby vo verejnej správe v súvislosti s riešením problematiky ochrany KDI.

Miesto, úlohy a pôsobnosť verejnej správy v súvislosti s riešením problematiky ochrany kritickej infraštruktúry. Plánované úlohy:

- Zhodnotenie súčasného stavu pôsobnosti orgánov verejnej správy SR v otázkach určovania a ochrany prvkov kritickej infraštruktúry.
- Legislatívny proces a stav implementácie záväzných dokumentov týkajúcich sa kritickej infraštruktúry vydávaných orgánmi EÚ v podmienkach SR.
- Konfrontácia dosiahnutej úrovne ochrany kritickej infraštruktúry v SR a vo vybratých krajinách EÚ.

- Integrácia sektoru dopravy s ostatnými sektormi kritickej infraštruktúry z pohľadu štátnej správy a samosprávy.

4.etapa 1/2018 – 12/2018 - vytvorenie, testovanie a verifikácia procesného modelu pre objektívne riadenie úrovne bezpečnosti prvkov KI v sektore dopravy.

V rámci aktivity je plánované riešenie nasledujúcich úloh:

- Definovanie účelu, funkcie a prioritných vlastností vytváraného procesného modelu pre riadenia rizík KDI.
- Vytvorenie hierarchického procesného modelu určeného pre objektívne riadenie úrovne bezpečnosti a ochrany prvkov KI v sektore doprava.
- Testovanie a verifikácia modelu určeného na objektivizované riadenie rizík vo vybraných podsektoroch KDI.
- Zhrnutie výsledkov, ich diskusia a vyslovenie záverov.

Zloženie riešiteľského kolektívu z pohľadu dĺžky pedagogickej a výskumnej praxe je vyvážené. Personálna matica projektu obsahuje viac skúsených a odborne spôsobilých riešiteľov, na strane druhej sú aktuálne medzi riešiteľmi 2 študenti doktorandského štúdia a 5 mladí pracovníci do 35 rokov. Riešiteľský kolektív tvoria riešitelia z viacerých pracovísk FBI UNIZA, ako aj ďalších fakúlt Žilinskej univerzity (FPEDAS a EF). Z iných rezortov sú v tíme dvaja odborníci z rezortu dopravy.

Metodologický aparát riešenia bude založený na využití štatistických nástrojov, optimalizačných postupov, metód operačnej a systémovej analýzy s cieľom objektivizovať vstupné údaje a hľadať optimálne riešenia problémov súvisiacich s bezpečnosťou a ochranou najdôležitejších systémov a služieb KDI.

Realizácia plánovaného výskumu smeruje najmä k matematického aparátu:

- viackriteriálneho rozhodovania (určovanie množiny prvkov KI),
- teórie grafov (charakteristika a optimalizácia náhrady líniových stavieb v doprave),
- sieťovej analýzy (pri tvorbe logických nadväzností v rámci procesného modelu riadenia bezpečnosti),
- systémovej analýzy (synergia pôsobenia rizikových činiteľov, citlivosť prvkov na zmeny v iných sektoroch KI, hodnotenie odolnosti KI a pod.),
- stochastických procesov
- teórie pravdepodobnosti (odhad frekvencie výskytu, príp. kvantifikácia následkov negatívneho javu),
- teórie stochastických dynamických systémov (stabilita systému, dynamika šírenia degradácie prvku, Domimo efekt a pod.).

ZÁVER

Zmeny bezpečnostného prostredia, turbulencie vo všetkých spoločenských dejoch a procesoch v súčasnom globalizovanom svete, nové možnosti moderných informačno-komunikačných technológií, ako aj nové sofistikované zariadenia a technológie výrazne napomáhajú rozvoju ľudskej spoločnosti, ale na strane druhej ju

neustále viac ohrozujú. Skúmanie súvislostí faktorov pokroku, synergickej podstaty možných ohrození, analyzovanie rizík, definovanie hraníc ich akceptovateľnosti, definovanie objektívnych scenárov rozvoja krízových javov, vytváranie nástrojov a súborov opatrení pre zníženie úrovne neakceptovateľných rizík sú aktuálnou úlohou súčasnej bezpečnostnej vedy.

Príspevok vznikol za podpory grantovej agentúry VEGA prostredníctvom riešenia projektu VEGA č. 1/0240/15.

LITERATÚRA

[1] 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.
[2] Zákon č.45/2011 Z.z. o kritickej infraštruktúre.
[3] Projekt APVV-0471-10 Ochrana kritickej infraštruktúry v sektore doprava. 2012 - 2014. Dostupné na: http://www2.fbi.uniza.sk/index.html.
[4] FP7 Project RAIN - Risk Analysis of Infrastructure Networks in Response to Extreme Weather. 2014 – 2017. Dostupné na: http://rain-project.eu/.
[5] Projekt VEGA č.1 /0240/15 – Procesný model riadenia bezpečnosti a ochrany kritickej infraštruktúry v sektore doprava. 2015 – 2018.
[6] Projekt MV ČR RESILIENCE2015 - Dynamické hodnocení odolnosti souvztažných sub-systémů kritické infrastruktury. 2015 – 2019. Dostupné na: http://www.tpeb.cz/blog/2015/10/21/projekt-evropskeho-rozmeru-resilience-2015