Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Technologické aspekty ochrany kritickej infraštruktúry SR

Dizertačná práca

Doktorand: Ing. Martin Hromada
Špecializácia: Inženýrská informatika

Školiteľ: doc. Ing. Luděk Lukáš, CSc.
Školiteľ špecialista brigádny generál doc. Ing. Miroslav Kelemen, PhD.

Zlín, 2011

POĎAKOVANIE

Rád by som poďakoval svojmu školiteľovi doc. Ing. Luďkovi Lukášovi, CSc. za odborné vedenie a cenné rady počas celého štúdia v rámci doktorského študijného programu. Ďalej by som chcel poďakovať brigádnemu generálovi doc. Ing. Miroslavovi Kelemenovi, PhD. za konzultácie, cenné pripomienky a možnosť využiť simulačné centrum Akadémie ozbrojených síl generála M. R. Štefánika v Liptovskom Mikuláši pri realizácii praktickej časti dizertačnej práce.

V neposlednej rade by som chcel poďakovať svojim rodičom, rodine, priateľke a blízkym za ich zhovievavosť, podporu a trpezlivosť, bez ktorej by bolo dokončenie dizertačnej práce nereálne.

ABSTRAKT

Ochrana kritickej infraštruktúry je v súčasnosti považovaná za prioritu zaistenia funkčnej kontinuity spoločnosti z ekonomického a sociálneho hľadiska. V tejto práci sú preto predstavené a popísané aktuálne prístupy k ochrane kritickej infraštruktúry v kontexte využitia technologických aspektov ochrany zameraných na systémy fyzickej ochrany.

Hlavným výsledkom práce je stanovenie štruktúry systému fyzickej ochrany prvku kritickej infraštruktúry, ktorá sa následne implementuje do metodiky hodnotenia systémov fyzickej ochrany z pohľadu prevádzkovateľa a sektoru kritickej infraštruktúry a je podporená verifikáciou výstupov pomocou informačnej podpory.

Prínos dizertačnej práce v teoretickej rovine spočíva v štúdiu a analýze aktuálnych požiadaviek v súvislosti s ochranou kritickej infraštruktúry. V praktickej rovine rieši absenciu prístupov k stanoveniu optimálnej štruktúry systémov fyzickej ochrany z pohľadu štrukturálnych a funkčných požiadaviek, použiteľných v predmetnej oblasti a zároveň absenciu metodiky pre hodnotenie spomínaných systémov.

Kľúčové slová:

Ochrana kritickej infraštruktúry, technologické aspekty ochrany kritickej infraštruktúry, systémy fyzickej ochrany, informačná podpora

ABSTRACT

Critical Infrastructure protection is presently considered as a priority to ensure vital societal functions from economical and social point of view. In this work there are presented approaches to Critical Infrastructure protection in the context of using the technological aspect of protection in relation to physical protection systems.

The main result of the work is determination of the structure of Critical Infrastructure component physical protection system, which is implemented into the methodology for physical protection system evaluation in connection with Critical Infrastructure operator and sector and it is supported by outputs verification by information support.

The contribution of the theoretical part of dissertation thesis is based on study and analysis of current requirements regarding the protection of Critical Infrastructure. In practical terms, it solves absence of determination of optimal physical protection system structural and functional requirements, applicable in this area and also the absence of methodology for evaluation the above-mentioned systems.

Key words:

Critical Infrastructure protection, technological aspect of Critical infrastructure protection, physical protection systems, information support,

OBSAH

1 ÚVOD

Súčasné bezpečnostné riziká vytvorili vo vyspelých štátoch potrebu definovania kritickej infraštruktúry (ďalej KI) ako takej oblasti infraštruktúry, ktorej narušenie či zničenie by vyvolalo závažné politické a hospodárske následky. Zabezpečenie ochrany dôležitých objektov národnej KI sa stalo objektívnou potrebou, vzhľadom na to, že k tradičným hrozbám, akými boli a sú katastrofy spôsobené prírodnými faktormi, ľudská nedbalosť, technologické a priemyselné havárie, vniknutia do počítačových systémov či organizovaná trestná činnosť, pribudli novodobé hrozby v podobe teroristických útokov. Veľa európskych krajín je považovaných za potenciálne ciele teroristických útokov, s prihliadnutím na skutočnosť, že európsky kontinent je jednou z oblastí pôsobenia teroristických skupín. Po teroristických útokoch v USA, v Španielsku a vo Veľkej Británii vzrástla nutnosť ochrany a obrany KI na nadnárodnej úrovni. Súčasne to prispelo k vytvoreniu inštitucionálnych, legislatívnych a organizačných nástrojov pre zabezpečenie ochrany a obrany KI, ktorá je strategický dôležitá pre fungovanie štátu a ktorej strata by mohla viesť k ohrozeniu života ľudí, k nezvratným, negatívnym, ekonomickým a sociálnym dosahom na spoločnosť a obyvateľov. V práci sa zameriam na ochranu kritickej infraštruktúry Slovenskej republiky z pohľadu využitia technologických aspektov.

2 SÚČASNÝ STAV PROBLEMATIKY OCHRANY KRITICKÉ INFRAŠTRUKTÚRY Z POHĽADU TECHNOLOGICKÝCH ASPEKTOV

2.1 Ochrana kritickej infraštruktúry - novodobý vývoj

Najvýznamnejším a zároveň aj najkritickejším historickým míľnikom ovplyvňujúcim vývoj problematiky KI a jej ochrany a obrany je 11. september 2001. Práve udalosti spojené s týmto dátumom prispeli k otvoreniu dialógu o potrebe ochrany a obrany dôležitých prvkov národnej infraštruktúry. Pred týmto dátumom sa predmetnej problematike venovali najviac USA a Austrália, ktoré si svojim spôsobom uvedomovali rozsah a zraniteľnosť KI. Je vhodné konštatovať, že ochrana KI nie je novodobý fenomén a bola zaisťovaná aj v minulosti no terminologicky sa táto skupina infraštruktúr neoznačovala súčasným pojmom.

2.1.1 NATO A USA

Prvým uceleným dokumentom, ktorý sa venoval rozoberanej problematike bola tzv. „Biela kniha“. Táto Smernica 63, bola vydaná v máji roku 1998 ako rozhodnutie prezidenta Billa Clintona (Presidential Decision Directive 63) [26]. Tento dokument vníma KI ako základné systémy, ktoré majú určitú hmotnú a kybernetickú základňu a majú vplyv na funkciu ekonomiky a štátu. Po útoku na WTC bolo 16. októbra 2001 vydané prezidentom Georgom W. Bushom „Vládne nariadenie na ochranu kritickej infraštruktúry“ [23], ktorého účelom bolo zabezpečiť ochranu a obranu informačných systémov KI, hmotných zariadení a zariadení, ktoré zabezpečovali funkciu ekonomiky, štátu a národnej obrany. Tvorbou ďalších dokumentov (dokument Plánovacieho výboru pre civilné núdzové plánovanie NATO (SCEPT) [3], Národná stratégia vnútornej bezpečnosti [24], Národná stratégia fyzickej ochrany kritickej infraštruktúry a kľúčových zariadení [27], Národná stratégia zabezpečenia kybernetického priestoru [25],) sa menila aj definícia a označenie KI. V súvislosti s týmito dokumentmi je KI vnímaná ako „systémy a zariadenia hmotné aj virtuálne, ktoré sú životne dôležité pre USA a zničenie či vyradenie z činnosti takýchto systémov alebo zariadení by malo vplyv na zníženie bezpečnosti, národnej ekonomickej bezpečnosti, národného verejného zdravia alebo bezpečia, alebo na akúkoľvek ich kombináciu“ [24]. Spomínané dokumenty sú len časťou legislatívnych nástrojov, ktoré upravujú KI ako takú. Ich množstvo poukazuje na význam KI pre spoločnosť a pre zachovanie jej funkčnej kontinuity. Pre zachovanie spomínanej kontinuity sú zodpovedné entity pripravené zasiahnuť aj do základných ľudských

práv aj napriek tomu, že v predmetnej problematike je vyzdvihovaný význam jednotlivca a jeho miesto v ochrane KI.

2.1.2 Európska Únia

Nie len spomínané udalosti, ale aj vývoj problematiky ochrany KI v USA a NATO prispel k vytváraniu rámca k ochrane KI v EU. Vznik ucelenej koncepcie KI a jej ochrany a obrany v rámci EU sa dá stanoviť na jún 2004, kedy na zasadaní Európskej rady bola požiadaná Európska Komisia o prípravu celkovej stratégie na ochranu KI následne na čo Komisia 20. septembra 2004 prijala správu „Ochrana kritickej infraštruktúry v boji proti terorizmu“ [15] v ktorej predložila návrhy na zlepšenie prevencie, pripravenosti a schopnosti reakcie na európskej úrovni na teroristické útoky zasahujúce KI. Táto správa stanovuje KI ako zariadenia a služby a informačné systémy, ktoré sú pre štáty životne dôležité, a ktorých zničenie alebo vyradenie z činnosti spôsobí oslabenie národnej bezpečnosti, národného hospodárstva, verejného zdravia a bezpečnosti a efektívneho fungovania vládneho systému.

Dokumentom, ktorý konkrétne rieši problematiku KI z pohľadu Európskej únie sa následne na to stala „Zelená kniha o európskom programe na ochranu kritickej infraštruktúry“[17], ktorá bola vydaná v Bruseli dňa 17. Novembra 2005. Cieľom tejto knihy je v podstate snaha o vytvorenie rámca pre spoluprácu väčšieho množstva subjektov, ktoré svojou činnosťou môžu prispieť k skvalitneniu ochrany KI. V Európskom programe pre ochranu kritickej infraštruktúry (ďalej len EPCIP) sa uvádza „Účinná ochrana kritickej infraštruktúry vyžaduje komunikáciu, koordináciu a spoluprácu ako na národnej úrovni tak na európskej úrovni a to medzi všetkými orgánmi, profesijnými organizáciami, vlastníkmi a prevádzkovateľmi kritickej infraštruktúry, rovnako tak na všetkých úrovniach štátnej a verejnej správy a tiež verejnosti“. Tento program by mal zaistiť aby v rámci EU existovala primeraná a rovnomerná úroveň ochrany a obrany kritickej infraštruktúry a aby sa znížila pravdepodobnosť zlyhania či aby existovali rýchle a overené nápravné opatrenia. V rámci tejto filozofie 8. decembra 2008 nadobudla platnosť „Smernica rady 2008/114/ES o identifikácii a označení európskych kritických infraštruktúr a zhodnotení potreby zlepšiť ich ochranu“ [16]. Tento dokument definuje „kritickú infraštruktúru“ ako zložku, systém alebo ich časť, nachádzajúca sa v členských štátoch, ktorá je nevyhnutná pre zachovanie základných funkcií spoločnosti, zdravia, ochrany, bezpečnosti, kvality života obyvateľov z ekonomického a sociálneho hľadiska, a ktorej narušenie alebo zničenie by malo závažné dôsledky v členskom štáte z dôvodu nemožnosti zachovať tieto funkcie. Následne na to je definovaný

pojem „európska kritická infraštruktúra“ alebo „ECI“ (European Critical Infrastructure) je kritická infraštruktúra nachádzajúca sa v členských štátoch ktorej narušenie alebo zničenie by malo závažné dôsledky minimálne v dvoch členských štátoch. Význam tohto dokumentu je hlavne v súvislosti so stanovením prierezových a sektorových kritérií pre sektory energetiky a dopravy, ktoré sú použiteľné aj v súvislosti s národnou KI, preto sa mu budem venovať aj ďalších častiach práce.

2.1.3 SLOVENSKO

Ochrana KI na Slovensku sa v minulosti vzťahovala na obrannú infraštruktúru v zmysle zákona č. 319/2002 Z. z. o obrane Slovenskej republiky v znení neskorších predpisov [22]. Obrannú infraštruktúru podľa citovaného zákona tvoria pozemky, stavby, budovy a zariadenia, telekomunikačné, energetické a dopravné systémy, informačné siete a zásoby štátnych hmotných rezerv, ktoré slúžia v čase vojny, vojnového stavu na zabezpečenie obrany štátu. Objekty obrannej infraštruktúry sa aj napriek skutočnosti, že spomínaný zákon dostatočne nepojednáva o ochrane a obrane KI považujú za prvky KI. Novodobý vývoj predmetnej problematiky na Slovensku sa dá spájať s rokom 2006, kedy bola prijatá Koncepcia kritickej infraštruktúry v Slovenskej republike a spôsob jej ochrany a obrany [18], ďalším významným dátumom je 14. február 2007, kedy na základe uznesenia vlády Slovenskej republiky č. 120 bol prijatý Národný program pre ochranu a obranu kritickej infraštruktúry v Slovenskej republike [19]. V súčasnosti sa ukončil proces tvorby legislatívneho nástroja týkajúceho sa predmetnej problematiky - zákon č. 45/2011 Zb. o kritickej infraštruktúre [21]. Vytvorenie tohto zákona je významným krokom v súvislosti s implementáciou Smernice 2008/114/ES. Spomínaným dokumentom sa budem venovať aj v ďalšej časti práce.

Význam vývoja a tvorby legislatívnych nástrojov je hlavne v súvislosti s optimalizovaním koordinácie a organizácie ochrany KI. Vzhľadom na vzájomnú prepojenosť a závislosť jednotlivých infraštruktúr je nevyhnutné vytvárať dokumenty, ktoré optimalizujú ochranu na čo najväčšom priestore. Súčasťou takejto optimalizácie je aj prijatie spoločných štandardov, pre vhodné a efektívne využívanie technologických aspektov ochrany kritických infraštruktúr a ich prvkov.

2.1.3.1 Sektory a prvky kritickej infraštruktúry

Význam aktuálnych dokumentov EU je hlavne v súvislosti s identifikovaním a označením KI pomocou už spomínanými kritérií. Napriek tomu, že sú tieto kritériá definované len pre sektor dopravy a energetiky existuje vymedzenie aj ďalších sektorov KI.

Podľa „zákona č. 45/2011 Zb. o kritickej infraštruktúre“ sa sektorom KI rozumie časť kritickej infraštruktúry, do ktorej sa zaraďujú prvky [21]. Je zrejmé, že najdôležitejšie prvky KI sa týkajú viacerých sektorov [15]. Ich zoznam podľa jednotlivých krajín uvádzam v tabuľke 1.

Sektory KI v USA	Sektory KI v EU	Sektory KI v SK
Poľnohospodárstvo, Potraviny, Voda, Zdravie obyvateľstva, Pohotovostné služby, Štátna správa, Obranný priemysel, Informačné a telekomunikačné systémy, Energia, Doprava, Bankovníctvo a financie, Chemický priemysel, Pošta a preprava zásielok,	Energetické zariadenia a siete, Komunikačné a informačné technológie, Financie, Zdravotníctvo, Potraviny, Voda, Doprava, Výroba, skladovanie a preprava nebezpečného tovaru, Štátna správa	Voda a atmosféra, Zdravotníctvo, Energetika, Elektronické komunikácie, Doprava, Priemysel, Pošta, Informačné a komunikačné technológie,

Tabuľka 1: Sektory kritickej infraštruktúry

Pre efektívne a optimálne riadenie ochrany KI je nevyhnutná identifikácia prvkov KI. Spôsob ich identifikácie a označenia je definovaný v spomínaných legislatívnych nástrojoch, ktoré vychádzajú z prierezových a sektorových kritérií definovaných už spomínanou smernicou. Vzhľadom na to, že spomínané kritériá sú utajované, môžeme len odhadovať zariadenia a subjekty, ktoré budú zaradené medzi prvky KI na Slovensku. Prehľad niektorých skupín prvkov je v tabuľke 2.

Sektor	**Prvky v rámci sektoru**
Voda a atmosféra	Významné vodné stavby, Vodné cesty , Monitorovacie zariadenia kvality zdrojov pitnej vody, Dispečerské zariadenia na distribúciu pitnej vody s ochranou dodávky pitnej vody
Zdravotníctvo	36 regionálnych úradov verejného zdravotníctva, 5 skladov mobilizačných rezerv, Operačné stredisko zdravotnej záchrannej služby Slovenskej republiky, osem operačných stredísk zdravotnej záchrannej služby pri koordinačných strediskách integrovaného záchranného systému, Národná transfúzna služba Slovenskej republiky,
Energetika	Tepelné elektrárne, Elektrárne s kombinovanou výrobou elektriny a tepla, Distribučné sústavy vrátane transformátorových staníc,

Elektronické komunikácie	Káblové vedenia, Prvky transportnej siete, Hlavné a záložné dáta centrá, Prvky dátovej siete, Objekty s prvkami transportnej dátovej a telefónnej siete, objekty managementu prvkov siete, Podporná infraštruktúra ako napájacie zdroje, bezpečnostné systémy a iné,
Doprava	Diaľnice, Rýchlostné cesty, Tunely, Významné mosty a Informačné káble, Technologické a technické komplexy riadenia dopravno - prepravného procesu, Významné železničné uzly , Železničné mosty a tunely, Sklady pohonných hmôt, Letiskové haly, či pohybové plochy letiska ako dráhy na vzlet a pristávanie, rolovacie dráhy a iná letisková infraštruktúra, Technické vybavenie letísk či prevádzkové budovy, Zradenia potrebné na navigáciu, Lietadlá a iné.
Priemysel	Spoločnosti v ktorých sa vyrábajú, skladujú či spracovávajú nebezpečné chemické látky a vlákna vrátane výroby, skladovania a spracovávania výbušnín, Prvky prepravy, zhodnotenia, znehodnotenia nebezpečných látok, Farmaceutické spoločnosti veľkého významu,
Pošta	Technologické a technické komplexy poštových služieb a iné.,

Tabuľka 2: Niektoré skupiny prvkov KI

Vývoj problematiky ochrany kritickej infraštruktúry je významným krokom k zaisteniu národnej bezpečnosti. Identifikovanie a označenie prvkov umožňuje zodpovedným autoritám využiť efektívne a optimálne opatrenia na zabezpečenie funkčnej kontinuity prvkov KI a tým funkčnej kontinuity spoločnosti. Je zrejmé, že identifikovanie národnej kritickej infraštruktúry je proces, ktorý vychádza zo stanovených prierezových a sektorových kritérií. Prístupmi k identifikácii a označení KI sa budem venovať v ďalšej časti práce, kde poukážem aj na nevyhnutnosť využívať technologické aspekty pri ochrane KI, pre ktoré je v už spomínaných dokumentoch vytvorený rámec.

2.2 Ochrana KI

2.2.1 Ochrana KI v EU

Organizáciu ochrany KI v EU pojmem ako analýzu jej najvýznamnejších a najaktuálnejších dokumentov. Jedná sa predovšetkým o Zelenú knihu o európskom programe na ochranu kritickej infraštruktúry, Oznámenie rade a európskemu parlamentu – Ochrana najdôležitejšej infraštruktúry v boji proti terorizmu a najaktuálnejší dokument Smernica rady 2008/114/ES o identifikácii a označení európskych kritických infraštruktúr a zhodnotení potreby zlepšiť ich ochranu, či manuál pre implementáciu tejto smernice. Keďže prvé dva dokumenty sú dlhodobejšie zaužívané a známe budem sa venovať spomínanej smernici o identifikácii a označení európskych kritických infraštruktúr (ďalej EKI) a zhodnotení potreby zlepšiť ich ochranu.

2.2.1.1 Smernica rady 2008/114/ES o identifikácii a označení európskych kritických infraštruktúr a zhodnotení potreby zlepšiť ich ochranu

Táto smernica predstavuje prvú etapu vo vzťahu k etapovitému prístupu k identifikácii a označení (EKI) a zhodnoteniu nevyhnutnosti zlepšiť jej ochranu. Smernica je zameraná na sektory energetiky a dopravy, s prihliadnutím na možnosť zaradenia ďalších sektorov, v závislosti na posúdení vplyvu tejto smernice. Dôležitým sa považuje identifikácia a označenie EKI na základe spoločného prístupu, ktorý by umožnil aj spoločné hodnotenie bezpečnostných požiadaviek, s akceptáciou špecifikácií jednotlivých sektorov. Na základe tejto smernice sa predpokladá so:

- Zavedením bezpečnostného plánu prevádzkovateľa (OSP – Operator Security Plan), ktorého súčasťou by bola identifikácia dôležitých zariadení, posúdenie rizika, identifikácia a výber protiopatrení či postupov,
- Určením styčného dôstojníka pre komunikáciu a spoluprácu s príslušnými orgánmi (SLO –Security Liason Officer),
- Identifikáciou rizík, hrozieb či zraniteľných miest v jednotlivých sektoroch, ktoré sú v rámci efektívnejšieho riadenia bezpečnosti zdieľané so zodpovednými orgánmi,
- Vytvorením európskych kontaktných bodov pre ochranu KI (ECIP contact points – European Critical Infrastructure Protection contact points).

Vo vzťahu k technologickým aspektom ochrany KI je najvýznamnejšou časťou smernice zavedenie bezpečnostného plánu prevádzkovateľa.

Bezpečnostné plány prevádzkovateľa

Bezpečnostné plány sú nástrojom zvyšujúcim bezpečnosť prvkov KI. Ich štruktúra a rozsah je formulovaný v prílohe II Smernice rady 2008/114/ES, ktorej sa budem venovať v inej časti textu. Prevádzkovatelia majú často vypracované bezpečnostné plány, ktoré sú ekvivalentom OSP, preto sa vo vzťahu k eliminácii duplicity ich zmena nevyžaduje pokiaľ sú tieto plány aktualizované. Absencia vypracovania OSP či ekvivalentu zaväzuje prevádzkovateľa aby túto absenciu vyriešil do roka od zaradenia do EKI.

Príloha II – Postup pri vypracovaní OSP pre EKI

Predmetom OSP je identifikácia zariadení KI a bezpečnostné riešenia, ktoré sa zavádzajú na ich ochranu. Postup pri vytváraní OSP - identifikácia dôležitých zariadení,

analýzy rizika na základe hlavných scenárov hrozieb, zraniteľných miest a možných následkov, výber a určenie optimálnych protiopatrení a postupov pričom sa rozlišuje medzi:

- Stálymi bezpečnostnými opatreniami, ktoré spresňujú investície a prostriedky nevyhnutné v oblasti bezpečnosti - prostriedky detekcie, kontroly prístupu, ochrany a vyrozumenia, postupy pre varovanie a krízové riadenie, kontrolné a overovacie opatrenia či bezpečnosť informačných systémov,
- Odstupňovanými bezpečnostnými opatreniami, ktoré sa môžu aktivovať v závislosti od rôznych úrovní rizika a hrozieb [16].

2.2.1.2 Manuál ku smernici na identifikáciu a označenie EKI

Vo vzťahu k manuálu sa budem venovať hlavne prierezovým kritériám, ktoré tento manuál konkretizuje. Ich existencia je nevyhnutná z pohľadu koncipovania sektorových a prierezových kritérií na národnej úrovni. Pri určovaní prierezových kritérií sa vychádza zo závažnosti následkov, ktoré narušenie alebo zničenie EKI spôsobí.

Kritérium strát na životoch

Na základe manuálu je množstvo mŕtvych a zranených v členskom štáte chápané ako významné ak:

- Potenciálne množstvo mŕtvych a zranených v členskom štáte vo vzťahu k strate činnosti danej EKI je vyššie ako stanovená horná hranica,
- V rámci smernice sa stanovili limity pre zranených – 5000 pričom 50% je v druhom členskom štáte a 500 mŕtvych, kde 50% je v druhom členskom štáte.

Kritérium hospodárskeho resp. ekonomického vplyvu

Ekonomické straty sú definované ako také straty, ktoré priamo vznikli v dôsledku narušenia funkčnosti EKI a sú postavené na vplyve narušenia na dynamiku rastu národných ekonomík. Tieto straty sa považujú za závažné, ak potenciálna ekonomická strata členského štátu v dôsledku narušenia danej EKI je vyššia ako stanovené hranica 500 miliónov Euro alebo 0,5% HDP.

- Potenciálna ekonomická strata členského štátu v dôsledku narušenia danej EKI je vyššia ako stanovená hranica 500 miliónov Euro alebo 0,5% HDP.

Ekonomické straty v dôsledku nedostupnosti služby či produktu

Za iniciačný bod sa považuje stav, kedy nefunkčnosť alebo zničenie prvku EKI má vplyv na dostupnosť služieb či produktov, kedy ich prípadná rozsiahla nedostupnosť negatívne vplýva na dodávateľské reťazce a ekonomickú stabilitu.

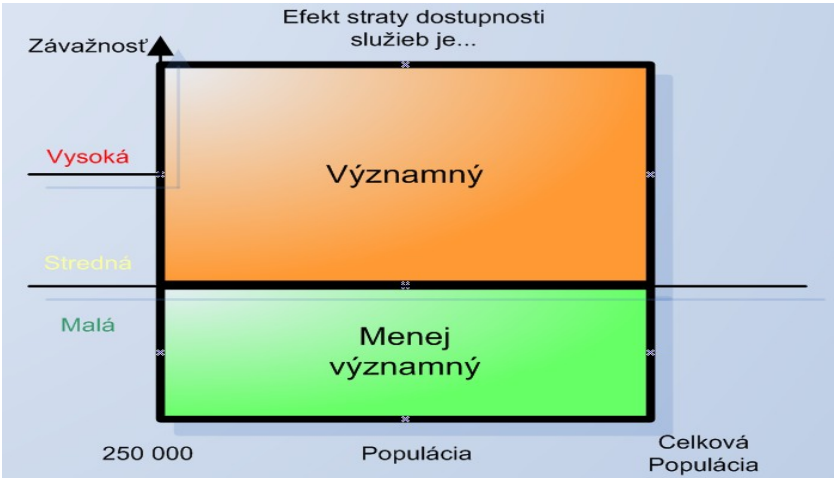
Environmentálne dopady

Pre potreby definovania environmentálnych dopadov sa hodnotia:

- Straty na krajine/pôde, ktoré sú formulované ako ekonomická hodnota krajiny/pôdy vyjadrená možným využitím danej krajiny resp. pôdy vo vzťahu k národným príjmom členských krajín,
- Vysťahované obyvateľstvo – kde sa posudzujú ekonomické náklady spojené s vysťahovaním obyvateľstva a ich vplyv na národnú ekonomiku.

Kritériu vplyvu na obyvateľstvo resp. verejnosť

Vplyv na obyvateľstvo sa posudzuje ako významný ak v členskom štáte v dôsledku narušenia alebo zničenia prvku EKI je hodnota vyjadrujúca množstvo zasiahnutého obyvateľstva v rámci fyzického utrpenia ako aj v rámci narušenia kvality každodenného života nad 250 000 obyvateľov viz. obr.1. [20]



Obrázok 1: Množstvo zasiahnutého obyvateľstva

Ochrana KI v EU je vnímaná hlavne v súvislosti s implementáciou spomínanej smernice do národných programov ochrany KI v členských štátov. Pre identifikáciu a označenie EKI boli vytvorené a formulované prierezové a sektorové kritériá, ktorých prínos je nie len v súvislosti s identifikáciou a o označením EKI, ale aj v súvislosti so stanovením prierezových a sektorových kritérií na identifikáciu a označenie národnej KI. Významným prvkom ochrany EKI je vypracovanie bezpečnostného plánu, ktorý poukazuje na nutnosť

využitia optimálnych protiopatrení a postupov, ktoré vytvárajú rámec pre vhodné použitie bezpečnostných opatrení, ktoré sú súčasťou technologických aspektov ochrany.

2.2.2 Ochrana KI na Slovensku

Ochrana KI patrí medzi priority zaistenia bezpečnosti Slovenskej republiky, preto je nevyhnutné venovať sa legislatívnym nástrojom, ktoré danú problematiku upravujú na národnej úrovni. Každý takýto nástroj by mal byť v súlade s európskymi normami.

Významnými dokumentmi mimo aktuálnej verzie zákona č. 45/2011 Zb. o kritickej infraštruktúre, súvisiacimi s ochranou KI na Slovensku sú najmä Národný program pre ochranu a obranu kritickej infraštruktúry v Slovenskej republike, Koncepcia kritickej infraštruktúry v Slovenskej republike a spôsob jej ochrany a obrany či súvisiace zákony č. 319/2002 Zb. o obrane Slovenskej republiky a č. 261/2002 Zb. o prevencii závažných priemyselných havárií, Národný akčný plán boja proti terorizmu, zákony č. 129/2002 Z.z. o IZS, č. 387/2002 Z.z. o riadení štátu v krízových situáciách mimo času vojny a vojnového stavu a iné. V tejto časti práce budem analyzovať spomínaný zákon o kritickej infraštruktúre a už existujúce dokumenty týkajúce sa predmetnej problematiky spomeniem len okrajovo vzhľadom na ich neaktuálnosť.

2.2.2.1 Zákon č. 45/2011 Zb. o kritickej infraštruktúre

Zákon č. 45/2011 Zb. o kritickej infraštruktúre (ďalej zákon o KI) upravuje postup zodpovedných orgánov pri identifikácii sektorov a prvkov KI a vytváraní predpokladov pre ich účinnú ochranu, úlohy orgánov štátnej správy, povinnosti fyzických osôb a právnických osôb pri zabezpečovaní ochrany KI či sankcie za porušenie týchto povinností.

Základné pojmy vychádzajú zo smernice o označení a identifikácii európskych kritických infraštruktúr – 2008/114/ES kde sú špecifikované pojmy európska kritická infraštruktúra, sektor KI a iné. Identifikácia KI sa na základe tohto zákona vykonáva uplatnením sektorových kritérií, ktoré budú stanovené pre každý sektor zodpovedným štátnym subjektom za daný sektor, s cieľom uskutočniť prvý výber prvkov KI, pričom následne sa aplikujú prierezové kritériá, ktoré vychádzajú a sú stanovené v manuáli pre implementáciu už spomínanej smernice. Riadenie ochrany KI riadi Ministerstvo vnútra SR pričom za ochranu KI zodpovedá prevádzkovateľ KI..

Významnou časťou zákona je formulovanie základných povinností prevádzkovateľov, ktorý na dosiahnutie zodpovedajúcej úrovne ochrany musia prijať všetky opatrenia potrebné na ochranu prvku KI a tým zaručiť funkčnosť, kontinuitu a integritu prvku KI a zaručiť

odvrátenie, zmiernenie alebo neutralizáciu identifikovaných hrozieb a rizík. Medzi významné aspekty vo vzťahu k povinnostiam prevádzkovateľa patria – vypracovanie a aktualizácia bezpečnostného plánu prevádzkovateľa (OSP), vymenovanie styčného úradníka pre bezpečnosť (SLO) či poskytnutie požadovaných informácii zodpovedným subjektom. Zákon o kritickej infraštruktúre formuluje požiadavky na styčného úradníka (dôstojníka) pre bezpečnosť či bezpečnostný plán prevádzkovateľa, ktorým som sa venoval pri rozbore spomínanej smernice.

Dôležitou časťou tohto zákona je riešenie financovania na zabezpečenie ochrany KI, ktoré bude riešené v rámci medzirezortného programu „kritickej infraštruktúry“, v ktorom budú stanovené priority, úlohy a opatrenia financované zo štátneho rozpočtu na zabezpečenie ochrany KI [21], je však potrebné konštatovať, že väčšiu časť nákladov na ochranu KI bude znášať prevádzkovateľ KI.

Zákon č. 45/2011 Zb. o KI vychádza zo spomínanej smernice a je nástrojom na implementáciu smernice o označení a identifikácii EKI a celého európskeho programu na ochranu KI (EPCIP). Z tohto legislatívneho procesu vyplynie aj vyhláška, ktorá bude upravovať prierezové a sektorové kritériá pre jednotlivé sektory.

Vo vzťahu k technologickým aspektom ochrany sa v rámci národného programu pre ochranu a obranu kritickej infraštruktúry považuje vymedzenie foriem ochrany ako využitie výstražných systémov (RAS), využitie EZS napojeného na PCO polície, integrovaný zabezpečovací systém v kombinácii s personálnou ochranou objektov čo sa chápe ako využitie, kvalifikovaného personálu, riadiacich centier, komunikačných a prenosových systémov v závislosti od stupňa ochrany, a iné [19].

Spomínaná koncepcia definuje v kapitole ciele ochrany a obrany prvkov KI, zásady ochrany a obrany prvkov, kde sa stanovujú aj orgány verejnej správy zodpovedné za ochranu, či nástroje ochrany a obrany prvkov KI, kde je ochrana a obrana rozdelená do segmentov (prevencia pred ohrozením, zníženie rizika ohrozenia existencie a stability prvku atď.), nástroje na prevenciu pred ohrozením (oddelenie vnútornej časti prvku KI od vonkajšieho prostredia, vyrozumenia orgánov verejnej správy a systém varovania obyvateľstva napojený na budovaný európsky varovný informačný systém, kontrolné a iné.), týmto nástrojom sa budem detailnejšie venovať v kapitole technologické aspekty ochrany KI SR

V zákone o KI je významný §10 ods. 2, v ktorom sa definujú bezpečnostné opatrenia, ktoré sú chápané ako bezpečnostné opatrenia na ochranu prvku sú najmä, mechanické

zábranné prostriedky, technické zabezpečovacie prostriedky, fyzická ochrana, režimové opatrenia a ich vzájomná kombinácia. V rámci medzirezortných stretnutí som odporúčal tento § doplniť o prostriedky pre bezpečnosť a ochranu technických a technologických zariadení a systémov, ktoré zohrávajú významnú úlohu v súvislosti s celkovou úrovňou ochrany prvku KI ako aj KI ako takej, viac sa im budem venovať v kapitole bezpečnostné opatrenia na ochranu prvku kritickej infraštruktúry**.**

2.3 Technologické aspekty ochrany kritickej infraštruktúry

V predošlých kapitolách som poukázal na významnosť KI a potrebu jej ochrany. Táto časť práce analyzuje prístupy k ochrane KI a pojednáva o možných faktoroch, ktoré úroveň ochrany priamo ovplyvňujú. Jedná sa o hrozby majúce vplyv na bezpečnosť a úroveň ochrany KI, stanovenie zraniteľnosti ako aj stanovenie odolnosti KI a jej prvkov. Posledné dva parametre priamo súvisia s bezpečnostnými opatreniami na ochranu prvku KI. Aktuálny stav využitia technologických aspektov ochrany KI z legislatívneho hľadiska je podrobený rozboru v časti technologické aspekty ochrany kritickej infraštruktúry v SR.

2.3.1 Hrozby majúce vplyv na bezpečnosť kritickej infraštruktúry

Použitie pojmu hrozba je často spájané s konkrétnym javom, procesom či udalosťou, ktorá svojou prítomnosťou vytvára nebezpečenstvo. Národná bezpečnostná stratégia USA vymedzuje hrozby ako environmentálne a zdravotné problémy, terorizmus, pašovanie drog, rozširovanie zbraní hromadného ničenia či iných potenciálne nebezpečných technológií [24].

Vplyv na bezpečnosť a funkčnosť KI môžu mať aj: dlhodobá inverzná situácia, povodne veľkého rozsahu, rozsiahle lesné požiare, snehová kalamita, víchrice, zosuvy pôdy resp. svahové pohyby, zemetrasenie, dlhotrvajúce teplo a sucho, epidémie, epifýtie, epizootie, radiačné havárie, havárie spôsobené chemickými látkami, technické havárie, narušenie hrádzí so vznikom umelo vyvolanej povodne, narušenie finančného a devízového hospodárstva, narušenie dodávky ropy a ropných produktov, narušenie dodávok elektrickej energie, terorizmus a iné [36]. Pre potreby tejto práce rozoberiem terorizmus a jeho prejavy, závažné priemyselné havárie či prírodné katastrofy.

2.3.1.1 Terorizmus

Existujú rôzne definície tohto pojmu, ktoré označujú terorizmus ako určitý súhrn neľudských spôsobov zastrašovania politických odporcov, štátnych zriadení či právnických a fyzických osôb. FBI (Federal Bureau of Investigation) definuje terorizmus ako „nezákonné

použitie sily a násilia proti osobám či majetku so zámerom zastrašiť alebo donútiť vládu, civilné obyvateľstvo či jeho určitú skupinu, k dosiahnutiu politických alebo spoločenských cieľov.“ [46]. Tento fenomén je možné rozdeliť podľa ideologickej príslušnosti (nacionalistický, revolučný, extrémizmu krajnej pravice, náboženský extrémizmus, jednoúčelové teroristické skupiny), či podľa oblasti pôsobenia (mestský, vidiecky, vnútroštátny, medzištátny).

Cieľom teroristického útoku je často len upútať pozornosť, môže sa jednať o určitú snahu zverejniť program teroristickej organizácie. V súčasnosti sa stretávame aj tzv. jednorazovým násilným aktom, ktorého cieľom je likvidácia osoby alebo osôb či zničenie konkrétneho objektu resp. objektov. Terorizmus predstavuje aj destabilizačný nástroj, ktorý chce vyprovokovať štátnu moc k represiám a násiliu či k samotnej revolučnej vzbure [47].

Z týchto definícií je zrejmé, že terorizmus v súčasnej dobe predstavuje jednu z najväčších hrozieb pre funkčnú kontinuitu KI a je zrejmé, že všetky aspekty ochrany KI budú vychádzať z rizika vzniku tejto hrozby.

2.3.1.2 Extrémizmus

Extrémizmus je termín, ktorým sa označuje jednanie či ideológia, na základe ktorej, určitá skupina ľudí, často selektovaná od spoločnosti, porušuje či neuznáva základné etické, právne či iné spoločenské princípy resp. štandardy, v spojení s verbálnou či fyzickou agresivitou, násilím motivovaným rasovou, národnostnou, náboženskou alebo sociálnou nenávisťou. Prejavmi extrémizmu bývajú radikalizmus, fanatizmus, fundamentalizmus, nacionalizmus, fašizmus, xenofóbia či rasizmus ako aj nátlakové akcie environmentálnych a ekologických aktivistov [42]. Čo sa týka vzťahu extrémizmu a KI resp. ekonomických a bezpečnostných záujmov štátu, ide hlavne o šírenie strachu a nedôvery v bezpečnostné zbory štátu, čo môže viesť až k frustrácii obyvateľstva smerujúcej k úplnej anarchii.

2.3.1.3 Šírenie zbraní hromadného ničenia

Jedná sa o šírenie zbraní, ktoré sú navrhnuté tak, aby boli schopné usmrtiť čo najväčšie množstvo ľudí alebo spôsobiť veľké materiálne škody. Sú určené k ničeniu vojenských ale aj civilných cieľov. Je možné ich rozdeliť na chemické zbrane (nervovoparalytické látky, pľuzgierotvorné látky, dusivé látky, psychoaktívne látky, zápalné látky), biologické zbrane (baktérie, vírusy, riketsie, nižšie huby, toxíny), jadrové zbrane (štepné jadrové zbrane (implozívne, hlavňové), termonukleárne jadrové zbrane)[40]. Zbrane hromadného ničenia boli v minulosti používané hlavne na demonštráciu moci v rozvojových štátnych zriadeniach, ktoré takýmto spôsobom získavali poddanosť a odovzdanosť určitých

etnických skupín (použitie chemických zbraní proti kurdským mestám počas občianskej vojny v Iraku). V dnešnej dobe znamenajú tieto zbrane skôr hrozbu vo vzťahu k teroristickým skupinám. Infikovanie vododistribučnej siete chemickými či rádioaktívnymi látkami by malo ďalekosiahle materiálne či zdravotné následky.

2.3.1.4 Organizovaný zločin

Organizovaný zločin je plánovitá činnosť smerujúca k dosiahnutiu zisku alebo moci formou krátkodobého či dlhodobého páchania závažného trestného činu či činov, pokiaľ sa tohto trestného činnú zúčastňujú aspoň dve osoby. Medzi formy organizovaného zločinu patrí výroba, pašovanie a distribúcia drog, organizovaná prostitúcia a obchod s ľuďmi, organizovaná nelegálna migrácia, pranie špinavých peňazí, vydieranie a vyberanie poplatkov za ochranu, korupcia, falšovanie, medzinárodný obchod zo zbraňami a výbušninami a iné. Organizovaný zločin výraznou mierou prispieva k spomaleniu ekonomického rastu krajiny, k znižovaniu sociálnej úrovne. Vytvára priestor na zníženie dôveryhodnosti verejných činiteľov čo môže následne vyústiť k protivládnym zhromaždeniam [32].

2.3.1.5 Závažné priemyselné havárie

Nehody, priemyselné havárie a iné nešťastia boli pred priemyselnou revolúciou spôsobené prevažne prírodnými katastrofami. V súčasnej dobe sú nebezpečenstvá omnoho ťažšie odhaliteľné a eliminovateľné, k čomu prispieva aj absencia predchádzajúcich skúseností, ktoré by nám mohli slúžiť ako zdroj potrebných informácií určených na zdokonaľovanie procesov. Závažné priemyselné havárie spôsobujú výrazné škody na majetku ľudských životoch či zdraví obyvateľstva. Na základe týchto znalostí a na základe skúseností s mimoriadnymi udalosťami (Radiačné havárie (USA, Harrisburg, Tree Mile Island, 1979) [30], Havárie spôsobené chemickými látkami (Taliansko, Seveso,1976), Technické havárie - požiare, explózie, deštrukcie budov (Anglicko, Flixborough, 1974 – explózia a požiar) [59], sú v súčasnej dobe prijaté prísne kritériá v prevádzkovaní potenciálne nebezpečných zariadení, zakotvené v legislatíve a v príslušných normách smerujúcich k efektívnejšej ochrane života či zdravia osôb, ochrane majetku a životného prostredia. Napriek týmto skutočnostiam je potrebné, aby boli tieto kritéria aktualizované v súlade s medzinárodnými dohodami a smernicami (hlavne Seveso II Directive [96/82/EC], Seveso Directive [82/501/EHS]).

2.3.1.6 Prírodné katastrofy

Či už v dôsledku klimatických zmien či iných prírodných faktorov, vznikajú prírodné katastrofy (povodne: Čína, Žltá rieka, 1887, 1931,1938) [45], zemetrasenia: Čína, Ťan-Šan,

1972, Nan-Šan, 1927 [43], sopečná činnosť: Indonézia, Tambora, 1815, Krakatoa, 1883, USA, Novarupta, 1912, Taliansko, Vesuv, 79 [48], lavíny: Rakúsko, Blonská lavína, 1954, Kanada, Saint-Jean-Vianney, 1971 [31], hurikány a extrémne sucho: štáty Afriky - Etiópia [33], rozsiahle požiare: Grécko,2007, Bradford,1985, Moskva, 1977, Kalifornia [35] a iné).

Tieto katastrofy často spôsobujú rozsiahle ekologické, sociálne, spoločenské ako aj ekonomické problémy, ktoré sú často len primárnym dopadom. Za katastrofu sa považuje mimoriadna udalosť, ktorá zasiahne najmenej päťdesiat ľudí. Intenzita je v mnohých prípadoch veľmi vysoká, preto aj prípadné preventívne opatrenia často zlyhávajú. Medzi sekundárne dopady patria hlave epidémie, epifýtie, epizootie, ako aj výskyt psychických porúch na zasiahnutom obyvateľstve.

Je zrejmé, že tieto vybrané negatívne faktory ovplyvňujúce funkčnosť KI sú len vybranými zástupcami celého spektra faktorov, ktoré priamo pôsobia na činnosť KI. Faktory, ktoré som v tejto časti podrobil rozboru by mohli mať však najzávažnejšie ekonomické a sociálne dopady, preto je vhodné sa im venovať v súvislosti s navrhovanými technologickými aspektmi ochrany KI.

2.3.2 Zraniteľnosť kritickej infraštruktúry

Zraniteľnosť je vnímaná ako náchylnosť k ujme, či stav kedy predmetná hodnota (aktívum) má slabiny, ktoré môžu spôsobiť jej poškodenie [39]. Na základe Amerického slovníka vojenských termínov (JP1-02) sa zraniteľnosť definuje:

- náchylnosť národov alebo vojenských síl k oslabeniu bojového potenciálu, bojovej účinnosti alebo vôle k boju prostredníctvom akýchkoľvek akcií a spôsobov,
- oslabenia charakteristických vlastností systému (neschopnosť plniť určené úlohy), ktorá je spôsobená pôsobením nepriateľského prostredia.

Zraniteľnosť je ďalej vnímaná ako súbor vlastností, ktoré môžu zoslabiť alebo obmedziť schopnosť systému poskytovať základné funkcie alebo služby v prípade vystavenia systému pôsobenia hrozby [7]. Vo vzťahu k existujúcim hrozbám, je zraniteľnosť podprocesov a rizikových elementov determinovaná mierou vplyvu a následkov zničenia. Čím sú tieto podprocesy a rizikové elementy zraniteľnejšie, tým je pôsobenie hrozby na produkt či služby infraštruktúry väčšie [34].

Z týchto definícií by sa následne dala vytvoriť definícia zraniteľnosti KI - zraniteľnosť KI môže byť chápaná ako miera citlivosti KI na hrozby a riziko ich vzniku v prostredí, v ktorom

sa vyžaduje jej fungovanie. Na základe tejto definície je zrejmé, že riziko vyplývajúce z hrozieb a jeho ohodnotenie v danom prostredí má významnú úlohu vo vzťahu k stanoveniu zraniteľnosti KI.

Riziko je obecne vnímané ako kombinácia pravdepodobností výskytu negatívnych javov (hrozieb) a ich dopadov (následkov) na systém (proces) [16]. Z toho vyplýva, že analýza rizík je významným aspektom ochrany KI a na základe Smernice 2008/114/ES [16] je definovaná ako zváženie relevantných scenárov hrozieb s cieľom posúdiť zraniteľné miesta a potenciálny vplyv narušenia alebo zničenia kritickej infraštruktúry. Napriek tomu, že nie sú stanovené metodiky na určenie miery rizika KI či jej prvku je zrejmé z tejto definície, že sú tu isté paralely s problematikou prevencie závažných priemyselných havárií. Vzhľadom na to, že problematika prevencie závažných priemyselných havárií je staršia, bol tu dostatočný priestor na vytvorenie nástrojov a metodík vo vzťahu k analýze rizika. Medzi najpoužívanejšie analýzy rizika patria:

- Bezpečnostná prehliadka – Safety Review – SR - Táto prehliadka má za cieľ identifikovať podmienky a okolnosti, ktoré môžu viesť k nehode a tým k následkom a ohrozeniu zdravia ľudí, poškodeniu životného prostredia alebo majetku [4],
- kontrolný zoznam - Checklist - CA - Kontrolné zoznamy sú deduktívne postupy odvodené od skúseností s predchádzajúcimi rizikami a poskytujú vhodné prostriedky pre rýchlu identifikáciu možných rizík. Majú často formu otázok alebo tém, ktoré je nevyhnutné zobrať do úvahy [34],
- analýza typu „What – if“ – W-I - Táto metóda je založená na brainstormingu, pri ktorom kvalifikovaný pracovný tým preveruje formou dotazov a odpovedí neočakávané udalosti, ktoré sa môžu v procese vyskytnúť [59],
- HAZOP analýza - sa používa pri vyhodnocovaní bezpečnosti zložitých zariadení. Identifikuje nebezpečné stavy a je charakteristická svojou náročnosťou. Často sa využíva aj pri vyhodnocovaní rôznych variant modifikácií v zariadení či ako nástroj slúžiaci na skúmanie havarijných situácií ktoré sa v minulosti vyskytli [38],

Medzi ďalšie metódy patria - Fault tree - strom porúch - FTA, Event tree - strom udalostí – ETA, analýza spôsobov a dôsledkov porúch – Failure Mode and Effects Analysis –FMEA, Analýza spoľahlivosti ľudského činiteľa (Human Reliability Analysis - HRA), analýza kvantitatívnych rizík procesu (Process Quantitative Risk Analysis - QRA) publikovaná

v „Purple Book“, metóda IAEA: TEC-DOC-727, metódy DOW: Fire & Explosion Index, Chemical Exposure Index a iné.

Všetky tieto analýzy stanovujú mieru rizika a sú obecne použiteľné aj vo vzťahu k analýze rizík KI.

Významným zdrojom rizík sú aj vzájomné interakcie prvkov KI, ktoré sa dajú rozdeliť na:

- Fyzické interakcie – jedná sa hlavne o materiálnu závislosť jednotlivých prvkov (materiálny výstup jedného prvku sa stáva materiálnym vstupom druhého),
- Územné interakcie – mimoriadna udalosť spôsobená jedným prvkom kritickej infraštruktúry môže pôsobiť na iný prvok kritickej infraštruktúry,
- Kybernetické interakcie – stav jedného prvku kritickej infraštruktúry závisí na informáciách z inej infraštruktúry.

Pre stanovenie a hodnotenie rizík zo vzájomnej interakcie by bolo možné použiť metódu IRAM [7] ktorá je vnímaná ako pravdepodobnostný model, ktorého cieľom je modelovanie vzájomných závislostí (interakcií) a prepojení a ktorý je rozdelený do nasledujúcich fáz:

- Identifikácie hrozieb a zraniteľností – umožňuje definovať prvky statické a dynamické, hierarchickú štruktúru systému, funkcie prvkov, subsystémov a systémov a iné,
- Modelovanie rizika – vytvárajú sa tu scenáre na základe stromu udalostí s cieľom špecifikovať možné dopady a následky,
- Stanovenie škôd a strát – vypočítavajú sa očakávané a extrémne škody a stanovuje sa index bezpečného stavu infraštruktúry,
- Riadenie opatrení – na základe využitia rozhodovacej analýzy sa stanovia alternatívy a úroveň prijateľnosti rizika.

Je dôležité si definované riziká ohodnotiť a stanoviť im určitú prioritu. Pre tieto účely sa využíva „Manažérska metóda pre stanovenie rizík a ich priorít“ [7], ktorá rozdeľuje riziká do nasledujúcich tried:

- Technické a technologické,
- Riziká rozhodovacích procesov,
- Riziká podporovateľnosti,
- Riziká nákladovosti,

- Riziká rozvrhovosti.

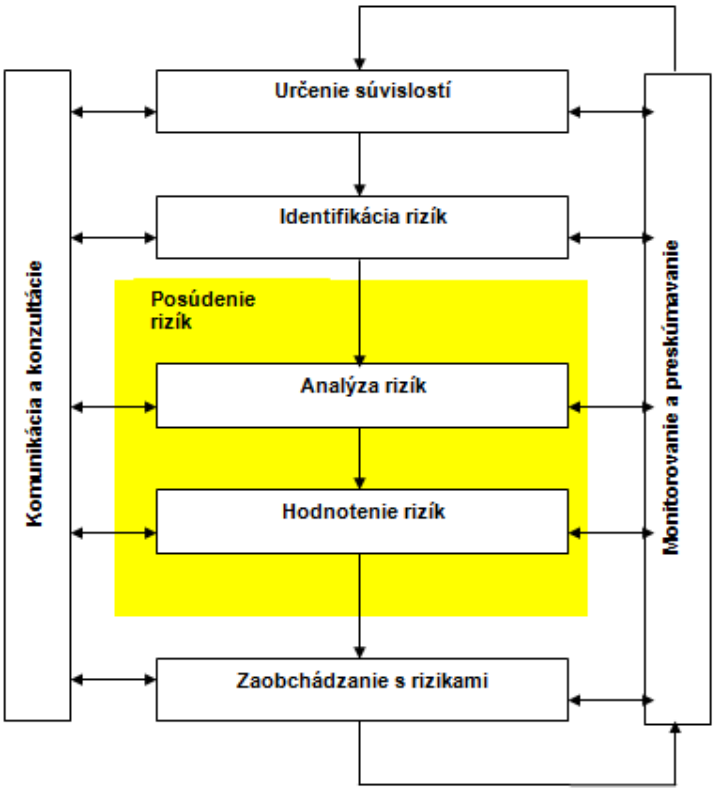
Následne táto metóda stanovuje kroky postupu:

- V prvotnej fáze sa stanovia rizikové faktory, ktoré zaradíme do tried, ktoré sú definované v predošlom bode,
- Pre každý rizikový faktor definovaný v prvotnej fáze sa určí pravdepodobnosť výskytu; spravidla sa používa trojstupňové odlíšenie (malá, stredná a veľká pravdepodobnosť výskytu),
- Určí sa dopad rizikových faktorov v rámci každej triedy rizík (malý, stredný, vážny),
- Určí sa celková pravdepodobnosť, ktorá je zaradená do určitej kategórie a riziká v rámci jednej triedy sa budú určovať ako kombinácia celkovej pravdepodobnosti a odhadnutého dopadu,
- Určí sa súhrnné riziko (nízke, mierne, vysoké) ako kombinácia celkovej pravdepodobnosti a dopadu (stanoveného expertným odhadom),

Vykonaná analýza veľkosti a závažnosti rizík nám vytvorí rámec pre určenie priority rizík a tým aj poradie činností vedúcich k eliminácii alebo k redukcii rizík.

Na základe predošlého textu je zrejmé, že celkové stanovenie rizika si bude vyžadovať kombináciu viacerých postupov a spôsobov hodnotenia rizika a následne jeho prioritizácia. Stanovenie hodnoty a popisu rizika nám umožňuje vzájomné porovnávanie rizikových udalostí [34]. Toto porovnávanie je významným prvkom pre ďalšie analýzy, ktoré by v konečnej fáze mali stanoviť vplyv rizikových udalostí na obyvateľstvo (počet zranených, počet mŕtvych), na ekonomické ukazovatele, či na kvalitu života obyvateľstva.

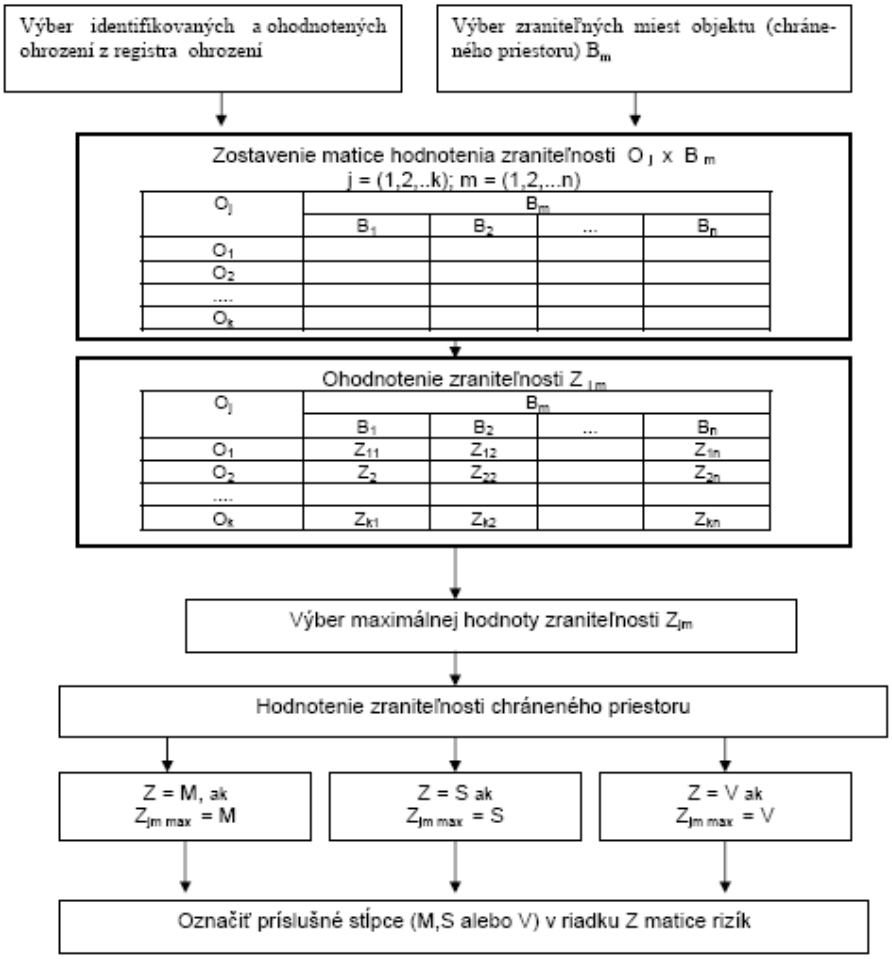
Ďalším vhodným prístupom k hodnoteniu rizík resp. manažérstvu rizika je implementácia štandardu pre manažment rizík STN 01 0380 resp. STN ISO 31000 (dátum vydania 1.4.2011) [58] do bezpečnostnej politiky prvku kritickej infraštruktúry. Význam tohto štandardu je hlavne v kontexte s formuláciou relevantnej terminológie v problematike manažmentu rizika na základe činnosti významných britských organizácii - The Institute of Risk Management (IRM), The Association of Insurance and Risk Managers (AIRMIC), The National Forum for Risk Management in the Public Sector (ALARM). Ďalším prínosom je stanovenie a formulovanie procesu manažmentu rizík z pohľadu činnosti organizácie. Hlavné procesné úkony manažérstva rizika na základe tohto štandardu sú zobrazené v obrázku 2.



Obrázok 2 Hlavné procesné úkony manažérstva rizika

Následne sú tieto procesné úkony detailne popísané a stanovujú konkrétne metódy pre stanovenie vzájomných súvislostí medzi entitami rizika, identifikáciu rizika či analýzu rizík, hodnotenie rizík či metódy zaobchádzania s rizikami. Dôležitým aspektom je určite a formulácia procesu manažérstva rizika či detailne rozpracovaný proces už spomínaného zaobchádzania s rizikami. Je nutné konštatovať, že proces manažmentu rizika prezentovaný a popísaný v tomto štandarde je použiteľný aj v kontexte s problematikou stanovenia zraniteľnosti prvku kritickej infraštruktúry.

Pre komplexné hodnotenie zraniteľnosti KI je potrebné využiť aj analýzy či postupy, ktoré budú vyjadrovať: akým spôsobom môžu byť časti objektu KI či prvky systému ochrany (bezpečnostného systému) prvku KI prekonané stanovenými a identifikovanými ohrozeniami, spôsoby akými môžu byť osoby (myslí sa tým zamestnanci, príslušníci FO) nápomocné pri narušení či útoku na prvok KI či spôsoby, ktoré môžu ochromiť požadované funkcie prvku KI. Medzi možné varianty by sa dala zaradiť metodika zobrazená na obr. 3 [37].



Obrázok 3: Hodnotenie zraniteľnosti

Ako je z diagramu zrejmé, v prvej fáze sa stanovuje vplyv jednotlivých hrozieb na všetky identifikované zraniteľné miesta, výsledkom čoho je stanovenie či ohodnotenie zraniteľnosti (O_i je vyjadrenie hrozby, B_i je vyjadrenie zraniteľného miesta objektu, Z_j je ohodnotenie celkovej zraniteľnosti, M,S,V je vydranie zraniteľnosti – malé, stredné, veľké). Po vykonaní hodnotenia zraniteľnosti v ďalšej fáze sa kategorizuje zraniteľnosť do skupín malej, strednej a vysokej zraniteľnosti. Je to jeden z možných spôsobov ako rozlíšiť a presne určiť zraniteľné miesta a ich význam z pohľadu zachovania funkčnosti KI. Z rozboru daných metodík je zrejmé, že stanovenie zraniteľnosti je významným aspektom celkovej ochrany KI a je mimoriadne dôležité venovať sa tvorbe metodík, ktoré budú použiteľné vo vzťahu ku KI, ktorá si svojou zložitosťou, previazanosťou a dôležitosťou vyžaduje osobitný prístup. Vhodným spôsobom by som odporúčal využiť softwarové nástroje (SVA-pro, Riskan), ktoré dopĺňajú rozoberané metodiky a tým vytvárajú rámec na minimalizáciu chýb v dôsledku prevádzkovej slepoty odborných pracovníkov.

2.3.3 Odolnosť kritickej infraštruktúry

Odolnosť je vnímaná ako vlastnosť systému prekonať (absorbovať) narušenie, znášať negatívne zmeny systému a pritom zabezpečiť základné (esenciálne) funkcie, štruktúru, identitu a spätnú väzbu systému[13]. Odolnosť je možné tiež vnímať ako schopnosť zaistiť funkciu systému, v podmienkach pôsobenia negatívnych vnútorných a vonkajších faktorov [14]. V súvislosti s definovaním pojmu odolnosť sa vyskytuje aj jej rozdelenie:

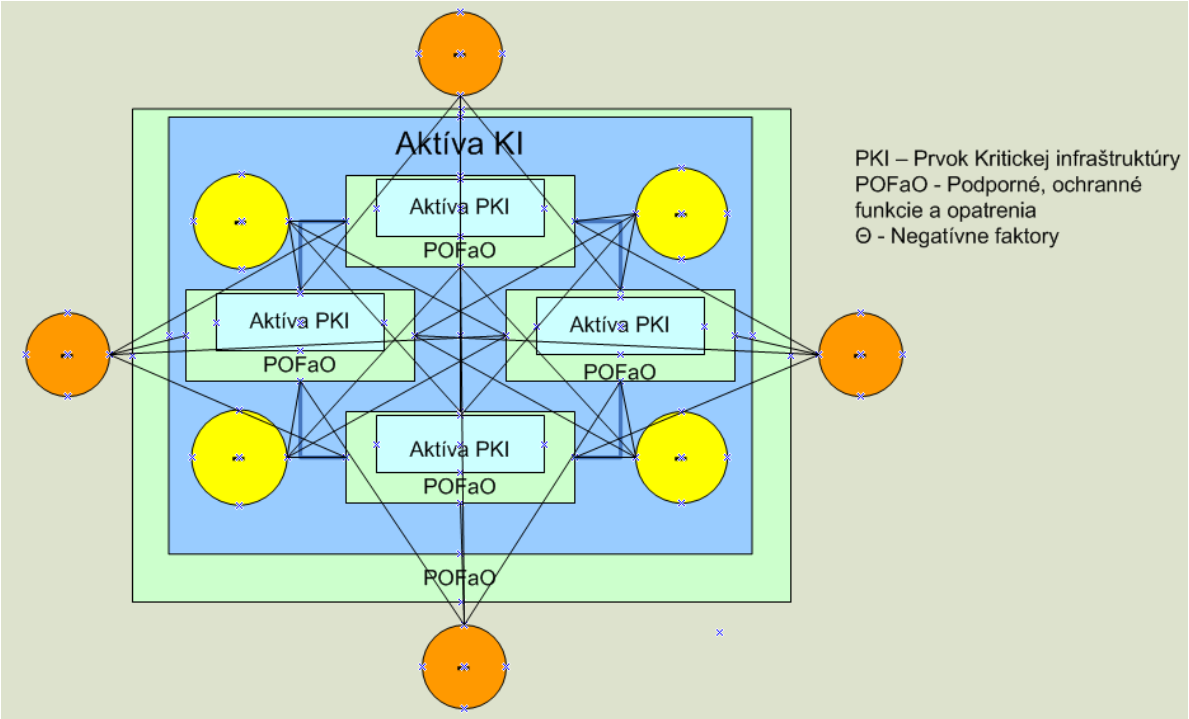
- Špeciálna resp. špecifická odolnosť je vnímaná ako prístup k pochopeniu a identifikovaniu tých systémových zmien, ktoré majú potenciálny vplyv na hranicu odolnosti systému, ktorej prekročenie znamená nechcené a nezmenné stavy systému,
- Všeobecná resp. generálna odolnosť je definovaná ako odolnosť hodnotiaca systém ako celok [49].

Z uvedených definícií je zrejmé, že stanovenie odolnosti je významným aspektom ochrany KI. Odolnosť KI či jej prvku vyjadruje vzájomné interakcie negatívnych vonkajších a vnútorných faktorov a bezpečnostných a ochranných opatrení. Významným krokom pri stanovení miery odolnosti je formulovanie jej ukazovateľov. Medzi tieto ukazovatele je možné zaradiť:

- Robustnosť - je definovaná ako vnútorná odolnosť systému voči vonkajším faktorom, pričom nedochádza k zmene funkčnosti systému. V rámci technických a organizačných aspektov sa jedná o dodržiavanie konštrukčných noriem a technologických postupov či využívanie krízového a núdzového plánovania. Významnou časťou robustnosti sú aj bezpečnostné opatrenia na ochranu prvku v súvislosti s fyzickou ochranou, ako aj prostriedky bezpečnosti a ochrany technických a technologických zariadení a systémov,
- Redundancia – je vnímaná ako vlastnosť systému využiť alternatívne voľby a zdroje v rámci riešenia porúch a bezpečnostných incidentov. V súvislosti s technickými a organizačnými nástrojmi sa uvažuje o technických náhradách a zdrojoch či o alternatívnych miestach pre riadenie záchranných a likvidačných prác,
- Reakcieschopnosť – schopnosť mobilizovať a využiť dostupné zdroje a prostriedky v prípade mimoriadnej udalosti či stavu. Podmienkou je dostupnosť zdrojov a materiálov pre záchranné a likvidačné práce či obnovu systému ako aj schopnosť určitej improvizácie či schopnosť využitia inovatívnych postupov.

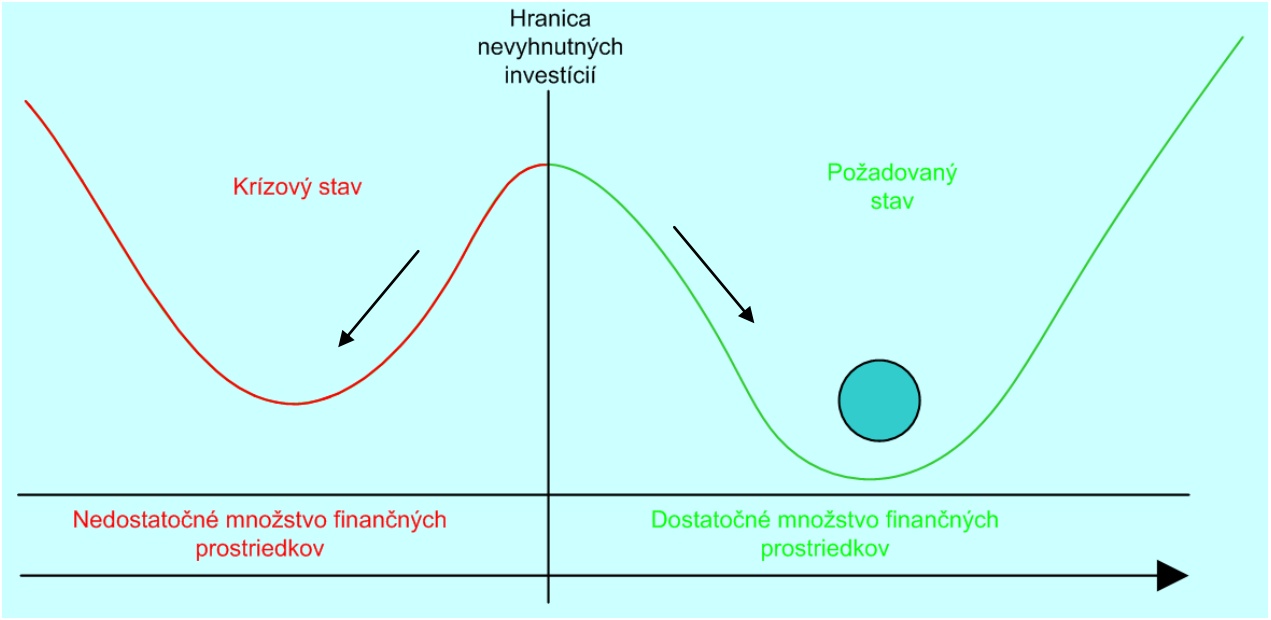
Je nutné poznamenať, že zložitosť systému akým KI bezpochyby je, vytvára rámec pre multikriteriálne hodnotenie odolnosti KI. Je zložité formulovať jednotlivé kritéria či ukazovatele, ktoré by objektívnym spôsobom vyjadrili mieru odolnosti prvku KI a následne hodnotu odolnosti KI ako takej. Práve v tejto súvislosti by sa mal využiť princíp, ktorý by umožnil stanoviť špeciálnu resp. špecifickú odolnosť, ktorá by odrážala hodnotu či mieru odolnosti prvku KI a následne generálnu či všeobecnú odolnosť v rámci KI ako celku. Medzi odporúčané spôsoby stanovenia či hodnotenia úrovne resp. miery odolnosti je využitie analýzy odolnosti, ktorá bude koncipovaná v nasledujúcich krokoch:

- Definovanie aktív prvku KI – umožní vyhľadať a stanoviť aktíva daného prvku a úroveň bezpečnostných opatrení, ktoré so svojimi podpornými a ochrannými funkciami vplývajú na celkovú hodnotu odolnosti, môže to byť chápané ako stanovenie tzv. špecializovanej odolnosti [7],
- Definovanie aktív KI ako celku – v rámci tohto kroku je možné využitie sieťových analýz či operačného výskumu, ktorého výstupom je identifikovanie a stanovenie KI, kritických funkcií systému či kritických uzlov systému. Následne sa identifikujú a označia spôsoby ochrany týchto kritických častí systému, môže byť chápané ako generálna odolnosť,
- Identifikovanie a označenie negatívnych vonkajších a vnútorných faktorov (hrozieb) – jedná sa o vytvorenie databázy ohrození, ktoré majú potenciál vyvolať resp. spôsobiť zlyhanie či narušenie činnosti KI. Je vhodné vytvoriť takúto databázu pre každý jeden prvok KI,
- Využitie analýzy zraniteľnosti a analýzy rizík – ide tu predovšetkým o stanovenie a určenie podmienok zraniteľnosti ich vzájomné súvislosti, vytvorenie databázy zraniteľností prvkov či celej infraštruktúry, ako aj stanovenie miery rizika, či pravdepodobnosti zlyhania systému či porúch,
- Využitie modelovacích nástrojov pre vyjadrenie škôd – vhodné pre stanovenie rozsahu škôd, pre vyjadrenie možného zhoršenia základných funkcií KI v súvislosti s poškodením jedného alebo viacerých prvkov ako aj ich podporných a ochranných prostriedkov či funkcií (viz. obr. 4).



Obrázok 4: Vyjadrenie vzájomných interakcií medzi negatívnymi faktormi, prvkami kritickej infraštruktúry a podpornými, ochrannými funkciami a opatreniami (zdroj: autor)

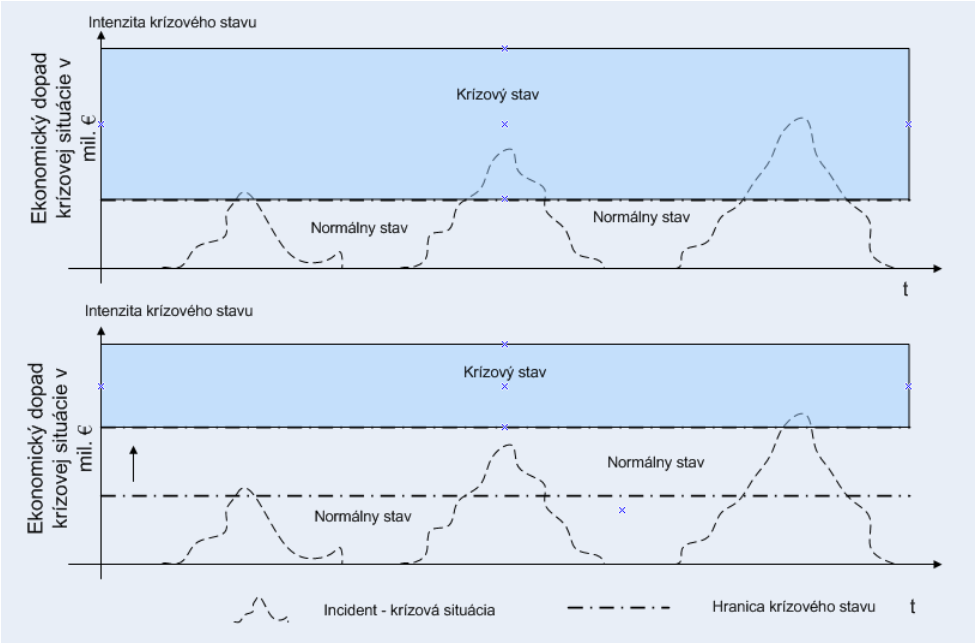
V predošlých častiach som sa venoval definíciám odolnosti a analýze možných prístupov hodnotenia odolnosti. Z môjho pohľadu je jedným z najvýznamnejších ukazovateľov odolnosti práve miera robustnosti jednotlivých prvkov, ktorá najvýraznejším spôsobom posúva hodnotu odolnosti. Je zrejmé, že miera robustnosti bude priamo závislá a úmerná veľkosti vynaložených finančných prostriedkov do tohto ukazovateľa. Pre lepšie chápanie daného tvrdenia je možné využiť metódy, ktoré nám definujú jednotlivé stavy v ktorých sa prvok KI nachádza a hraničné hodnoty, ktoré vyjadrujú zlomový bod medzi normálnym stavom a krízovým. Definovanie stavov nám pomôže pochopiť okolnosti, ktoré vedú k prechodu z jedného stavu do druhého a význam investovaných prostriedkov v tomto procese obr.5.



Obrázok 5: Miera investovaných finančných prostriedkov a jej vplyv na celkovú robustnosť a odolnosť systému (zdroj: autor)

Z obrázku (obr. 5) je možné vysledovať, že hranica nevyhnutných investícií je určitou prelomovou hranicou medzi požadovaným stavom a krízovým stavom. Jednotlivé zakrivenia krivky vyjadrujú správanie sa systému (modrý kruh) v prípade mimoriadnej udalosti. Množstvo investovaných prostriedkov do robustnosti a tým pádom do odolnosti systému nám aj z bodu blízkemu hranici nevyhnutných investícií dokáže systém vrátiť do požadovaného stavu čo vyjadruje šípka v pravej časti obrázku. Tým sa vyjadruje určitá pružnosť systému a jeho schopnosť odolávať negatívnym faktorom. Na druhej strane, pokiaľ sme v stave nedostatočného množstva finančných prostriedkov, systém sa stále vracia do krízového stavu, až kým miera investícií do robustnosti neprekročí definovanú hranicu nevyhnutných investícií [41].

Ďalšou možnosťou ako vyjadriť nevyhnutnosť investícií do robustnosti systému je stanovenie či vyjadrenie hraničných hodnôt, ktoré sa menia v závislosti od už spomínanej robustnosti obr. 6.



Obrázok 6: Stanovenie hraničných hodnôt odolnosti systému (zdroj: autor)

Z predchádzajúceho grafu je zrejmé, že hodnota odolnosti systému v dôsledku nedostatočných investícií do robustnosti je na nízkej úrovni, čo spôsobuje citlivosť a zraniteľnosť systému aj na krízové situácie malej intenzity. V druhom prípade sa nám v dôsledku investícií do robustnosti posunula hranica krízového stavu, z čoho vyplýva aj väčšia odolnosť systému a zníženie jeho citlivosti na krízové stavy [34].

Z daných grafov je zrejmé, že využívanie dostatočných investičných prostriedkov na bezpečnostné opatrenia pre ochranu prvku v súvislosti s fyzickou ochranou, ako aj prostriedky bezpečnosti a ochrany technických a technologických zariadení a systémov je významným aspektom zvyšovania robustnosti a tým aj odolnosti či ochrany KI ako takej. Dostupnosť dostatočných investičných prostriedkov by mala byť nie len v gescii prevádzkovateľov, ale aj štátu, ktorý je na funkcii KI priamo závislí.

2.3.4 Bezpečnostné opatrenia na ochranu prvku kritickej infraštruktúry

Využívanie bezpečnostných opatrení na ochranu prvkov KI patrí medzi najdôležitejšie aspekty ochrany kritickej infraštruktúry, čo vyplynulo aj s predošlých kapitol. Rozmanitosť týchto opatrení a možnosť ich využitia má rovnako progresívny charakter ako zvyšujúca sa zložitosť zariadení a systémov. Práve spomínaná zložitosť systémov si vyžaduje ich efektívne kombinovanie a využívanie. Spomínané prostriedky ochrany je možné rozdeliť do týchto skupín:

- Bezpečnostné opatrenia pre ochranu prvku v súvislosti s fyzickou a objektovou ochranou,

- Prostriedky bezpečnosti a ochrany technických a technologických zariadení a systémov.

Bezpečnostné opatrenia pre ochranu prvku v súvislosti s fyzickou a objektovou ochranou je možné rozdeliť na:

- Mechanické zábranné systémy – sú definované ako systémy alebo zariadenia, ktoré slúžia na fyzické zabránenie či sťaženie prístupu nepovolaným osobám. Medzi tieto systémy je možné zaradiť:
  - prostriedky obvodovej ochrany (pevné bariéry, ploty, vrcholové zábrany, brány, závory, turnikety, bezpečnostné priepuste a iné),
  - prostriedky plášťovej ochrany (mreže, rolety, fólie, žalúzie, bezpečnostné sklá, okná, dvere, zárubne, steny, zámky, zámkové vložky, petlice, visacie zámky a iné),
  - prostriedky predmetovej ochrany (komorové trezory, komerčné úschovné objekty a iné).
- Technické zabezpečovacie prostriedky – predstavujú zariadenia alebo systémy informujúce o stave a narušení objektu či objektov alebo chránených priestorov. Za technické zabezpečovacie prostriedky je možné považovať:
  - systémy na kontrolu vstupu,
  - poplachové systémy na hlásenie narušenia,
  - kamerové systémy v rámci uzatvoreného televízneho okruhu,
  - elektrická požiarna signalizácia,
  - zariadenia na detekciu látok a predmetov,
  - zariadenia proti aktívnemu a pasívnemu odpočúvaniu,
  - zariadenia fyzického ničenia nosičov informácií,
  - tiesňové systémy.
- Fyzickú ostrahu – jedná sa o ochranu objektu a chráneného priestoru, ktorá môže byť vykonávaná príslušníkmi ozbrojených bezpečnostných zborov, ozbrojených síl Slovenskej republiky, trvalo prítomnými ozbrojenými vlastnými zamestnancami či miestnou nepretržitou ochranou. V súvislosti so slovenskou terminológiou sa pojem fyzická ostraha nepoužíva a je nahradený pojmom fyzická ochrana no v súvislosti s implementáciou výstupov z diz. práce vyplývajúcich do prostredia ČR budem používať názov ostraha.

- Režimové opatrenia – sú opatrenia, ktoré určujú podmienky vstupu, pohybu osôb, automobilov či postupy v prípade mimoriadnej udalosti ako aj podmienky manipulácie s mechanickými zábrannými systémami či technickými zabezpečovacími prostriedkami a iné [37].

Prostriedky bezpečnosti a ochrany technických a technologických zariadení a systémov sú využívané hlavne v súvislosti s ochranou prevádzok majúcich potenciál spôsobiť závažnú priemyselnú haváriu či inú rozsiahlu udalosť. Táto problematika je rozsiahla a je významným aspektom bezpečnosti a ochrany zdravia pri práci, preto sa budem venovať len vybraným systémom a zariadenia na to určeným. Medzi tieto zariadenie je možné zaradiť:

- Zariadenia na ochranu pred explóziou:
  - preventívne zariadenia (obmedzujúce množstvo paliva, obmedzujúce množstvo oxydantov, na potlačovanie zdrojov zapálenia, na klasifikáciu zón explozívneho prostredia a iné.),
  - zariadenia a prostriedky na ochranu pred účinkami explózie (používanie materiálov odolných proti tlaku, zabránenie inštalácie ventilov na ventiláciu tlaku, inštalácia prostriedkov, ktoré hlásia plamene explózie okamžite, využitie zachycovačov plameňov alebo izolačných ventilov a iné),
- Zariadenia pre efektívne skladovanie a manipuláciu s nebezpečnými látkami:
  - zariadenia pre bezpečné skladovanie, oddeľovanie a ochranu pred faktormi prostredia,
  - opatrenia pre použitie všeobecných bezpečnostných a hygienických pravidiel,
  - prostriedky osobnej ochrany,
  - vzduchotechnické zariadenia,
  - prostriedky na ochranu životného prostredia a bezpečnú likvidáciu nebezpečných látok a iné,
- Nevyhnutné prostriedky potrebné k zaisteniu požiarnej ochrany:
  - prostriedky na zabránenie vzniku požiaru,
  - prostriedky na zabránenie alebo obmedzenie šírenia požiaru,
  - prostriedky na zaistenie bezpečnej evakuácie,

- prostriedky na zaistenie bezpečného a účinného požiarneho zásahu a iné [59].

Táto časť pojednávala o prostriedkoch a zariadeniach, ktoré sú využiteľné v prípade ochrany prvku KI a v prípade zachovania funkčnej kontinuity KI. Je nevyhnutné skonštatovať, že analýza možností využitia týchto prostriedkov a zariadení by si zaslúžila väčší priestor. Spomínané prostriedky a zariadenia budú neodmysliteľnou časťou bezpečnostného systému prvku KI, preto je potrebné sa zaoberať ich štruktúrou a konštrukčnými vlastnosťami a následne stanoviť ich optimálnu vzájomnú kombináciu.

Významným aspektom ochrany KI je použitie technológií, ktorých účelom je zvyšovanie odolnosti prvku či celej KI, vzhľadom na ich vzájomnú prepojenosť a ovplyvniteľnosť. Zvyšovanie odolnosti KI je vnímané v súvislosti so schopnosťou ohrozeného systému odolávať čo najširšiemu spektru hrozieb a škodlivých faktorov pri zachovaní základných funkcií. Ochrana prvku KI by mala byť v tomto kontexte chápaná a vnímaná ako komplex ochranných opatrení na všetkých úrovniach riadenia rizík a bezpečnosti organizácie. Pre účely tejto práce sa budem v časti technologické aspekty ochrany kritickej infraštruktúry v SR zaoberať problematikou stanovenia požiadaviek pre mechanické zábranné systémy, elektronické zabezpečovacie systémy či systémy pre kontrolu vstupu v súvislosti s legislatívnymi usmerneniami.

2.3.5 Technologické aspekty ochrany kritickej infraštruktúry v SR

Ochrana KI je organizovaná vzhľadom na absenciu konkrétneho zákona dokumentmi, ktoré som podrobil rozboru v úvodných kapitolách. Vo vzťahu k technologickým aspektom ochrany sa spomínajú len nasledovné súvislosti: používanie autonómnych dispečerských systémov, vybudovanie integrovaných bezpečnostných systémov v kombinácii s fyzickou ochranou, napojenie objektov na signalizačný systém polície, a iné [19]. Vymedzenie konkrétnych opatrení a nástrojov na ochranu KI je vnímané ako stanovenie nástrojov na:

- Ochranu a obranu prvkov KI,
- Prevenciu pred ohrozením,
- Zníženie rizika ohrozenia,
- Existenciu a stability prvku [18], atď.

Podrobnejšie budú analyzované v ďalších častiach textu. Napriek týmto faktom, je tu výrazná absencia smernice, normy či štandardu, ktorý by jasne formuloval štruktúru bezpečnostného systému prvku KI a požiadavky na jeho komponenty.

Pri vytváraní takéhoto dokumentu sa zrejme bude vychádzať s dokumentov, ktoré štruktúru a požiadavky komponentov bezpečnostného systému formulujú vo vzťahu k ochrane hmotného a nehmotného majetku či utajovaných skutočností. Jedná sa predovšetkým o vyhlášku Národného bezpečnostného úradu Slovenskej Republiky č. 336/2004 Z.z. o fyzickej a objektovej bezpečnosti či zákon č. 483/2001 Z.z., zákon č. 483/2001 Z.z o bankách a o zmene a doplnení niektorých predpisov, Vyhláška Úradu jadrového dozoru Slovenskej republiky č. 51 ktorou sa ustanovujú podrobnosti o požiadavkách na zabezpečenie fyzickej ochrany či norma ČSN CLC/TS 50131-7 príloha E, zákon č. 261/2002 Zb. o prevencii závažných priemyselných havárií ako aj ďalšie legislatívne dokumenty. Pre účely tejto práce budem analyzovať len niektoré s týchto dokumentov. Kým prejdem k analýze spomínaných dokumentov je treba spomenúť, že určitými zásadami ochrany KI sa zaoberá spomínaná koncepcia kritickej infraštruktúry a spôsob jej ochrany a obrany kde sú stanovené:

- Nástroje na prevenciu pred ohrozením - oddelenie vnútornej časti prvku od vonkajšieho priľahlého prostredia využitím mechanických zábranných systémov, oddelenie kritických počítačových systémov a ich komponentov od internetovej siete či využitie špeciálneho prepojenia užívateľov zaradených do úzkej skupiny,
- Nástroje na zníženie rizika ohrozenia existencie a stability prvku - technické prostriedky ochrany (elektronické a mechanické), na verifikáciu, detekciu, signalizáciu a odradenie potenciálneho páchateľa, ako aj využitie dohliadacej činnosti bezpečnostných služieb,
- Nástroje na odvrátenie útoku na prvok alebo systém jeho ochrany a obrany - zásah bezpečnostnej služby či zásah bezpečnostných zborov a ozbrojených síl,
- Nástroje na odstránenie následkov útoku na prvok alebo na systém jeho ochrany a obrany či nástroje využiteľné pri reakcii na narušenie alebo zničenie prvku - využitie dostupných záložných zariadení, využitie všetkých možných prepojení na zabezpečenie náhradnej prevádzky, či vytvorenie prostriedkov na čo najpromptnejšie obnovenie či náhradu poškodeného prvku kritickej infraštruktúry [18].

2.3.5.1 Vyhláška Národného bezpečnostného úradu Slovenskej Republiky č. 336/2004 Z.z. o fyzickej a objektovej bezpečnosti

Cieľom tejto vyhlášky je vytvorenie bezpečnostného štandardu fyzickej bezpečnosti a objektovej bezpečnosti vo vzťahu k stanoveniu minimálnej požadovanej úrovne ochrany objektov a chránených priestorov určených na ukladanie a manipuláciu s utajovanými

skutočnosťami. Štruktúra tohto štandardu by mala umožňovať vytvorenie variabilného systému bezpečnostných opatrení podľa individuálnych podmienok každého objektu. Na stanovenie a ohodnotenie úrovne fyzickej bezpečnosti a objektovej bezpečnosti sa používa bodovací systém, ktorý umožňuje voliť v závislosti od konkrétnych podmienok takú kombináciu bezpečnostných opatrení, ktoré najlepšie vyhovujú daným podmienkam. Pre objekty a chránené priestory sú stanovené najmenšie bodové hodnoty, ktoré treba dosiahnuť. Využíva sa tu matematická metóda, ktorá prideľuje jednotlivým bezpečnostným opatreniam ustanovené bodové hodnoty, ktorých súčet sa príslušným spôsobom vyhodnocuje. Vyhláška obecne vymedzuje požiadavky na mechanické zábranné systémy[1], technické zabezpečovacie prostriedky[2], fyzickú ochranu a režimové opatrenia, ktoré sú potenciálne použiteľné na ochranu objektu a chráneného priestoru. Každá bezpečnostná úroveň je bodovo ohodnotená na základe bezpečnostnej úrovne jej komponentov. Následne sa stanovuje hodnota kombinácií jednotlivých opatrení napr. fyzická ochrana a elektrický zabezpečovací systém.

Postupne sa posudzujú opatrenia ochrany objektu, kontrola vstupov a režim návštev, fyzická ochrana a elektrický zabezpečovací systém či opatrenia vonkajšej ochrany. Po ohodnotení spomínaných opatrení sa kompletizuje tabuľka bodového hodnotenia bezpečnostných opatrení v chránenom priestore (bodové hodnoty pre - úschovné objekty, chránený priestor, objekt, kontrola vstupu, režim návštev v objekte a iné).

Táto vyhláška vytvára ucelený spôsob hodnotenia stupňa ochrany, stanovenia požiadaviek bezpečnostných opatrení v súvislosti s utajovanými skutočnosťami. Je predpoklad, že by tento systém bolo možné použiť aj v súvislosti s hodnotením stupňa ochrany prvku KI spolu so stanovením požiadaviek na jednotlivé komponenty bezpečnostného systému. Nevýhodou tohto systému je, že nezohľadňuje prielomovú odolnosť či pravdepodobnosť detekcie jednotlivých komponentov, ktoré sú zložkou časovej závislosti narušiteľa a zásahovej jednotky [28].

[1] Podľa noriem STN P ENV1627, STN P ENV1628, STN P ENV1629, STN P ENV1630, STN EN 356 (70 0595), STN 74 7731, STN EN 1303 (16 5191), STN EN 1906 (16 5192), STN 16 5190 a iných noriem

[2] STN EN 50133-1, STN EN 50133-2-1, STN EN 50133-7, STN EN 50131-1, STN EN 50131-1 Zmena Z1, STN EN 50131-6, STN 33 4590-1, STN 33 4590-2, STN 33 4590-3, STN 33 4590-4, a iných noriem

2.3.5.2 Vyhláška Úradu jadrového dozoru Slovenskej republiky č. 51 ktorou sa ustanovujú podrobnosti o požiadavkách na zabezpečenie fyzickej ochrany

Táto vyhláška ustanovuje podrobnosti o požiadavkách na zabezpečenie fyzickej ochrany vrátane jadrového zariadenia alebo jadrového materiálu do kategórií na zabezpečenie fyzickej ochrany. Účelom systému fyzickej ochrany podľa tejto vyhlášky je zabezpečenie prístupu do stráženého priestoru, chráneného priestoru a vnútorného priestoru len osobám alebo vozidlám, ktorým bolo vydané povolenie, či včasná detekcia narušiteľov a spomalenie ich postupu využitím kombinácie elektronického zabezpečovacieho systému a mechanických zábranných prostriedkov,

Sú tu formulované požiadavky na bariéry stráženého priestoru, chráneného priestoru a vnútorného priestoru, či priestoru v ktorom sú umiestnené jadrové materiály a to vo vzťahu k ich konštrukcii, osvetleniu, ochrane voči poškodeniu týchto zábran a sú stanovené ich konštrukčné požiadavky.

Definujú sa tu požiadavky a štruktúra či konštrukcia izolačných zón, požiadavky na zabezpečenie budovy, ktorá je súčasťou izolačnej zóny, konštrukcia a režim používania dverí, brán, okien a ostatných zariadení, určených na prechod bariérou. Účelom elektronického zabezpečovacieho systému podľa tejto vyhlášky je hlavne spoľahlivá detekcia neoprávneného prekonávania bariér, signalizácia poruchy alebo pokusu o poškodenie alebo narušenie činnosti tohto zariadenia, optická a zvuková signalizácia vyvedená na pult centralizovanej ochrany pri pokuse o neoprávnené prekonanie bariér, lokalizácia miesta neoprávneného prekonávania bariéry a iné. Významným aspektom fyzickej ochrany podľa tohto dokumentu je vypracovanie predbežného plánu fyzickej ochrany, na ktorý sa následne vypracuje konečný plán fyzickej ochrany, ktorý obsahuje zhodnotenie výsledkov skúšok fyzickej ochrany, spôsob ochrany a kontroly osôb a vjazdov dopravných prostriedkov a iné režimové opatrenia, ako aj limity a podmienky systému fyzickej ochrany či opatrenia týkajúce sa obmedzenia prevádzky pri pokuse o neoprávnenú činnosť alebo pri narušení fyzickej ochrany [29].

Vyhláška, ktorou sa ustanovujú podrobnosti o požiadavkách na zabezpečenie fyzickej ochrany formuluje požiadavky na bezpečnostný systém vo vzťahu k fyzickej ochrane. Vymedzenie jednotlivých komponentov a ich konštrukčné či funkčné požiadavky nie sú konkrétne definované v závislosti na miere rizika, ale je to komplexný dokument ktorý rieši fyzickú ochranu ako takú.

2.3.5.3 Norma ČSN CLC/TS 50131-7 príloha E

Táto časť normy a v nej uvedená tabuľka slúžia ako pomôcka pre klientov či zadávateľov pri stanovovaní, potenciálnych druhov narušenia v rôznych miestach strážených objektov. Tabuľka vychádza z rizika posúdeného v priebehu previerky lokality a uvažuje o pravdepodobných spôsoboch narušenia používaných narušiteľmi s rôznymi úrovňami skúseností. Tabuľka nešpecifikuje podrobný prehľad možných metód narušenia, ktoré sú pravdepodobné, vzhľadom na rozdielnosť podmienok v jednotlivých objektoch.

	Stupeň 1	**Stupeň 2**	**Stupeň 3**	**Stupeň 4**
Obvodové dvere	O	O	OP	OP
Okná		O	OP	OP
Ostatné otvory		O	OP	OP
Steny				P
Stropy alebo strechy				P
Podlahy				P
Miestnosti	T	T	T	T
Predmet (vysoké riziko)			S	S
O - otvorenie P - prienik T - pasca, nástraha S - predmet vyžadujúci špeciálne				

Tabuľka 3: Minimálne úrovne zabezpečenia

Tabuľka nestanovuje, akým spôsobom by mali byť navrhovateľmi stanovené všetky systémy EZS pre daný stupeň zabezpečenia. V mnohých prípadoch bude zadávateľ schopný dosiahnuť požadovanej úrovne zabezpečenia aj s použitím prvkov EZS s iným stupňom zabezpečenia. Je dôležité sa venovať aj iným metódam narušenia, ktoré nie sú v tabuľke popísané a definované. Tento spôsob stanovenia úrovne zabezpečenia objektu je len obecný a zohľadňuje len niektoré faktory, ktoré sú v rozhodovacom procese navrhovateľa [50].

Táto časť poskytla ucelený pohľad na spôsoby hodnotenia stupňa resp. úrovne ochrany hmotného či nehmotného majetku, ktoré sú aplikovateľné a implementovateľné do problematiky ochrany KI. Na jednej strane je hodnotenie zamerané na stanovenie minimálnej bodovej hodnoty pre jednotlivé stupne ochrany, ktoré vyjadruje suma bodových hodnôt jednotlivých komponentov ochrany. Významný aspektom ochrany KI je využitie fyzickej ochrany, ktorej požiadavky určitým spôsobom formuluje rozoberaná vyhláška. Právny dokument, ktorý by pojednával resp. rozoberal a špecifikoval technologické aspekty ochrany KI však absentuje. Jeho formulovanie, si vyžaduje bezpečnostný výskum, ktorý by

implementoval tieto dokumenty do smernice či vyhlášky pre technologické aspekty ochrany KI.

Jednotlivé kapitoly tejto časti práce boli koncipované na základe analýzy aktuálnych poznatkov v predmetnej problematike. Medzi publikácie, ktoré významným spôsobom ovplyvnili elaboráciu je možné zaradiť „All Hazards Risk and Resilience: Priorizing Critical Infrastructures Using The RAMCAP Plus Approach“ [1], „Critical Infrastructure: Reliability and Vulnerability“ [8], „Homeland Security and Private Sector Business: Corporations´ Role in Critical Infrastructure Protection“ [5], „Critical Infrastructure: Understanding Its Component Parts, Vulnerabilities, Operating Risks and Interdependencies“ [6] či „Homeland Security and Critical Infrastructure Protection“ [2] a iné.

Záver teoretickej časti

Rozbor dostupných domácich a aktuálnych zahraničných materiálov a legislatívnych nástrojov poukázal na nevyhnutnosť ochrany KI, vzhľadom na ich význam z pohľadu fungovania spoločnosti a jej ekonomických a sociálnych aspektov. Zmena bezpečnostného prostredia ako aj zvyšujúca sa zložitosť systémov prispieva k tvorbe nových dokumentov, štandardov, ktoré usmerňujú ochranu KI a vytvárajú rámec na jej optimálnu a efektívnu úroveň. Významným faktorom ochrany KI a jej prvkov je využívanie technológií, ktoré priamo súvisia so zvyšovaním robustnosti prvku a následne tak odolnosti KI ako celku. Napriek tomu, že sa predmetnej problematike venuje dostatočný priestor, je tu určitá absencia noriem a postupov pre zaistenie požadovanej úrovne ochrany, a ktoré by presne špecifikovali prístupy k stanoveniu požiadaviek na bezpečnostné systémy jednotlivých prvkov KI a ktoré by formulovali štruktúru a vlastnosti bezpečnostných opatrení v súvislosti s využívaním mechanických zábranných systémov, technických zabezpečovacích prostriedkov, fyzickej ostrahy či režimových opatrení. Riešením tohto stavu by mohlo byť väčšie využívanie akademického potenciálu a jeho aktívna účasť v rámci jednotlivých bezpečnostných projektov, ako aj vytvorenie rámca pre efektívnu a koordinovanú spoluprácu štátneho a súkromného sektoru.

3 CIELE DIZERTAČNEJ PRÁCE

Po analýze dostupných materiálov, smerníc, legislatívnych, organizačných a inštitucionálnych nástrojov som dospel k záveru, že absentuje metodika, ktorá by komplexne hodnotila a stanovila požiadavky na technologické aspekty ochrany kritickej infraštruktúry. Táto absencia je vnímaná aj v kontexte činnosti zodpovedných entít, ktoré vytvárajú rámec pre tvorbu metodík, riešiacich túto absenciu, pričom sa predpokladá, že vznik takejto metodiky bude previazaný s výskumnou činnosťou akademického sektoru. Vzhľadom na priority štátnych orgánov v predmetnej problematike je nutné formulovať požiadavky na implementáciu systémov fyzickej ochrany do procesu optimalizácie ochrany kritickej infraštruktúry na všetkých jej úrovniach.

Cieľom dizertačnej práce je vytvorenie takejto metodiky, ktorá umožní komplexne hodnotiť a stanoviť štruktúru bezpečnostného systému prvku KI z pohľadu systémov fyzickej ochrany, využívajúcich mechanické zábranné systémy, technické zabezpečovacie prostriedky, fyzickú ostrahu a režimové opatrenia a to nie len z pohľadu definovania jej štrukturálnych vlastností a požiadaviek, ale aj z prihliadnutím na funkčnosť jednotlivých komponentov systému fyzickej ochrany prvku KI. Táto metodika vytvorí rámec pre hodnotenie jednotlivých komponentov a pre vyjadrenie vzťahu štruktúry bezpečnostného systému a úrovne ochrany prvku ako aj celej KI v rámci daného sektoru. Vytvorenie spomínanej metodiky bude mať tieto čiastkové časti:

- Stanovenie štruktúry systému fyzickej ochrany prvku KI,
- Stanovenie štrukturálnych a funkčných požiadaviek systému fyzickej ochrany pre jednotlivé bezpečnostné triedy,
- Vytvorenie prístupu k hodnoteniu štruktúry systému fyzickej ochrany prvku KI,
- Vyjadrenie vzťahu štruktúry systému fyzickej ochrany a úrovne ochrany prvku KI,
- Vyjadrenie vzťahu úrovne ochrany prvkov KI a úrovne ochrany sektoru KI,
- Overenie štruktúry a funkčnosti systému fyzickej ochrany objektov KI pomocou informačnej podpory.

4 METÓDY SPRACOVANIA DIZERTAČNEJ PRÁCE

Dizertačná práca „Technologické aspekty ochrany kritickej infraštruktúry SR“ bola elaborovaná využitím metód, ktoré zodpovedajú metódam riešenia vedeckej práce. Pri procese tvorby práce boli použité tieto metódy riešenia vedeckej práce:

- Analýza,
- Komparácia,
- Syntéza,
- Analógia,
- Indukcia a dedukcia
- Simulácia.

Primárnou metódou vedeckého prístupu pri spracovaní dizertačnej práce bola metóda analýzy, ktorá bola použitá hlavne v súvislosti s objektivizáciou a objasnením jednotlivých skúmaných aspektov a vzťahov v tých častiach práce, ktoré pojednávali o problematike ochrany kritickej infraštruktúry, o aktuálnych prístupoch k technologickým aspektom ochrany dôležitých infraštruktúr, o oblastiach legislatívy v súvislosti s ochranou kritickej infraštruktúry, o využití simulačných technológii a nástrojov ako aj o procese návrhu metodiky pre systém fyzickej ochrany prvku kritickej infraštruktúry.

Kvantitatívna a systémová analýza s využitím popisných metód, umožnila aj vďaka získaným informáciám, definovať a identifikovať potreby stanovenia štrukturálnych a funkčných vlastností systému fyzickej ochrany prvku kritickej infraštruktúry, čo vytvorilo predpoklady pre aplikáciu týchto poznatkov do experimentálnej časti práce (stanovenie štruktúry systému fyzickej ochrany prvkov kritickej infraštruktúry, vyjadrenie funkčnosti systému fyzickej ochrany na základe pravdepodobností a prielomových odolností pre jednotlivé bezpečnostné triedy).

Metódy komparácie a analógie boli využité hlavne v kontexte s formulovaním a prezentáciou poznatkov a znalostnej základne o stave legislatívneho prostredia v oblasti využiteľnosti systémov fyzickej ochrany vo vzťahu k ochrane majetku a osôb, prevencie závažných priemyselných havárií, obrane štátu či krízovým riadením štátu. Metóda bola zdrojom identifikácie požiadaviek, ktoré aktuálny stav riešenia ochrany kritickej infraštruktúry požaduje.

Pre stanovenie vzťahov medzi štrukturálnymi a funkčnými parametrami jednotlivých komponentov systému fyzickej ochrany a celkovou funkčnosťou spomínaného systému boli použité metódy indukcie a dedukcie. Pri samotnej tvorbe a návrhu štrukturálny a funkčných

požiadaviek bola použitá aj metóda syntézy, pri ktorej boli získané teoretické aj praktické poznatky využité v časti metodika hodnotenia systému fyzickej ochrany prvkov kritickej infraštruktúry, ako aj v časti posudzovanie funkčnosti systému fyzickej ochrany pomocou modelu EASI.

Pre verifikáciu definovanej štruktúry a funkčných požiadaviek systému fyzickej ochrany prvku kritickej infraštruktúry bola využitá metóda simulácie a to predovšetkým v kontexte so simulačným nástrojom OTB SAF, ktorého výstupy boli použité v súvislosti s doplnením modelu EASI pre jednotlivé bezpečnostné triedy ako aj v súvislosti s penetračnými testami systémov fyzickej ochrany prvku kritickej infraštruktúry.

Významným aspektom tvorby a elaborácie dizertačnej práce bolo použitie praktických osobných skúseností autora, ktoré boli získané pôsobením v uzavretej pracovnej skupine Ministerstva vnútra SR pre tvorbu zákona o ochrane kritickej infraštruktúry SR, ako aj pôsobením v iných odborných a profesných združeniach (Expertná skupina MV ČR pre posudzovanie a hodnotenie projektov bezpečnostného výskumu, Česká asociácia bezpečnostných manažérov).

Autor taktiež využil svoje skúsenosti a znalosti v oblasti ochrany majetku a osôb, získané štúdium oboru bezpečnostné technológie, systémy a management ako aj vedením seminárov predmetov Modelovanie krízových situácií, Objektová bezpečnosť II – elektronické prvky a Technické prostriedky bezpečnostného priemyslu.

5 TEORETICKÝ ZÁKLAD PRE STANOVENIE ŠTRUKTÚRY SYSTÉMU FYZICKEJ OCHRANY PRVKU KRITICKEJ INFRAŠTRUKTÚRY

Z analytickej časti práce je možno vydedukovať, že za významný aspekt ovplyvňujúci celkovú mieru odolnosti prvku a sektoru kritickej infraštruktúry je možné považovať systém fyzickej ochrany objektov. Využiteľnosť tohto systému vytvára rámec pre konkrétne riešenie ochrany objektov a zvyšuje mieru robustnosti daného prvku. V súvislosti s aktuálnymi legislatívnymi požiadavkami sa vytvára priestor pre implementáciu tohto systému do problematiky ochrany KI. Vzhľadom na to, že systém fyzickej ochrany objektov je zložitým systémom, ktorý sa skladá zo vzájomne pôsobiacich subsystémov, je pre stanovenie jeho optimálnej štruktúry nevyhnutné definovať základné funkcie systému a jeho elementárne časti. Na základe tohto procesu je následne možné stanoviť štruktúru a metodiku jeho hodnotenia. Pre overenie funkčnosti celého systému ako aj jeho subsystémov je nevyhnutné využiť všetky dostupné simulačné a modelovacie systémy v optimálnej kombinácii. Problematika ochrany KI je multirezortná a multidisciplinárna preto vhodnou formou kombinácie sa v kontexte tejto práce rozumie využiteľnosť technológii jednak z civilného tak z armádneho prostredia vzhľadom na ich rozdielne funkcie, ktoré sú však využiteľné v problematike ochrany KI a vhodne sa dopĺňajú. Pre experimentálnu časť práce som si zvolil armádny simulačný nástroj OTB SAF, ktorý je využiteľný pre simulovanie činnosti fyzickej ostrahy objektu a vytvára premenné pre modelovací nástroj EASI. Výstupom kombinácie týchto dvoch nástrojov je parameter, ktorý vyjadruje pravdepodobnosť úspešného zásahu fyzickej ostrahy pre rôzne typy napadnutia objektu.

5.1 Hlavné funkcie systému fyzickej ochrany prvkov KI

Definovanie hlavných funkcií systému fyzickej ochrany prvkov KI je významným faktorom ovplyvňujúcim celkovú štruktúru systému a jeho subsystémov. Dôležitým krokom v tomto smere je definovanie si potenciálneho páchateľa resp. narušiteľa a spôsoby vniknutia tohto narušiteľa do objektu. Budem vychádzať z normy ENV 1627, kde sú stanovené aj možné spôsoby vniknutia. Vzhľadom na dôležitosť kritickej infraštruktúry v kontexte udržania funkčnej kontinuity spoločnosti budem brať do úvahy narušiteľov resp. páchateľov:

- Príležitostný páchateľ, ktorý sa pokúša o vniknutie pomocou dvoch alebo viacerých šraubovákov a páčidla,

- Skúsený páchateľ, používajúci pílu, kladivo a dláto, sekeru a prenosnú akumulátorovú vŕtačku,
- Skúsený páchateľ používajúci aj elektrické náradie, ako napríklad vŕtačku, elektrickú pílu a uhlovú brúsku s kotúčom s priemerom 125 mm,
- Skúsený páchateľ používajúci aj výkonnejšie elektrické náradie, ako napr. vŕtačku, priamočiaru pílu a uhlovú brúsku s kotúčom o priemere 230 mm.

Aj na základe tohto rozdelenia je možné definovať a stanoviť základné funkcie systému fyzickej ochrany prvkov KI. V súvislosti s komplexným využitím systému fyzickej ochrany sa uvažuje o troch hlavných funkciách systému a o týchto parametroch jeho subsystémov:

- Detekcia (detection) – detekcia narušiteľa s využitím technických zabezpečovacích prostriedkov (AIR, PIR, MW Bistatic, MW Monostatic, dual senzor ...atď) a overenie poplachovej informácie pomocou kamerového systému (CCTV), parameter – pravdepodobnosť správnej detekcie, čas potrebný pre overenie poplachovej informácie a pravdepodobnosť úspešnej komunikácie ,
- Spomalenie (delay) – spomalenie narušiteľa s využitím mechanických zábranných systémov (ploty, brány, prelezové bariéry, mreže, bezpečnostné dvere, sklá a iné), parameter – prielomová odolnosť,
- Odozva (response) – reakcia fyzickej ostrahy objektu – zamedzenie, prerušenie alebo zadržanie narušiteľa aj s využitím režimových opatrení, parameter – čas potrebný na presun fyzickej ostrahy z miesta A do miesta B.

Tieto základné funkcie sú následne využiteľné a výrazným spôsobom formulujú štruktúru systému fyzickej ochrany prvkov KI.

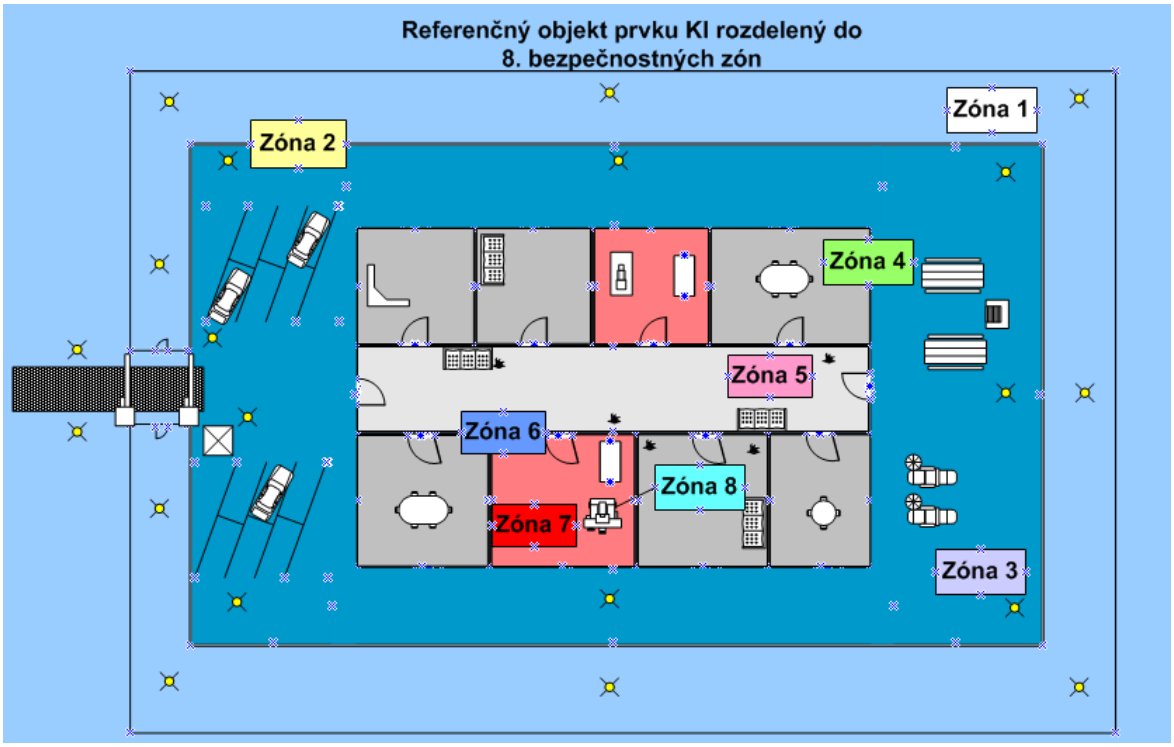
V tejto časti práce budem používať terminologické pojmy:

- Pravdepodobnosť komunikačnej podpory – je definovaná ako pravdepodobnosť úspešnej komunikácie fyzickej ostrahy s parametrami,
- Pravdepodobnosť správnej detekcie – je definovaná ako kumulatívna pravdepodobnosť detekcie narušiteľa detekčnými systémami,
- Prielomová odolnosť – čas potrebný na prekonanie mechanického zábranného systému,
- Dostupnosť fyzickej ostrahy – čas potrebný na presun fyzickej ostrahy na miesto narušenia objektu.

6 EXPERIMENTÁLNA ČASŤ

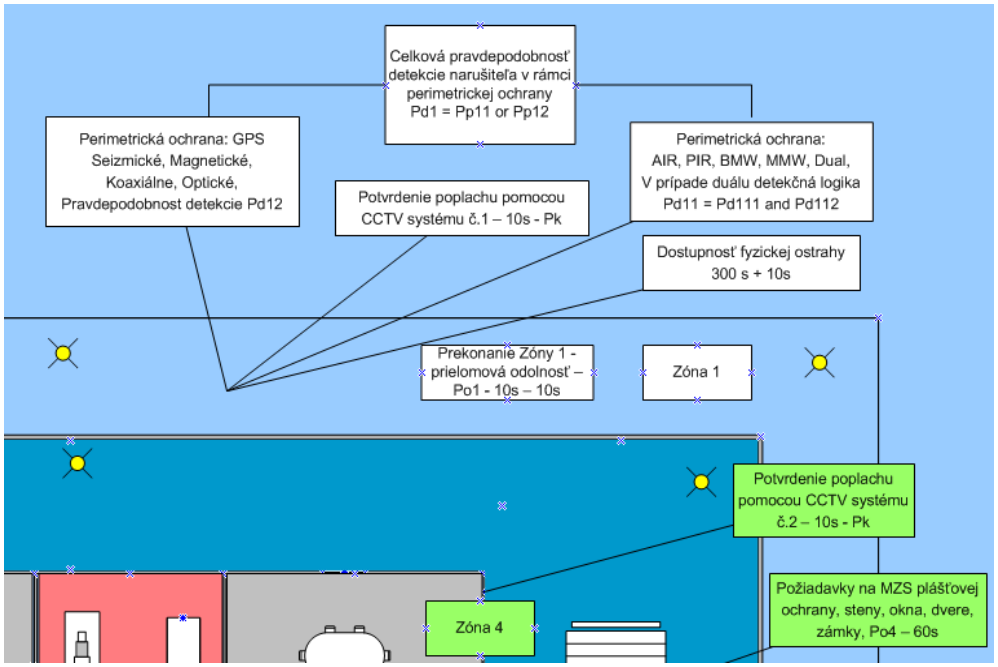
6.1 Stanovenie štruktúry systému fyzickej ochrany prvkov KI

Pre stanovenie, formulovanie a definovanie štruktúry systému fyzickej ochrany prvkov KI som si vytvoril referenčný model prvku KI, ktorý je rozdelený do jednotlivých bezpečnostných zón (obr.7). Stanovenie počtu bezpečnostných zón vychádza z analýzy relevantnej literatúry a z určitých zaužívaných prístupov v predmetnej problematike, pričom ich počet je zvyčajne 4-8. Pre potreby dizertačnej práce ako aj v súvislosti s kritickosťou objektov KI je model rozdelený do 8 zón, ktoré sú rozlíšené rôznou farbou textových polí. V každej tejto zóne sa uvažuje o už definovaných funkciách systému fyzickej ochrany a o parametroch jeho subsystémov. V ďalších častiach práce sa budem jednotlivým zónam venovať podrobnejšie.



Obrázok 7: Rozdelenie prvku KI na 8 zón

Každá zóna je posudzovaná z hľadiska parametrov pre jednotlivé subsystémy systému fyzickej ochrany prvku KI. V nasledujúcej časti definujem a popíšem jednotlivé bezpečnostné triedy a parametre, ktorým sa budem venovať aj v ďalšom texte.



Obrázok 8: Zóna 1

6.1.1 Parametre zóny 1

Na základe obrázku je možné parametre rozdeliť do skupín na:

Technické zabezpečovacie prostriedky v zóne 1

Parametre technických zabezpečovacích prostriedkov budú v ďalších častiach práce vnímané a posudzované v súvislosti s pravdepodobnosťou správnej detekcie.

- Perimetrická ochrana – **Pd11** (pravdepodobnosť správnej detekcie), ktorú tvoria systémy ako AIR, PIR, BMW, MMW Dual v prípade dual detekčná logika **Pd11 = Pd111 (PIR) and Pd112 (MW)**[3],
- Perimetrická ochrana – **Pd12**, ktorú tvoria systémy GPS (ground perimeter system), či už magnetické, koaxiálne, optické a iné,
- Celková pravdepodobnosť správnej detekcie v rámci zóny 1 - **Pd1**– perimetrickej ochrany **Pd1=Pd11 or Pd12**
- Potvrdenie poplachu CCTV **č.1** – má časový rámec n (vyjadrenie času potrebného na overenie poplachovej informácie) + **Pk** pravdepodobnosť komunikačnej podpory fyzickej ochrany.

[3] V tejto časti textu vstupuje do procesu stanovenia celkovej pravdepodobnosti vzťah jednotlivých detekčných systémov vyjadrený matematickou logikou (or, and)

Mechanické zábranné systémy v zóne 1

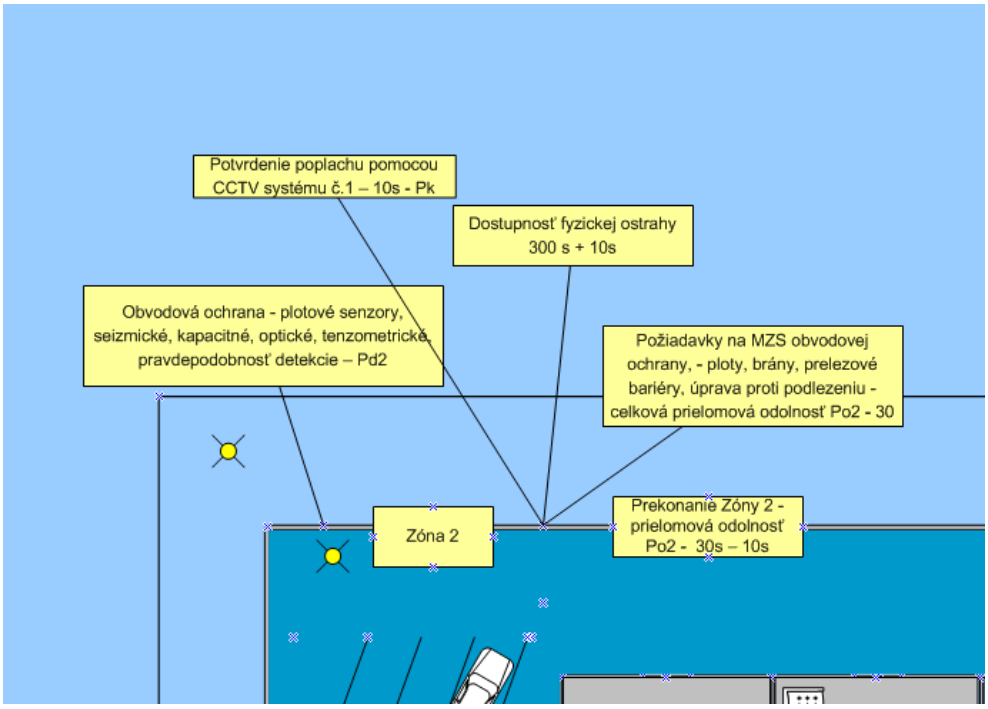
Parametre mechanických zábranných systémov budú v ďalších častiach práce vnímané a posudzované v súvislosti s ich prielomovou odolnosťou vyjadrenou časovým úsekom potrebným na ich prekonanie.

- V zóne 1 sa nepredpokladá s využitím MZS je tam tenkou čiarou vyznačený plot, ktorý slúži len k minimalizácii falošných poplachov v dôsledku vonkajších vplyvov (zver, porast....) napriek tomu sa predpokladá, že prekonanie tejto zóny na základe obrázku bude trvať 10s z čoho vyplýva, že prielomová odolnosť **Po1** bude 10s, ale keďže overenie poplachovej informácie trvá 10s v tomto prípade je reálna prielomová odolnosť **Po1** – 0s[4].

Fyzická ostraha prvku KI v zóne 1

Parametre fyzickej ostrahy budú v ďalších častiach práce vnímané a posudzované v súvislosti s časovou závislosťou ich činnosti.

- Dostupnosť fyzickej ostrahy (čas prechodu z bodu A – stanovište na bod narušenia) je **300**s (poprípade čas stanovený simuláciou na OTB SAF) + 10s – tu vstupuje čas potrebný na overenie poplachovej informácie.



Obrázok 9: Zóna 2

[4] Uvedené časové hodnoty v celej tejto kapitole sú len orientačné a reálne hodnoty budú stanovené v ďalších častiach práce.

6.1.2 Parametre zóny 2

Technické zabezpečovacie prostriedky v zóne 2:

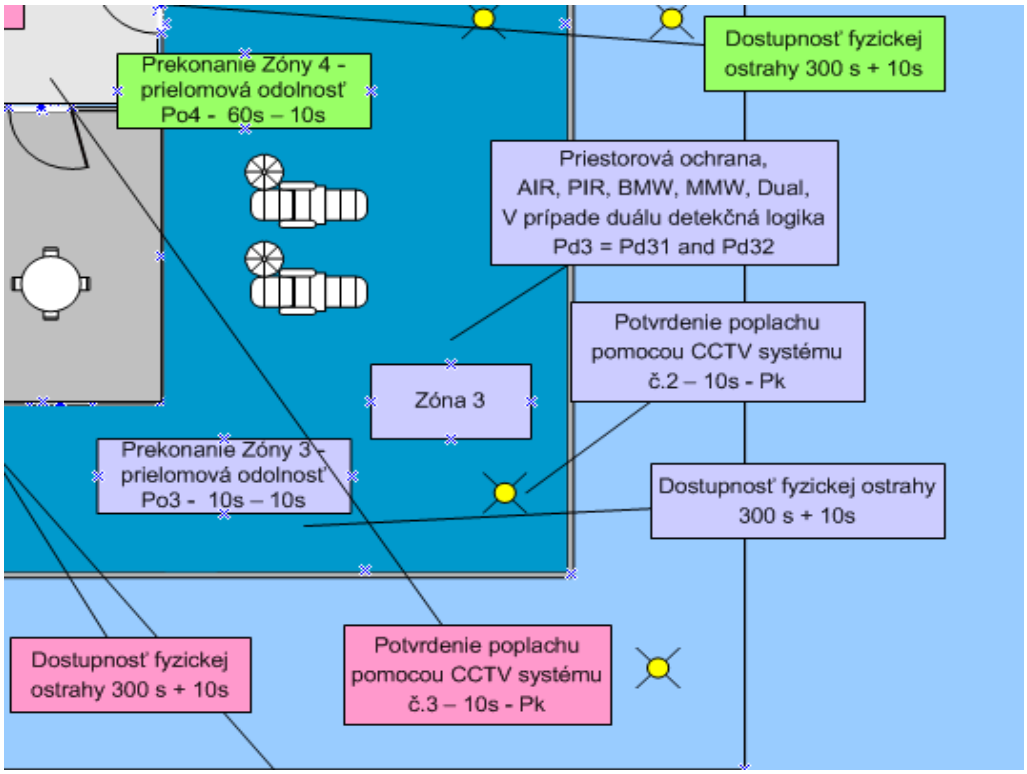
- Obvodová ochrana je v tomto kontexte chápaná ako súčasť perimetrickej ochrany – **Pd2** (pravdepodobnosť správnej detekcie), ktorú tvoria systémy ako plotové senzory, seizmické, kapacitné, optické, tenzometrické,
- Potvrdenie poplachu CCTV **č.1** – má časový rámec 10s (vyjadrenie času potrebného na overenie poplachovej informácie) + **Pk** pravdepodobnosť komunikačnej podpory fyzickej ostrahy.

Mechanické zábranné systémy v zóne 2:

- Tu je potrebné definovať požiadavky na MZS (ploty, brány, prelezové bariéry, úprava proti podlezeniu) v rámci zóny 2 aby spĺňali stanovenú podmienku prielomovej odolnosti napr. **Po2** - 30s, ale keďže overenie poplachovej informácie trvá 10s v tomto prípade je reálna prielomová odolnosť **Po2** – **20**s

Fyzická ostraha objektu

- Dostupnosť fyzickej ostrahy (čas prechodu z bodu A – stanovište na bod narušenia) je **300**s + 10s –čas potrebný na overenie poplachovej informácie.



Obrázok 10: Zóna 3

6.1.3 Parametre zóny 3:

Technické zabezpečovacie prostriedky v zóne 3:

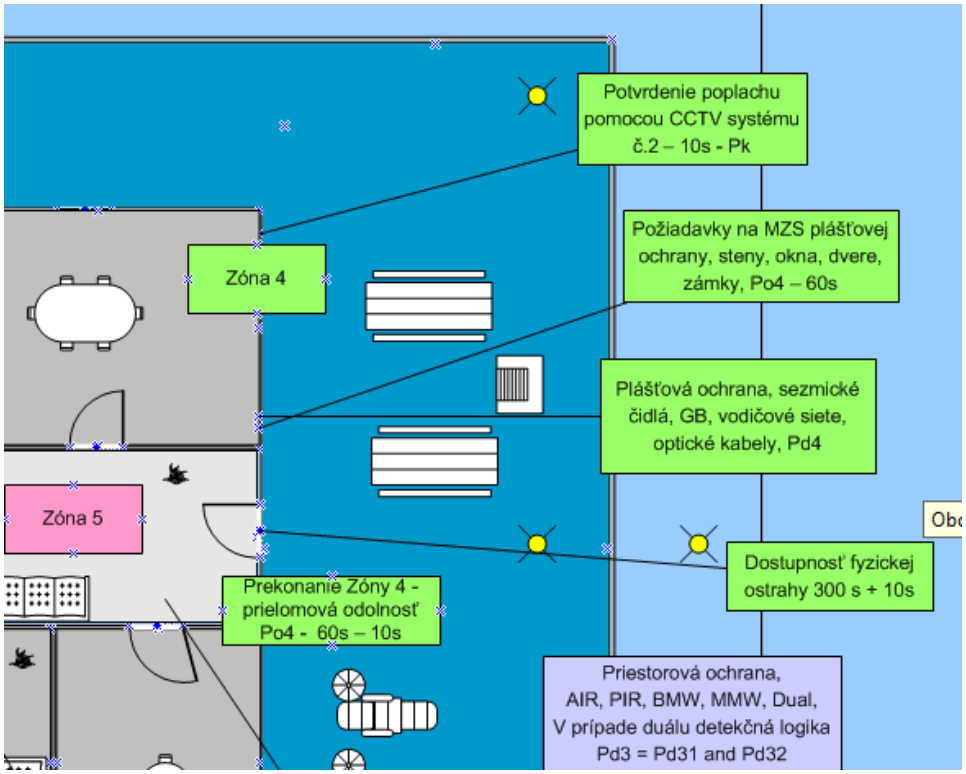
- Priestorová ochrana – **Pd3** (pravdepodobnosť správnej detekcie), ktorú tvoria systémy ako AIR, PIR, BMW, MMW Dual v prípade dual detekčná logika **Pd3** = **Pd31** (PIR) and **Pd32** (MW),
- Potvrdenie poplachu CCTV **č.2** – má časový rámec 10s (vyjadrenie času potrebného na overenie poplachovej informácie) + **Pk** pravdepodobnosť komunikačnej podpory fyzickej ostrahy.

Mechanické zábranné systémy v zóne 3:

- V zóne 3 sa nepredpokladá s využitím MZS, napriek tomu sa predpokladá, že prekonanie tejto zóny na základe obrázku bude trvať 10s z čoho vyplýva, že prielomová odolnosť **Po3** bude napr. 10s, ale keďže overenie poplachovej informácie trvá 10s v tomto prípade je reálna prielomová odolnosť **Po3** – 0s.

Fyzická ostraha objektu

- Dostupnosť fyzickej ostrahy (čas prechodu z bodu A – stanovište na bod narušenia) je 300s + 10s – čas potrebný na overenie poplachovej informácie.



Obrázok 11: Zóna 4

6.1.4 Parametre zóny 4

Technické zabezpečovacie prostriedky v zóne 4

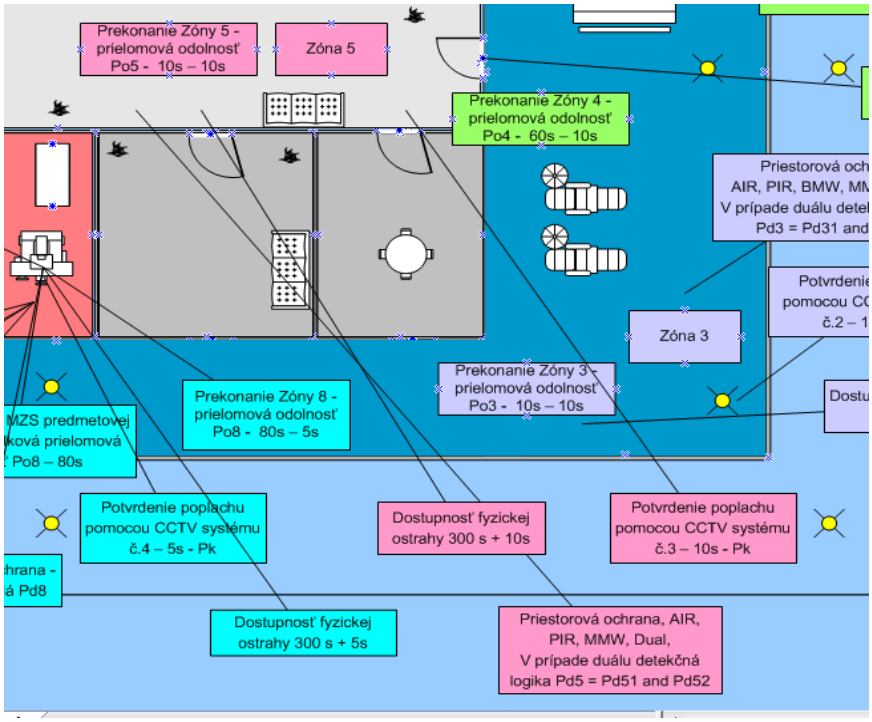
- Plášťová ochrana – **Pd4** (pravdepodobnosť správnej detekcie), ktorú tvoria systémy ako sezmické čidlá, GB (Glass Break), vodičové siete, optické kabely,
- Potvrdenie poplachu CCTV **č.2** – má časový rámec 10s (vyjadrenie času potrebného na overenie poplachovej informácie) + **Pk** pravdepodobnosť komunikačnej podpory fyzickej ochrany.

Mechanické zábranné systémy v zóne 4

- Tu je potrebné definovať požiadavky na MZS (steny, okna, dvere, zámky) v rámci zóny 4 tak aby spĺňali podmienku prielomovej odolnosti pre danú bezpečnostnú triedu, napr. **Po4** - 60s, ale keďže overenie poplachovej informácie trvá 10s v tomto prípade je reálna prielomová odolnosť **Po4** – **50**s

Fyzická ostaha prvku KI v zóne 4

- Dostupnosť fyzickej ostrahy (čas prechodu z bodu A – stanovište na bod narušenia) je **300**s (poprípade čas stanovený simuláciou na OTB SAF) + 10s – tu vstupuje čas potrebný na overenie poplachovej informácie.



Obrázok 12: Zóna 5

6.1.5 Parametre zóny 5

Technické zabezpečovacie prostriedky v zóne 5:

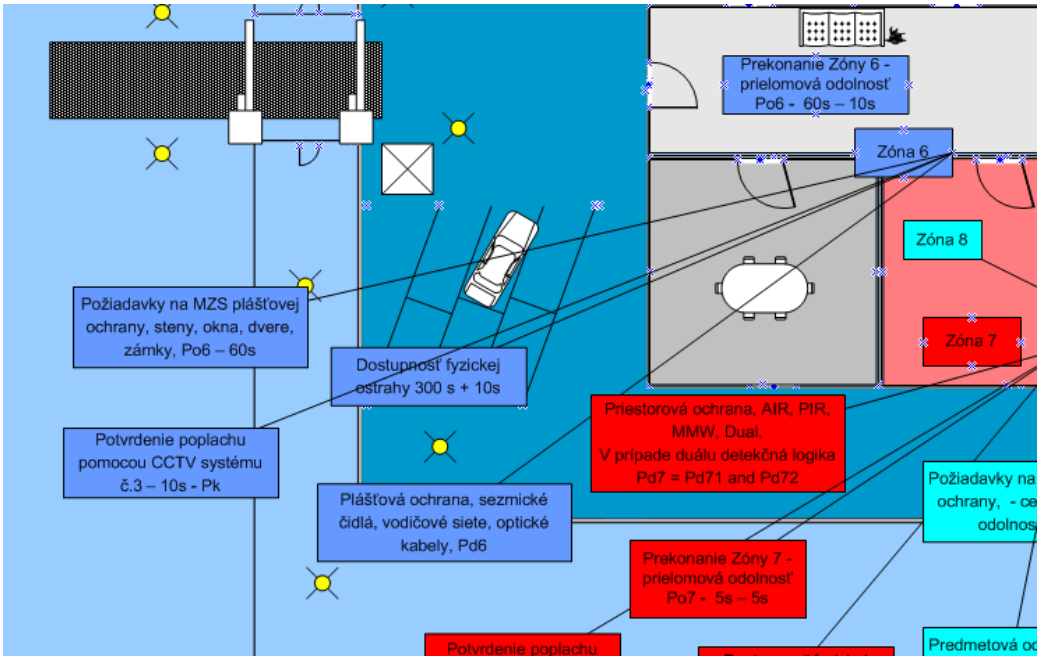
- Priestorová ochrana – **Pd5** (pravdepodobnosť správnej detekcie), ktorú tvoria systémy ako AIR, PIR, BMW, MMW Dual v prípade dual detekčná logika **Pd5** = **Pd51** (PIR) and **Pd52** (MW),
- Potvrdenie poplachu CCTV **č.3** – má časový rámec 10s (vyjadrenie času potrebného na overenie poplachovej informácie) + **Pk** pravdepodobnosť komunikačnej podpory fyzickej ostrahy.

Mechanické zábranné systémy v zóne 5:

- V zóne 5 sa nepredpokladá s využitím MZS, napriek tomu sa predpokladá, že prekonanie tejto zóny na základe obrázku bude trvať napr. 10s z čoho vyplýva, že prielomová odolnosť **Po5** bude 10s, ale keďže overenie poplachovej informácie trvá 10s v tomto prípade je reálna prielomová odolnosť **Po5**– 0s.

Fyzická ostraha objektu

- Dostupnosť fyzickej ostrahy (čas prechodu z bodu A – stanovište na bod narušenia) je **300**s + 10s – čas potrebný na overenie poplachovej informácie.



Obrázok 13: Zóna 6

6.1.6 Parametre zóny 6

Technické zabezpečovacie prostriedky v zóne 6:

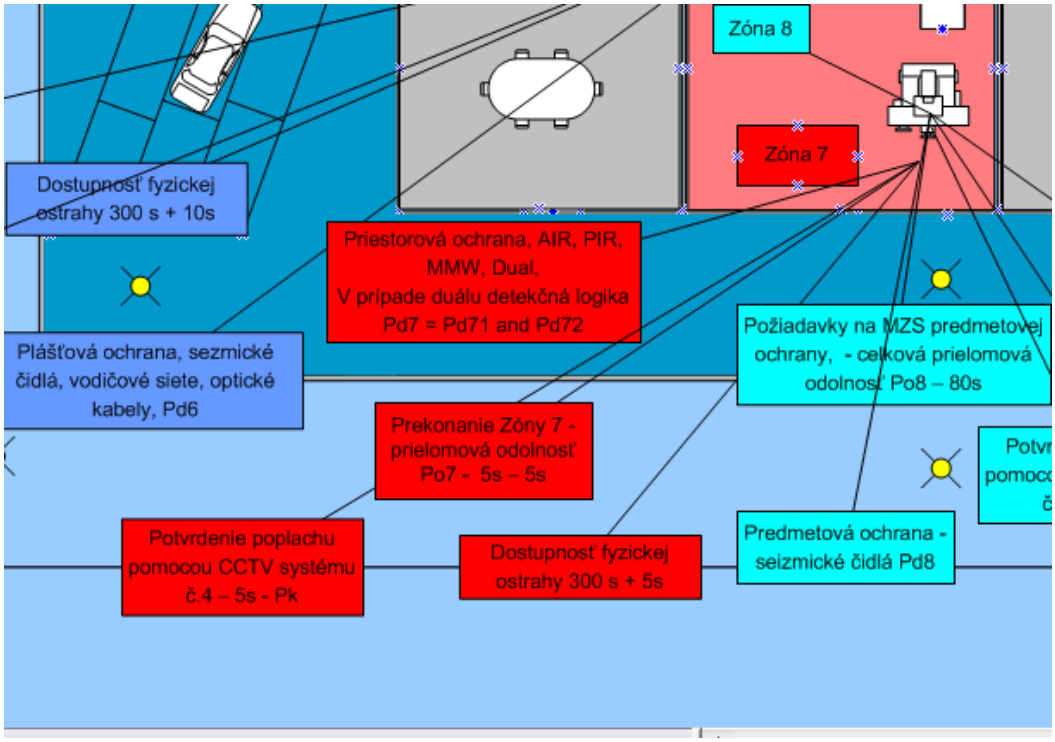
- Plášťová ochrana – **Pd6** (pravdepodobnosť správnej detekcie), ktorú tvoria systémy ako sezmické čidlá, GB, vodičové siete, optické kabely,
- Potvrdenie poplachu CCTV **č.3** – má časový rámec 10s (vyjadrenie času potrebného na overenie poplachovej informácie) + **Pk** pravdepodobnosť komunikačnej podpory fyzickej ostrahy.

Mechanické zábranné systémy v zóne 6:

- Tu je potrebné definovať požiadavky na MZS (steny, dvere, zámky) v rámci zóny 6 tak aby spĺňali podmienku prielomovej odolnosti pre danú bezpečnostnú triedu, napr. **Po6** - 60s, ale keďže overenie poplachovej informácie trvá 10s v tomto prípade je reálna prielomová odolnosť **Po6** – **50**s

Fyzická ostraha objektu

- Dostupnosť fyzickej ostrahy (čas prechodu z bodu A – stanovište na bod narušenia) je **300**s + 10s – čas potrebný na overenie poplachovej informácie.



Obrázok 14: Zóna 7

6.1.7 Parametre zóny 7

Technické zabezpečovacie prostriedky v zóne 7:

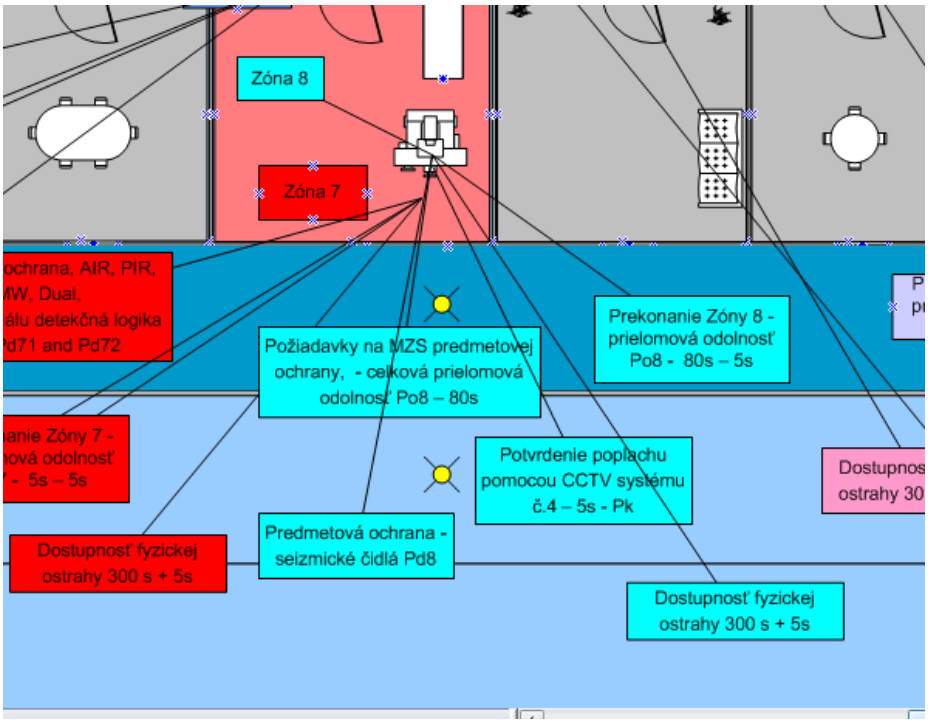
- Priestorová ochrana – **Pd7** (pravdepodobnosť správnej detekcie), ktorú tvoria systémy ako AIR, PIR, MMW, Dual v prípade dual detekčná logika **Pd7** = **Pd71** (PIR) and **Pd72** (MW),
- Potvrdenie poplachu CCTV **č.4** – má časový rámec 10s (vyjadrenie času potrebného na overenie poplachovej informácie) + **Pk** pravdepodobnosť komunikačnej podpory fyzickej ostrahy.

Mechanické zábranné systémy v zóne 7:

- V zóne 7 sa nepredpokladá s využitím MZS, napriek tomu sa predpokladá, že prekonanie tejto zóny na základe obrázku bude trvať narp. 10s z čoho vyplýva, že prielomová odolnosť **Po7** bude 10s, ale keďže overenie poplachovej informácie trvá 10s v tomto prípade je reálna prielomová odolnosť **Po7**– 0s.

Fyzická ostraha objektu

- Dostupnosť fyzickej ostrahy (čas prechodu z bodu A – stanovište na bod narušenia) je **300**s + 10s – čas potrebný na overenie poplachovej informácie.



Obrázok 15: Zóna 8

6.1.8 Parametre zóny 8

Technické zabezpečovacie prostriedky v zóne 8:

- Predmetová ochrana – **Pd8** (pravdepodobnosť správnej detekcie), ktorú tvoria systémy ako sezmické čidlá, polohové, kapacitné detektory a iné,
- Potvrdenie poplachu CCTV **č. 4** – má časový rámec 10s (vyjadrenie času potrebného na overenie poplachovej informácie) + **Pk** pravdepodobnosť komunikačnej podpory fyzickej ostrahy.

Mechanické zábranné systémy v zóne 8:

- Tu je potrebné definovať požiadavky na MZS (steny, dvere, zámky) v rámci zóny 8 tak aby spĺňali podmienku prielomovej odolnosti pre danú bezpečnostnú triedu, napr. **Po8** - 80s, ale keďže overenie poplachovej informácie trvá 5s v tomto prípade je reálna prielomová odolnosť **Po8** – **75**s

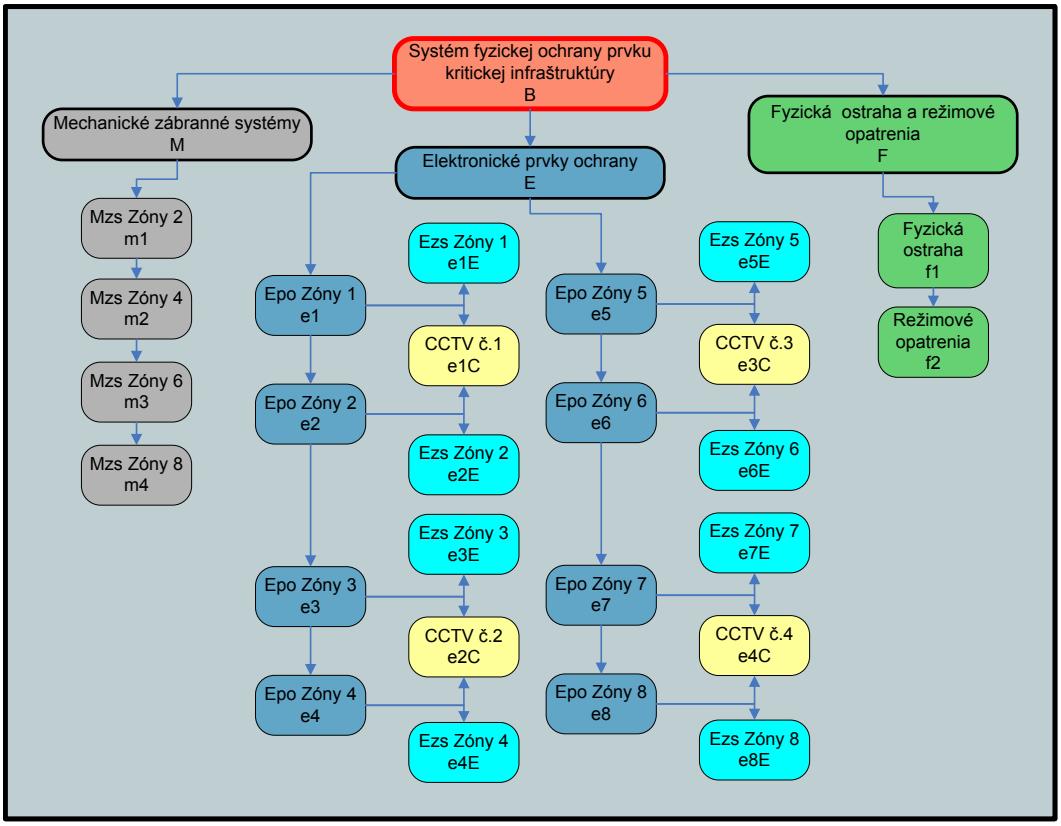
Fyzická ostraha objektu

- Dostupnosť fyzickej ostrahy (čas prechodu z bodu A – stanovište na bod narušenia) je **300**s + 10s – zase tu vstupuje čas potrebný na overenie poplachovej informácie.

6.1.9 Štruktúra systému fyzickej ochrany prvku KI

Po uplatnení tohto modelu a princípu na všetky zóny referenčného prvku KI je možné definovať štruktúru systému fyzickej ochrany prvku KI obr. 16, na základe ktorej je možné následne kvantitatívne vyjadriť hodnotu systému fyzickej ochrany, pokiaľ každému subsystému pridám bodové hodnoty od 1 - 4 vyjadrujúce určitú kvalitu – vyššiu prielomovú odolnosť či pravdepodobnosť. Systém fyzickej ochrany prvku kritickej infraštrkutúry je na základe obrázku rozdelený na tri základné časti – mechanické zábranné systémy, ktoré tvoria mechanické zábranné systémy pre zóny 2, 4, 6, 8; elektronické prvky ochrany, ktoré tvoria elektronické prvky ochrany zón 1-8, kamerové systémy 1-4; fyzická ostraha a režimové opatrenia. Vzhľadom na skutočnosť, že neboli stanovené obecné požiadavky na štruktúru systému fyzickej ochrany v súvislosti s problematikou ochrany KI, v ďalšej časti práce formulujem tieto požiadavky. Vo vzťahu k nekonštantnej dôležitosti jednotlivých prvkov kritickej infraštruktúry je vhodné si prvky rozdeliť do bezpečnostných tried uplatnením kritérií, ktoré boli navrhnuté v súvislosti s implementáciou smernice 2008/114/ES

o identifikácii a označení európskych kritických infraštruktúr a o potrebe zlepšiť ich ochranu a v súvislosti s činnosťou Ministerstva dopravy pôst a telekomunikácii v legislatívnej tvorbe.



Obrázok 16: Štruktúra systému fyzickej ochrany prvku kritickej infraštruktúry

6.2 Rozdelenie prvkov kritickej infraštruktúry do bezpečnostných tried

Rozdielna dôležitosť a nekonštantná rizikovosť jednotlivých prvkov KI vytvára potrebu definovania kritérií, na základe ktorých je možné dané prvky rozdeliť do bezpečnostných tried. Ako som už naznačil je vhodné využiť prierezové kritéria, ktoré boli stanovené v súvislosti s identifikáciou a označením európskych kritických infraštruktúr a ktoré by zohľadňovali národný aspekt týchto kritérií. V analytickej časti boli tieto kritériá popísané preto ich definujem len stručne:

- Kritérium strát na životoch
- Kritérium ekonomického vplyvu
- Kritérium vplyvu na obyvateľstvo.

6.2.1 Stanovenie bezpečnostných tried

Horná a spodná hranica definujúca intervalové hranice najvyššej a najnižšej bezpečnostnej triedy bude vychádzať zo smernice 2008/114/ES (horná hranica – prierezové kritéria pre označenie a identifikáciu európskej kritickej infraštruktúry) a z legislatívne činnosti Ministerstva dopravy pôst a telekomunikácii (spodná hranica – navrhované prierezové kritéria pre označenie a identifikáciu národnej kritickej infraštruktúry). Po uplatnení a doplnení tohto procesu môžeme podľa týchto kritérií rozdeliť prvky do 4 bezpečnostných tried – tabuľka 4.

Počet zranených	Počet mŕtvych	Ekonomická strata v mil. €	Fyzické utrpenie v tis. obyv.	Narušenie života v tis. obyv.	Bezpečnostná trieda
Nad 5 000	Nad 500	Nad 500	Nad 250	Nad 250	**IV**
2500 - 5000	250 - 500	250 - 500	125 - 250	125 - 250	**III**
1250 - 2500	125 - 250	125 - 250	62,5 - 125	62,5 - 125	**II**
Pod 1250	Pod 125	Pod 125	Pod 62,5	Pod 62,5	**I**

Tabuľka 4 : Stanovenie bezpečnostných tried pre prvky kritickej infraštruktúry (zdroj: autor)

Na základe tohto rozdelenia budú následne stanovené požiadavky na štruktúru a parametre systému fyzickej ochrany prvkov KI pre jednotlivé bezpečnostné triedy, čo vytvorí rámec pre definovanie metodiky hodnotenia tohto systému a efektívnejšiu ochranu týchto prvkov.

6.3 Hodnotenie mechanických zábranných systémov pre jednotlivé bezpečnostné triedy

V súvislosti so stanovením požiadaviek na mechanické zábranné systémy budem vychádzať z aktuálnych noriem (ENV 1627, EN 12209, EN 1303, EN 1906, EN 356,), ktoré s ochranou majetku priamo súvisia ako aj s pripravovaných noriem, ktoré budú vnímané a pripravované v kontexte prevencie kriminality a kde sa predpokladá implementovanie problematiky kritickej infraštruktúry v súvislosti so stanovením všeobecných štandardov systému fyzickej ochrany týchto objektov. Jedná sa predovšetkým o pripravovanú normu ČSN/P CEN/TS 14383-3. V súčasnej verzii tejto normy sú definované úrovne zabezpečenia no pre bežné objekty resp. objekty nižšej dôležitosti. Navzdory tomuto faktu je táto vedomostná základňa použiteľná aj v súvislosti s témou a potrebami dizertačnej práce. Na

základe tohto faktu špecifikujem požiadavky na mechanické zábranné systémy pre jednotlivé bezpečnostné triedy tabuľka 5.

Mechanický zábranný systém	Európska norma	Bezpečnostná trieda a priradené bodové hodnoty			
		I - 1	II - 2	III - 3	IV - 4
Vchodové dvere	ENV 1627	Trieda 3	Trieda 4	Trieda 5	Trieda 6
Bezpečnostný zámok	EN 12209	Trieda 4	Trieda 5	Trieda 5	Trieda 5
Cylindrická vložka	EN 1303	Trieda 4	Trieda 5	Trieda 5	Trieda 5
Dvere v ktorých je zámok uložený	EN 1906	Trieda 3	Trieda 4	Trieda 4	Trieda 4
Dosažiteľné okná	ENV 1627	Trieda 3	Trieda 4	Trieda 5	Trieda 6
Dosažiteľné zasklené plochy	EN 356	Trieda P6B	Trieda P7B	Trieda P8B	Trieda P8B
Okenice chrániace dosažiteľné okná alebo dvere	ENV 1627	Trieda 3	Trieda 4	Trieda 5	Trieda 6
Okna alebo dvere dosiahnuteľné iba z rebríku	ENV 1627	Trieda 1	Trieda 2	Trieda 3	Trieda 4
Zasklenie dosiahnuteľné iba z rebríku	EN 356	Trieda P4A	Trieda P4A	Trieda P5A	Trieda P6B
Úschovné objekty	EN 1143	Trieda III	Trieda IV	Trieda V	Trieda VI

Tabuľka 5: Bezpečnostná trieda a priradené bodové hodnoty - mechanický zábranný systém

Uvedená tabuľka stanovila bodové hodnoty jednotlivých mechanických zábranných systémov, ktoré zodpovedajú určitým požiadavkám špecifikovaným v konkrétnych európskych normách. Táto špecifikácia sa prejaví aj ďalších častiach práce, kde bude na základe tejto špecifikácie stanovená prielomová odolnosť pre jednotlivé bezpečnostné triedy.

Je možné konštatovať, že v súčasnosti absentuje komplexné stanovenie požiadaviek a spôsob hodnotenia mechanických zábranných systémov perimetrickej ochrany v súvislosti s využitím oplotenia v predmetnej problematike. V tomto smere použijem už existujúce prístupy k stanoveniu požiadaviek, ktoré upravím pre potreby tejto práce. Jedná sa predovšetkým o štandardy fyzickej ochrany objektov spoločnosti ČEZ a.s..

6.3.1 Mechanické zábranné systémy perimetrickej ochrany – Oplotenie

V tejto časti stanovím určité všeobecné požiadavky a následne definujem požiadavky, ktoré budú korešpondovať s jednotlivými bezpečnostnými triedami. Čo sa týka všeobecných požiadaviek na konštrukciu plotov malo by sa dodržať:

- Oplotenie musí byť zostavené z plotových dielov, stĺpov,

- Všetky diely pozinkované a upravené povrchovou ochranou z PVC, mimo prípadu využitia žiletkového drôtu. Oká budú zvarované z dôvodu uzemnenia oplotenia, kde sa predpokladá príprava na uchytenie zemných páskov,
- Osová rozteč medzi jednotlivými stĺpikmi nesmie byť dlhšia ako 255 cm,
- Plotové diely s konštrukciou oka max 200 x 55 mm,
    - priemer drôtu
        - horizontálneho drôtu nesmie byť menšia ako 8 mm,
        - vertikálneho drôtu nesmie byť menšia ako 6 mm,

Alternatíva:

- Plotové diely s konštrukciou oka max 100 x 55 mm,
    - priemer drôtu
        - horizontálneho drôtu nesmie byť menšia ako 6 mm,
        - vertikálneho drôtu nesmie byť menšia ako 5 mm,
- Stĺpiky s priemerom 60 mm poprípade s podobným 70X45mm, pričom stena stĺpiku nesmie byť menšia ako 1,5 mm v pozinkovanej verzii s PVC povrchovou úpravou,
- Plotové dielce uchytené priamo do stĺpika tak, aby sa vylúčilo vysunutie alebo ich demontáž,
- Stĺpiky musia byť vsadené do zeme a spojené s boku opernými stenami podhrabovej dosky min. štyrmi kotvami alebo inou podobnou metódou, aby sa zabránilo demontáži. Základy budú z prefabrikovaných dielov,
- Životnosť oplotenia bez údržby nesmie byť nižšia ako 15 rokov a musí byť doložená certifikátom konkrétneho akreditovaného ústavu,
- Mechanická odolnosť musí byť dodávateľom stanovená na pevnosť v ťahu a to min. 400/550 Nmm^2 , predĺženie max. 15%, 40g zinku / m^2 a doložené certifikátom.

V nasledujúcej tabuľke stanovím ďalšie požiadavky na oplotenie pre jednotlivé bezpečnostné triedy, kde sa zameriam na parametre ako:

- Celková výška oplotenia,
- Rozmery podhrabovej dosky,

- Mechanická zábrana na korune,
- Udržované pásmo.

Oplotenie	**Bezpečnostná trieda a priradené bodové hodnoty**			
	I - 1	**II - 2**	**III - 3**	**IV - 4**
Celková výška oplotenia (vrátane podhrabovej dosky a mechanickej zábrany na korune)	min. 220 cm nad terénom,	min. 230 cm nad terénom,	min. 240 cm nad terénom,	min. 250 cm nad terénom,
Podhrabová doska	min. 20 cm nad terénom,	min. 20 cm nad terénom,	min. 30 cm nad terénom,	min. 30 cm nad terénom,
Mechanická zábrana na korune	Jednostranný bavolet	Jednostranný bavolet	Dvojstranný bavolet	Dvojstranný bavolet
Udržované pásmo	120 cm na obe strany	120 cm na obe strany	150 cm na obe strany	150 cm na obe strany

Tabuľka 6: Bezpečnostná trieda a priradené bodové hodnoty - oplotenie

V tomto smere sa predpokladá, že jednostranným bavoletom je mechanická zábrana na korune tvorená tromi radami žiletkového drôtu a dvojstranným je zábrana tvorená špirálou zo žiletkového drôtu.

6.3.2 Mechanické zábranné systémy perimetrickej ochrany – Vstupy a vjazdy

Nasledujúca tabuľka stanoví požiadavky na vstupy a vjazdy, ktoré vychádzajú z už definovaných požiadaviek na oplotenie, pričom sa predpokladá, že všeobecné požiadavky na konštrukciu vstupov a vjazdov budú vychádzať zo všeobecných požiadaviek na oplotenie.

Vstupy a vjazdy	**Bezpečnostná trieda a priradené bodové hodnoty**			
	I - 1	**II - 2**	**III - 3**	**IV - 4**
Celková výška oplotenia (vrátane mechanickej zábrany na korune)	min. 220 cm nad terénom,	min. 230 cm nad terénom,	min. 240 cm nad terénom,	min. 250 cm nad terénom,
Podhrabová doska – zpevnen povrch	min. 20 cm pod terénom,	min. 20 cm pod terénom,	min. 30 cm pod terénom,	min. 30 cm pod terénom,
Mechanická zábrana na korune	Jednostranný bavolet	Jednostranný bavolet	Dvojstranný bavolet	Dvojstranný bavolet
Uzamykací systém alebo visací zámok	Trieda 4	Trieda 5	Trieda 5	Trieda 5

Tabuľka 7: Bezpečnostná trieda a priradené bodové hodnoty – Vstupy a vjazdy

Táto časť práce sa zamerala na stanovenie požiadaviek na mechanické zábranné systémy, kde sa vychádzalo z určitého normotvorného procesu na jednej strane a na strane druhej z už existujúcich štandardov a požiadaviek implementovaných v rámci ochrany

dôležitých objektov, kde sa predpokladá, že tieto požiadavky budú vnímané aj v spojitosti so všeobecnými štandardami systému fyzickej ochrany prvkov kritickej infraštruktúry.

6.4 Hodnotenie elektronických prvkov ochrany pre jednotlivé bezpečnostné triedy

V súvislosti so stanovením požiadaviek na elektronické prvky ochrany budem postupovať rovnako ako v prípade stanovenia požiadaviek mechanických zábranných systémov teda sa budem odvolávať na už existujúce normy a to prevažne normy rady 50131, pričom budem zohľadňovať stupeň zabezpečenia (SZ) a triedu prostredia (TP) a v prípade CCTV systémov snímacie schopnosti kamier (identifikácia, rekognoskácia, detekcia a monitorovanie).

6.4.1 Elektronická zabezpečovacia signalizácia – EZS

Pre potreby práce si nadefinujem požiadavky pre jednotlivé bezpečnostné zóny na základe už definovaného referenčného objektu a štruktúry bezpečnostného systému. Vzhľadom na meniace sa podmienky a nekonštantnosť prostredia vytvorím priestor pre používanie konkrétnych detekčných systémov aby nevznikli prípady, kedy tento model nie je aplikovateľný. Je to určitá forma zovšeobecnenia podmienok, ktorá ma prispieť k širšiemu využitiu výstupov z tejto práce vyplývajúcich.

	Bezpečnostná trieda a priradené bodové hodnoty			
	I - 1	**II - 2**	**III - 3**	**IV - 4**
Perimetrická ochrana – zóna 1	EZS poďla rady noriem EN 50131 SZ 1, TP 4	EZS poďla rady noriem EN 50131 SZ 2, TP 4	EZS poďla rady noriem EN 50131 SZ 3, TP 4	EZS poďla rady noriem EN 50131 SZ 4, TP 4
Obvodová ochrana – zóna 2	EZS poďla rady noriem EN 50131 SZ 1, TP 4	EZS poďla rady noriem EN 50131 SZ 2, TP 4	EZS poďla rady noriem EN 50131 SZ 3, TP 4	EZS poďla rady noriem EN 50131 SZ 4, TP 4
Ochrana vonkajšieho priestoru – zóna 3	EZS poďla rady noriem EN 50131 SZ 1, TP 4	EZS poďla rady noriem EN 50131 SZ 2, TP 4	EZS poďla rady noriem EN 50131 SZ 3, TP 4	EZS poďla rady noriem EN 50131 SZ 4, TP 4
Ochrana vonkajšieho plášťa – zóna 4	EZS poďla rady noriem EN 50131 SZ 1, TP 4	EZS poďla rady noriem EN 50131 SZ 2, TP 4	EZS poďla rady noriem EN 50131 SZ 3, TP 4	EZS poďla rady noriem EN 50131 SZ 4, TP 4
Ochrana vnútorného priestoru – zóna 5	EZS poďla rady noriem EN 50131 SZ 1, TP 2	EZS poďla rady noriem EN 50131 SZ 2, TP 2	EZS poďla rady noriem EN 50131 SZ 3, TP 2	EZS poďla rady noriem EN 50131 SZ 4, TP 2
Ochrana vnútorného plášťa – zóna 6	EZS poďla rady noriem EN 50131 SZ 1, TP 2	EZS poďla rady noriem EN 50131 SZ 2, TP 2	EZS poďla rady noriem EN 50131 SZ 3, TP 2	EZS poďla rady noriem EN 50131 SZ 4, TP 2
Priestorová ochrana – zóna 7	EZS poďla rady noriem EN 50131 SZ 1, TP 1	EZS poďla rady noriem EN 50131 SZ 2, TP 1	EZS poďla rady noriem EN 50131 SZ 3, TP 1	EZS poďla rady noriem EN 50131 SZ 4, TP 1

	Bezpečnostná trieda a priradené bodové hodnoty			
	I - 1	**II - 2**	**III - 3**	**IV - 4**
Predmetová ochrana – zóna 8	EZS poďla rady noriem EN 50131 SZ 1, TP 1	EZS poďla rady noriem EN 50131 SZ 2, TP 1	EZS poďla rady noriem EN 50131 SZ 3, TP 1	EZS poďla rady noriem EN 50131 SZ 4, TP 1

Tabuľka 8: Bezpečnostná trieda a priradené bodové hodnoty - EZS

6.4.2 CCTV

Z prezentovanej štruktúry a základných funkcií bezpečnostného systému vyplýva, že kamerový systém je významným komponentom hlavne v súvislosti s podmienkou naplnenia základnej funkcie detection. Napriek skutočnosti, že CCTV systémy nie sú kategorizované požadovanými stupňami zabezpečenia a často sa používajú ako doplnok EZS, kde o spomínanej kategorizácii môžeme hovoriť, použijem túto kategorizáciu aj v nasledujúcej tabuľke. Vzhľadom na veľké spektrum ponúkaných systémov CCTV stanovím len obecné požiadavky na tento systém pričom hlavným rozlišovacím aspektom bude už spomínaná snímacia charakteristika (identifikácia, rekognoskácia, detekcia a monitorovanie).

CCTV	**Bezpečnostná trieda a priradené bodové hodnoty**			
	I - 1	**II - 2**	**III - 3**	**IV - 4**
CCTV systém č.1 a č.2	CCTV podľa normy EN 50132-7 s možnosťou monitorovania, SZ 2, TP4 vo vyhotovení antivandal	CCTV podľa normy EN 50132-7 s možnosťou detekcie, SZ 3, TP4 vo vyhotovení antivandal	CCTV podľa normy EN 50132-7 s možnosťou rekognoskácie, SZ 3, TP4 vo vyhotovení antivandal	CCTV podľa normy EN 50132-7 s možnosťou Identifikácie, SZ 4, TP4 vo vyhotovení antivandal
CCTV systém č.3	CCTV podľa normy EN 50132-7 s možnosťou monitorovania, SZ 2, TP2	CCTV podľa normy EN 50132-7 s možnosťou detekcie, SZ 3, TP2	CCTV podľa normy EN 50132-7 s možnosťou rekognoskácie, SZ 3, TP2	CCTV podľa normy EN 50132-7 s možnosťou Identifikácie, SZ 4, TP2
CCTV systém č.4	CCTV podľa normy EN 50132-7 s možnosťou monitorovania, SZ 2, TP1	CCTV podľa normy EN 50132-7 s možnosťou detekcie, SZ 3, TP1	CCTV podľa normy EN 50132-7 s možnosťou rekognoskácie, SZ 3, TP1	CCTV podľa normy EN 50132-7 s možnosťou Identifikácie, SZ 4, TP1

Tabuľka 9: Bezpečnostná trieda a priradené bodové hodnoty - CCTV

6.5 Hodnotenie fyzickej ostrahy a režimových opatrení pre jednotlivé bezpečnostné triedy

Využívanie fyzickej ostrahy a režimové opatrenia sú aj na základe definovaných funkcií systému fyzickej ochrany prvkov kritickej infraštruktúry významným subsystémom, ktorý rozhodujúcou mierou ovplyvňuje funkčnosť celého systému ako aj pravdepodobnosť úspešného zadržania či prerušenia činnosti páchateľa. V tejto časti definujem spôsob

hodnotenia fyzickej ostrahy a režimových opatrení a stanovím požiadavky na tento subsystém pre jednotlivé bezpečnostné triedy.

6.5.1 Fyzická ostraha

Pri stanovovaní požiadaviek a spôsobu hodnotenia budem vychádzať s už existujúcej legislatívy, ktorá aj na základe predošlých publikačných aktivít úzko súvisí s predmetnou problematikou a týka sa fyzickej bezpečnosti a objektovej bezpečnosti (vyhláška NBU 336/2004).

Požiadavky na fyzickú ostrahu pre jednotlivé bezpečnostné triedy	Bezpečnostná trieda	Priradená bodová hodnota
Fyzická ostraha sa vykonáva: • príslušníkmi ozbrojených bezpečnostných zborov, • obchôdzkami vo vnútri objektu, • prvá obchôdzka sa vykonáva bezprostredne po skončení pracovného času, pričom sa skontroluje uzatvorenie okien a dverí a zároveň sa identifikuje personál pracujúci v chránenom priestore po skončení pracovného času, • na stanovišti sa zabezpečí nepretržitá prítomnosť najmenej jedného člena fyzickej ostrahy.	IV	4
Fyzická ostraha sa vykonáva: • príslušníkmi ozbrojených zborov alebo trvalo prítomnou vlastnou ozbrojenou strážnou službou, • fyzická ostraha sa vykonáva obchôdzkami z vnútornej aj vonkajšej časti objektu, • na stanovišti sa zabezpečí nepretržitá prítomnosť najmenej jedného člena fyzickej ostrahy.	III	3
Fyzická ostraha sa vykonáva: • trvalou vlastnou ozbrojenou službou alebo ozbrojenými príslušníkmi súkromnej bezpečnostnej služby, • obchôdzkami popri vonkajšej časti objektu, • na stanovišti sa zabezpečí nepretržitá prítomnosť najmenej jedného člena fyzickej ostrahy.	II	2
Fyzická ostraha sa vykonáva: • trvalou vlastnou ozbrojenou službou alebo ozbrojenými	I	1

príslušníkmi súkromnej bezpečnostnej služby, • nevyžaduje obchôdzky a vykonáva sa spôsobom miestnej ochrany s využitím nepretržite prítomných osôb.		

Tabuľka 10: Požiadavky na fyzickú ostrahu pre jednotlivé bezpečnostné triedy

6.5.2 Režimové opatrenia

Z prezentovanej štruktúry systému fyzickej ostrahy nevyplýva význam využiteľnosti a režimových opatrení no napriek týmto skutočnostiam práve režimové opatrenia významným spôsobom dopĺňajú a skvalitňujú činnosť fyzickej ostrahy. V nasledujúcej tabuľke stanovím požiadavky na systém režimových opatrení pre jednotlivé bezpečnostné triedy a priradím k nim bodové hodnoty.

Požiadavky na systém režimových opatrení pre jednotlivé bezpečnostné triedy	Bezpečnostná trieda	Priradená bodová hodnota
• Kontrola funkčnosti systémov technickej ochrany. • Podmienky vstupu a výstupu osôb, vjazdu a výjazdu vozidiel do objektu a chráneného priestoru, v pracovnom a mimopracovnom čase. • Podmienky používania mobilných telefónov, videokamier, fotoaparátov či iných záznamových zariadení. • Podmienky na kontrolu objektu a chráneného priestoru po opustení pracoviska zamestnancami. • Podmienky používania, prideľovania, označovania, úschovy a evidencie originálov a kópií bezpečnostných kľúčov iných prístupových médií. • Podmienky používania, prideľovania, označovania, úschovy a evidencie kódových nastavení a hesiel pre prístup do objektov. • Podmienky postupu pri narušení či pri pokuse o narušenie objektu a chráneného priestoru. • Podmienky postupu v prípade mimoriadnej udalosti do ktorého patria plán na ochranu, evakuáciu s uvedením zodpovedných osôb.	IV	4
• Kontrola funkčnosti systémov technickej ochrany. • Podmienky vstupu a výstupu osôb, vjazdu a výjazdu vozidiel do objektu a chráneného priestoru, v pracovnom a mimopracovnom čase. • Podmienky používania mobilných telefónov, videokamier, fotoaparátov či iných záznamových zariadení. • Podmienky na kontrolu objektu a chráneného priestoru po opustení pracoviska zamestnancami. • Podmienky používania, prideľovania, označovania, úschovy a evidencie originálov a kópií bezpečnostných kľúčov iných prístupových médií. • Podmienky postupu pri narušení či pri pokuse o narušenie objektu a chráneného priestoru. • Podmienky postupu v prípade mimoriadnej udalosti do ktorého	III	3

patria plán na ochranu, evakuáciu s uvedením zodpovedných osôb.		
• Kontrola funkčnosti systémov technickej ochrany. • Podmienky vstupu a výstupu osôb, vjazdu a výjazdu vozidiel do objektu a chráneného priestoru, v pracovnom a mimopracovnom čase. • Podmienky na kontrolu objektu a chráneného priestoru. • Podmienky používania, prideľovania, označovania, úschovy a evidencie originálov a kópií bezpečnostných kľúčov iných prístupových médií. • Podmienky postupu pri narušení či pri pokuse o narušenie objektu a chráneného priestoru. • Podmienky postupu v prípade mimoriadnej udalosti do ktorého patria plán na ochranu, evakuáciu s uvedením zodpovedných osôb.	II	2
• Kontrola funkčnosti systémov technickej ochrany. • Podmienky vstupu a výstupu osôb, vjazdu a výjazdu vozidiel do objektu a chráneného priestoru, v pracovnom a mimopracovnom čase. • Podmienky používania, prideľovania, označovania, úschovy a evidencie originálov a kópií bezpečnostných kľúčov iných prístupových médií. • Podmienky postupu pri narušení či pri pokuse o narušenie objektu a chráneného priestoru.	I	1

Tabuľka 11: Požiadavky na systém režimových opatrení pre jednotlivé bezpečnostné tried

6.6 Metodika hodnotenia systému fyzickej ochrany prvkov kritickej infraštruktúry

Bodové hodnoty, ktoré boli stanovené pre jednotlivé bezpečnostné triedy pre mechanické zábranné systémy, elektronické prvky ochrany či fyzickú ostrahu a režimové opatrenia nám vytvorili rámec pre formulovanie požiadaviek na systém fyzickej ochrany prvkov kritickej infraštruktúry pre konkrétne bezpečnostné triedy. Tieto požiadavky rozdelím do jednotlivých skupín a tried v nasledujúcich tabuľkách.

Mechanické zábranné systémy – **M**:

Hodnota Mzs Zóny 2 m1	Hodnota Mzs Zóny 4 m2	Hodnota Mzs Zóny 6 m3	Hodnota Mzs Zóny 8 m4	Bezpečnostná trieda	Minim. hodnota MZS BT	Maxim. hodnota MZS BT
4	3	3	3	**IV**	13	16
3	2	2	2	**III**	9	12
2	1	1	1	**II**	5	8
1	1	1	0	**I**	3	4

Tabuľka 12: Hodnota mechanických zábranných systémov

Elektronické prvky ochrany - **E**:

Hodnota Epo Zóny 1 e1		Hodnota Epo Zóny 2 e2		Hodnota Epo Zóny 3 e3		Hodnota Epo Zóny 4 e4		Bezpečnostná trieda
8	e1E - 4	7	e2E - 3	6	e3E - 3	6	e4E - 3	IV
	e1C - 4		e1C - 4		e2C - 3		e2C - 3	
6	e1E - 3	5	e2E - 2	4	e3E - 2	4	e4E - 2	III
	e1C - 3		e1C - 3		e2C - 2		e2C - 2	
4	e1E - 2	3	e2E - 1	2	e3E - 1	2	e4E - 1	II
	e1C - 2		e1C - 2		e2C - 1		e2C - 1	
2	e1E - 1	2	e2E - 1	2	e3E - 1	2	e4E - 1	I
	e1C - 1		e1C - 1		e2C - 1		e2C - 1	
Hodnota Epo Zóny 5 e5		**Hodnota Epo Zóny 6 e6**		**Hodnota Epo Zóny 7 e7**		**Hodnota Epo Zóny 8 e8**		**Bezpečnostná trieda**
6	e5E - 3	6	e6E - 3	6	e7E - 3	6	e8E - 3	IV
	e3C - 3		e3C - 3		e4C - 3		e4C - 3	
4	e5E - 2	4	e6E - 2	4	e7E - 2	4	e8E - 2	III
	e3C - 2		e3C - 2		e4C - 2		e4C - 2	
2	e5E - 1	2	e6E - 1	2	e7E - 1	2	e8E - 1	II
	e3C - 1		e3C - 1		e4C - 1		e4C - 1	
2	e5E - 1	2	e6E - 1	2	e7E - 1	1	e8E - 0	I
	e3C - 1		e3C - 1		e3C - 1		e3C - 1	

Tabuľka 13: Elektronické prvky ochrany

Hodnota elektronických prvkov ochrany pre jednotlivé bezpečnostné triedy – **EPO BT**:

Bezpečnostná trieda	Minim. hodnota EPO BT	Maxim. hodnota EPO BT
IV	51	64
III	35	50
II	19	34
I	15	18

Tabuľka 14: Hodnota elektronických prvkov ochrany

Fyzická ostraha a režimové opatrenia – **F:**

Hodnota FO f1	Hodnota RO f2	Bezpečnostná trieda	Min. hodnota F	Max. hodnota F
4	3	IV	7	8
3	2	III	5	6
2	1	II	3	4
1	1	I	2	2

Tabuľka 15: Hodnota fyzickej ostrahy a režimových opatrení

Na základe tohto stanovenia minimálnych a maximálnych hodnôt jednotlivých komponentov bezpečnostného systému môžeme stanoviť celkovú hodnotu systému fyzickej ochrany prvkov kritickej infraštruktúry pre jednotlivé bezpečnostné triedy. Je možné konštatovať, že koncové hodnoty budú sumami hodnôt jednotlivých komponentov podľa vzťahu:

$$B = \sum_{i=m1}^{m4} M_i + \sum_{i=e1}^{e8} E_i + \sum_{i=f1}^{f2} F_i \qquad (6.1)$$

Na základe tohto vzťahu dostaneme tabuľku maximálnych a minimálnych hodnôt systému fyzickej ochrany pre jednotlivé prvky KI:

Minim. hodnota MZS BT	Minim. hodnota EPO BT	Min. hodnota F BT	Bezpečnostná trieda	Minimálna hodnota SFO B	Maximálna hodnota FSO B
13	51	7	**IV**	71	**88**
9	35	5	**III**	49	70
5	19	3	**II**	27	48
3	15	2	**I**	**20**	26

Tabuľka 16: Hodnota bezpečnostného systému prvku kritickej infraštruktúry

Vyjadrenie maximálnych a minimálnych požadovaných hodnôt systému fyzickej ochrany prvku kritickej infraštruktúry pre jednotlivé bezpečnostné triedy vytvára priestor aj na hodnotenie priemernej úrovne resp. hodnoty systémov fyzickej ochrany pre konkrétny sektor KI, keďže prvky KI sú vnímané ako elementárne zložky sektoru. Pre stanovenie priemernej hodnoty systémov fyzickej ochrany vnímanej ako úroveň ochrany v danom sektore použijeme vzťahy:

$$B_{norm} = \frac{B - B_{\min}}{B_{\max} - B_{\min}} \qquad (6.2) \qquad O_{ki} = \frac{1}{K}\sum_{k=1}^{K} B_{norm,k} \qquad (6.3)$$

Kde:

B_{min} – 20

B_{max} – 88

O_{ki} – hodnota úrovne ochrany v rámci sektoru

K – počet prvkov kritickej infraštruktúry v danom sektore

Po dosadení stanovených hodnôt do týchto vzťahov dostaneme intervaly, ktoré si môžeme kvalitatívne pomenovať a vytvoriť tak základ pre stanovenie požadovanej úrovne ochrany v danom sektore:

Interval	Úrovne ochrany KI v danom sektore
<-0,294; -0,014>	nevyhovujúca
<0; 0,088>	veľmi nízka
<0,103; 0,412>	nízka
<0,426; 0,735>	stredná
<0,750; 1>	vysoká úroveň ochrany

Tabuľka 17: Úroveň ochrany kritickej infraštruktúry v danom sektore

Kvantitatívne vyjadrenie úrovne systémov fyzickej ochrany je vhodným spôsobom pre vytvorenie určitého komparačného nástroja, ktorý bude následne slúžiť ECIP čiže národným entitám určeným a označeným ako európsky kontaktný bod pre ochranu kritickej

infraštruktúry na poukázanie rozdielnosti a nekonštantnosti úrovne systému fyzickej ochrany v rámci daného sektoru a následne stanoviť požiadavky na zvýšenie tejto úrovne v závislosti na kritickosť resp. dôležitosť prvku či celého sektoru z pohľadu zabezpečenia funkčnej kontinuity.

6.7 Vyjadrenie funkčnosti systému fyzickej ochrany na základe pravdepodobností a prielomových odolností pre jednotlivé bezpečnostné triedy

Definovanie štrukturálnych požiadaviek na systémy fyzickej ochrany pre prvky KI však nezabezpečuje a nepopisuje jeho reálne funkčné vlastnosti, ktoré sú vnímané ako významný hodnotiaci aspekt. Vzhľadom na túto skutočnosť v nasledujúcej časti stanovím a definujem požiadavky na funkčné vlastnosti, ktoré vyplývajú z už uvedených požiadaviek na jednotlivé komponenty. Jedná sa predovšetkým o prielomovú odolnosť mechanických zábranných systémov, pravdepodobnosť správnej detekcie EZS či časovú závislosť overovania poplachovej informácie systémom CCTV. V tomto smere budem vychádzať ako v predošlej kapitole aj z pripravovanej normy ČSN/P CEN/TS 14383-3 zameranej na prevenciu kriminality, kde sú stanovené úrovne odolnosti proti manuálnemu napadnutiu dverí okeníc a okien. Následne pre ostatné komponenty budú tieto prielomové odolnosti stanovené. V súvislosti s pravdepodobnosťou detekcie stanovím požiadavky na celkovú pravdepodobnosť v konkrétnej zóne a na časovú závislosť overovania poplachovej informácie. Tento prístup je použitý v kontexte s využiteľnosťou modelu EASI (Estimate of Adversary Sequence Interruption), ktorého vstupnými parametrami sú práve parametre stanovené v nasledujúcich častiach.

6.7.1 Mechanické zábranné systémy a prielomová odolnosť

V spomínanej pripravovanej norme sú v prílohe A tabuľky 3 formulované požadované úrovne odolnosti (prielomovej odolnosti) proti manuálnemu napadnutiu dverí, okeníc a okien. Toto stanovenie prielomových odolností je použiteľné aj v kontexte dizertačnej práce preto budem z neho vychádzať.

Úroveň odolnosti	**Doba odolnosti** (v minútach)	**Maximálne trvanie skúšky** (v minútach)	**Možný spôsob vniknutia**
1	3	5	Príležitostný páchateľ, ktorý skúša otvoriť okno, dvere alebo okenice s použitím fyzické sily kopnutím, vyrazením ramenom, naddvihnutím alebo odtrhnutím.
2	3	15	Príležitostný páchateľ, ktorý skúša otvoriť okno, dvere alebo okenice aj pomocou jednoduchých nástrojov, napr. pomocou šraubováku, klieští alebo klinu.
3	5	20	Príležitostný páchateľ, ktorý sa pokúša o vniknutie pomocou dvoch alebo viacerých šraubovákov a páčidla.
4	10	30	Skúsený páchateľ používajúci aj pílu, kladivo a dláto, sekeru a prenosnú akumulátorovú vŕtačku.
5	15	40	Skúsený páchateľ používajúci aj elektrické náradie, napr. vŕtačku, elektrickú pílu a uhlovú brúsku s kotúčom o priemere max. 125 mm.
6	20	50	Skúsený páchateľ používajúci aj elektrické náradie, napr. vŕtačku, priamočiaru pílu a uhlovú brúsku s kotúčom o priemere max.230 mm.

Tabuľka 18: Prielomová odolnosť mechanických zábranných systémov podľa úrovní odolnosti

Po použití tohto prístupu a stanovenia prielomových odolností dosadím tieto parametre do už špecifikovanej tabuľky pre stanovenie štruktúry mechanických zábranných systémov. V súvislosti s úschovnými objektmi budem vychádzať zo vzorca [44]:

$$T_{vl} = \frac{V_r - BV}{C_1} \qquad (6.4)$$

Kde:

T_{vl} - hodnota minimálnej prielomovej odolnosti úschovného objektu

V_r - hodnota prielomovej odolnosti úschovného objektu (RU)

BV - základné ohodnotenie určitého náradia

C_1 - koeficient prielomovej odolnosti úschovného objektu

Na základe tohto vzťahu som dosadil spomínané premenné, čo sa prejaví v konečnej tabuľke:

Mechanický zábranný systém	**Európska norma**	**Minimálna prielomová odolnosť pre jednotlivé bezpečnostné triedy**			
		I	**II**	**III**	**IV**
Vchodové dvere	ENV 1627	5 min.	10 min.	15 min.	20 min.
Bezpečnostný zámok	EN 12209	15 min.	20 min.	20 min.	20 min.
Cylindrická vložka	EN 1303	15 min.	20 min.	20 min.	20 min.
Dvere v ktorých je zámok uložený	EN 1906	10 min	20 min.	20 min.	20 min.

Mechanický zábranný systém	**Európska norma**	**Minimálna prielomová odolnosť pre jednotlivé bezpečnostné triedy**			
		I	**II**	**III**	**IV**
Dosažiteľné okná	ENV 1627	10 min	10 min	15 min.	20 min.
Dosažiteľné zasklené plochy	EN 356	5 min.	10 min	15 min.	20 min.
Okenice chrániace dosažiteľné okná alebo dvere	ENV 1627	5 min.	10 min	15 min.	20 min.
Okna alebo dvere dosiahnuteľné iba z rebríku	ENV 1627	3 min.	3 min.	5 min.	10 min
Zasklenie dosiahnuteľné iba z rebríku	EN 356	3 min.	3 min.	3 min.	5 min.
Úschovné objekty	EN 1143	9 min.	11 min.	16 min.	23 min.

Tabuľka 19: Minimálna prielomová odolnosť pre jednotlivé bezpečnostné triedy – mechanické zábranné systémy

Podobne ako v prípade stanovenia požiadaviek na štruktúru jednotlivých komponentov mechanických zábranných systémov, normatívne absentuje charakteristika oplotenia a jeho súčastí, preto pre túto časť stanovím prielomovú odolnosť, ktorá bude vychádzať aj z penetračných testov oplotenia (charakteristického podľa stanovenej štruktúry) spoločnosti Dirickx Bohemia s.r.o..

Oplotenie a jeho uzamykací systém	**Minimálna prielomová odolnosť pre jednotlivé bezpečnostné triedy**			
	I	**II**	**III**	**IV**
Požadovaná prielomová odolnosť oplotenia	90s	120s	150 s	180 s
Uzamykací systém alebo visací zámok EN 1303	15 min.	20min.	20 min.	20 min.

Tabuľka 20: : Minimálna prielomová odolnosť pre jednotlivé bezpečnostné triedy – oplotenie a jeho uzamykací systém

Formulovanie a stanovenie prielomových odolností je jedným z funkčných ukazovateľov, ovplyvňujúcich celkovú funkčnosť systému fyzickej ochrany prvkov KI. Je zrejmé, že určité komponenty mechanických zábranných systémov nemajú definovanú minimálnu požadovanú prielomovú odolnosť, preto riešením tohto stavu je jej stanovenie, ktoré vytvorí priestor na normatívnu charakteristiku a definovanie aj v rámci pripravovaného normalizačného procesu v súvislosti s technickou normalizačnou komisiou pre prevenciu kriminality.

6.7.2 EZS a pravdepodobnosť správnej detekcie

Vzhľadom na skutočnosť, že normatívne nie sú stanovené požiadavky na pravdepodobnosť detekcie jednotlivých detekčných systémov je vhodnou alternatívou jej stanovenie na základe vedomostnej základne už prezentovanej v tejto práci a v súvislosti s potrebami modelu EASI a s potrebami stanovenia pravdepodobnosti úspešného prerušenia činnosti narušiteľa v stráženom objekte. V prípade, že by model EASI nebol použitý pre komplexné vyjadrenie spomínanej pravdepodobnosti je možné použiť vzťahy[10], ktoré sú však štatisticky nezávislé a použité v súvislosti so zjednodušením vyjadrenia potrebných pravdepodobností:

$$P_{KD} = \left[1 - \prod_{i=1}^{n}(1 - P_{Di})\right] * P_{PPS} * P_P * P_{LF} \qquad (6.5)$$

Kde:

P_{KD} – kumulatívna pravdepodobnosť správnej detekcie narušiteľa

n – počet detekčných zón počas cesty narušiteľa

P_{Di} – pravdepodobnosť správnej detekcie v i-itej detekčnej zóne počas cesty narušiteľa.

P_P – pravdepodobnosť bezporuchového stavu EZS

P_{PPS} – pravdepodobnosť prenosu poplachového signálu

P_{LF} – spoľahlivosť ľudského faktoru

Následne by sa s využitím tohto vzťahu a výstupov z neho vyplývajúcich stanovila pravdepodobnosť úspešnosti zásahu fyzickej ostrahy na základe vzťahu[10]:

$$P_Z = P_{KD} * P_R \qquad (6.6)$$

Kde:

P_Z – pravdepodobnosť zásahu zásahovej jednotky

P_{KD} – kumulatívna pravdepodobnosť správnej detekcie narušiteľa

P_R – pravdepodobnosť včasného a správneho vyhodnotenia poplachového stavu

Aj z týchto vzťahov je zrejmá potreba stanovenia celkovej pravdepodobnosti správnej detekcie pričom pre potreby tejto práce stanovím minimálnu celkovú pravdepodobnosť systémov EZS pre jednotlivé zóny, ktorá bude akceptovať aj rôznorodosť použitia

jednotlivých systémov, pričom sa berú do úvahy aj rôzne detekčné (matematické) logiky (or a and).

	Minimálna požadovaná celková pravdepodobnosť detekcie EZS			
	I	**II**	**III**	**IV**
Perimetrická ochrana – zóna 1	0,9	0,9	0,95	0,95
Obvodová ochrana – zóna 2	0,9	0,9	0,95	0,95
Ochrana vonkajšieho priestoru – zóna 3	0,9	0,9	0,95	0,95
Ochrana vonkajšieho plášťa – zóna 4	0,9	0,9	0,95	0,95
Ochrana vnútorného priestoru – zóna 5	0,9	0,9	0,95	0,95
Ochrana vnútorného plášťa – zóna 6	0,9	0,9	0,95	0,95
Priestorová ochrana – zóna 7	0,9	0,9	0,95	0,95
Predmetová ochrana – zóna 8	0	0,9	0,95	0,95

Tabuľka 21: Minimálna požadovaná celková pravdepodobnosť detekcie EZS

6.7.3 CCTV – stanovenie časovej závislosti overenia poplachovej informácie

Overenie poplachovej informácie je významným aspektom a súčasťou jednej z hlavných funkcií systému fyzickej ochrany - detection. V prípade neoverenia tejto informácie sa výrazným spôsobom predlžuje reakčný čas fyzickej ostrahy. Aj na základe tejto skutočnosti sú časové hodnoty stanovené rádovo v sekundách aby nedochádzalo k znižovaniu prielomových odolností jednotlivých bezpečnostných zón. Hodnoty vychádzajú z teoretickej základne, ktorá je určitým prienikom armádneho a civilného sektoru.

CCTV	**Minimálne časové hodnoty potrebné na overenie poplachovej informácie**			
	I	**II**	**III**	**IV**
CCTV systém č.1 a č.2	15s	15s	10s	10s
CCTV systém č.3	10s	10s	5s	5s
CCTV systém č.4	10s	10s	5s	5s

Tabuľka 22: Minimálne časové hodnoty potrebné na overenie poplachovej informácie

6.7.4 Stanovenie pravdepodobnosti úspešnej komunikácie fyzickej ostrahy

Jedným z posledných funkčných ukazovateľov, ktorý je potrebné stanoviť a formulovať je spomínaná pravdepodobnosť úspešnej komunikácie fyzickej ostrahy. V tomto prípade sa predpokladá a vychádza z testov v Sandia National Laboratories [3], kde hodnota pravdepodobnosti mala priemernú hodnotu 95%. Z analýzy dostupných metodík je pre stanovenie spomínanej pravdepodobnosti aj vzhľadom na náročnosť tohto procesu a absenciu štatistických údajov, možné použiť vzťah, ktorý sa primárne používa na stanovenie pravdepodobnosti prenosu poplachového systému cez poplachovú prenosovú cestu a je možné ho vnímať aj ako určitý koeficient spoľahlivosti systému [11]:

$$MD = \left(\frac{(1 - S_p)}{P_m * P_{kk}} * 100\% \right) \qquad (6.7)$$

kde:

MD – mesačná dostupnosť [%]

S_p – súčet časových porúch [min]

P_m – priemerný počet minút v jednom mesiaci (43 800)

P_{kk} – počet komunikačných kanálov,

Aj na základe tohto vzťahu a z poznatkov prezentovaných v rámci odborných konferencií je možné špecifikovať požadovanú pravdepodobnosť úspešnej komunikácie fyzickej ostrahy na:

	Minimálne hodnoty pravdepodobnosti úspešnej komunikácie FO			
	I	**II**	**III**	**IV**
Pravdepodobnosti úspešnej komunikácie FO v období jedného roka.	0,970	0,993	0,995	0,998

Tabuľka 23: Minimálne hodnoty pravdepodobnosti úspešnej komunikácie FO

Táto kapitola stanovila a definovala funkčné požiadavky systému fyzickej ochrany prvku KI pričom ako som v úvode už naznačil vychádzal som s už existujúcich prípadne pripravovaných normatívnych dokumentov. Naplnenie hlavnej funkcie detection a stanovenie parametrov komponentov tejto funkcie vychádzalo z objektívnych potrieb v rámci riešenia komplexnej ochrany, rôznych podmienok použitia konkrétnych EZS či s potrebami a požiadavkami na systém CCTV ako aspektu overovania poplachových informácií.

V súvislosti s funkciou systému delay sa vychádza z pripravovanej normy ČSN/P CEN/TS 14383-3, ktorej súčasťou bude aj problematika KI, ako aj z už prijatých a používaných noriem. V súvislosti s absenciou definovania normatívnych požiadaviek na oplotenie a jeho súčasti boli pre potreby tejto práce stanovené minimálne prielomové odolnosti, ktoré sú však podložené penetračnými testami.

Formulovanie požiadaviek na funkciu systému response budem vychádzať z konkrétnych simulácii na armádnom simulačnom nástroji OTB SAF (One Tested Baseline Semi Automated Force), ktorý dokáže reálne zhodnotiť a nasimulovať čas potrebný jednak na prekonanie definovaných bezpečnostných zón neobsahujúcich mechanické zábranné systémy ako aj činnosť fyzickej ostrahy v danom objekte a jej reakčné časy.

6.8 Posudzovanie funkčnosti systému fyzickej ochrany pomocou modelu EASI

Stanovenie funkčných požiadaviek na jednotlivé komponenty systému fyzickej ochrany objektov je vnímané v súvislosti s posudzovaním a hodnotením funkčných parametrov systému ako celku. V kontexte s týmto posudzovaním a hodnotením je vhodné použiť vhodnú formu informačnej podpory, ktorá bude zohľadňovať parametre, štruktúru a hlavné funkcie tohto systému. Vo vzťahu k zameraniu dizertačnej práce je možnou informačnou podporou práve využitie už spomínaného modelu EASI (Estimate of Adversary Sequence Interruption – pravdepodobnosť prerušenia činnosti narušiteľa [12]), ktorý vhodným spôsobom posudzuje funkčnosť a ako výstup je vnímaná pravdepodobnosť úspešného prerušenia činnosti narušiteľa v stráženom objekte teda v rámci objektu prvku KI.

6.8.1 Model EASI (Estimate of Adversary Sequence Interruption/ pravdepodobnosť prerušenia činnosti narušiteľa)

Ako som už naznačil vhodná informačná podpora na posudzovanie funkčnosti systému fyzickej ochrany by mala zohľadňovať a využívať závislosti, ktoré vyplývajú zo základnej štruktúry, funkčných požiadaviek a hlavných funkcií systému, ktorý bol prezentovaný v predošlých častiach práce. Tieto závislosti je možné vyjadriť aj vzťahom [3]:

$$P_D = P_S * P_T * P_A \qquad (6.8)$$

Kde:

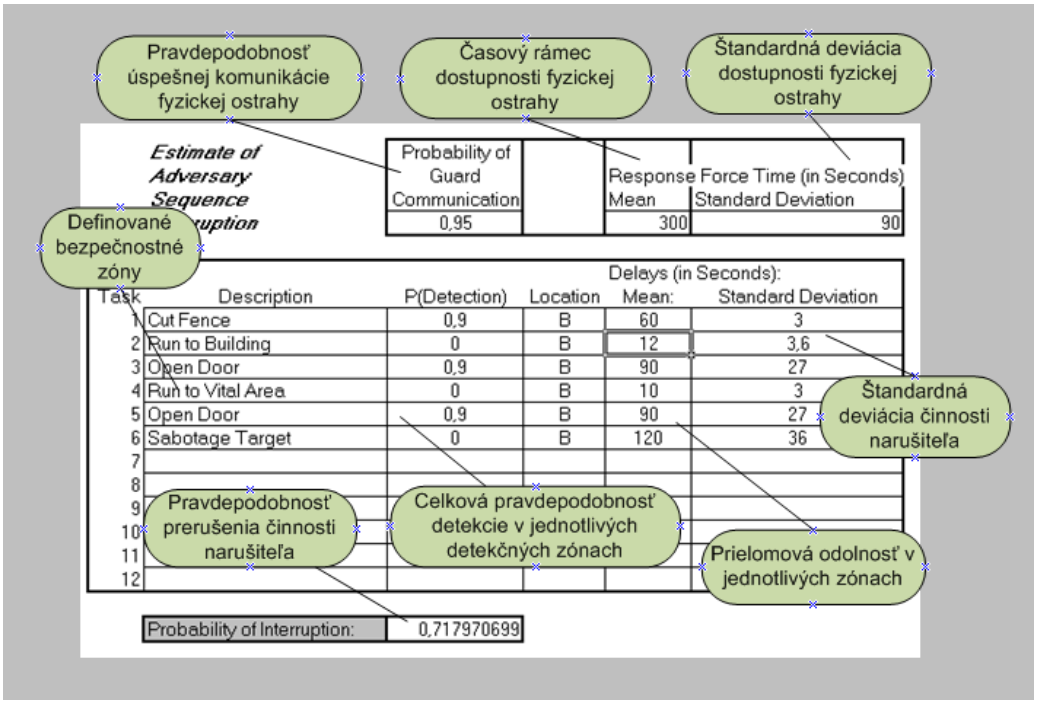
P_D - Pravdepodobnosť správnej detekcie,

P_S - Pravdepodobnosť schopnosti detekcie,

P_T - Pravdepodobnosť úspešného prenosu,

P_A - Pravdepodobnosť úspešného vyhodnotenia,

V súvislosti s týmto faktom bol pre tieto účely zvolený model EASI, ktorý aj podľa obrázku posudzuje a pracuje s už stanovenými parametrami komponentov systému fyzickej ochrany.



Obrázok 17: Model EASI

V súvislosti s používaním tohto modelu je nutné konštatovať, že štandardná deviácia (stredná kvadratická odchýlka spracovania štatistických údajov (σ)) je stanovená na 30% pričom táto hodnota korešponduje s výskumnou činnosťou Sandia National Laboratories, ktorá bola čiastočne prezentovaná v publikácii Mary Lynn Garcia Physical Protection Systems (2007) [3]. Pre potreby dizertačnej práce bude hodnota 30% použitá len v súvislosti s bezpečnostnými zónami, kde je pevne stanovená prielomová odolnosť.

6.8.2 Využiteľnosť modelu EASI v problematike hodnotenia funkčnosti systému fyzickej ochrany prvkov KI zaradených do jednotlivých bezpečnostných tried.

V nasledujúcej časti dosadím minimálne parametre komponentov definovaného systému fyzickej ochrany v konkrétnej bezpečnostnej triede do modelu EASI, pričom hodnota štandardnej deviácie v zónach, kde je možné jej hodnotu získať využitím ďalšej vhodnej formy informačnej podpory nebude vyjadrená. Hodnoty prielomových odolností v zónach kde sú použité mechanické zábranné systémy budú vyjadrovať prielomovú odolnosť najslabšieho

článku v danom systéme od ktorej sa odpočíta čas potrebný na overenie poplachovej informácie za predpokladu úspešnej detekcie.

Bezpečnostná trieda I:

Estimate of Adversary Sequence Interruption	Pravdepodo. úspešnej komunikácie		Dostup. fyzick. ostrahy:	(v sekundách) Štandardná deviácia
	0,97		?	?

	Zóny	P(Detecie)	Bez.Tr.	Prielom. (v sekundách): Odolnosť:	Štandardná deviácia
1	Zóna 1	0,9	I	?	?
2	Zóna 2	0,9	I	75	22,5
3	Zóna 3	0,9	I	?	?
4	Zóna 4	0,9	I	285	85,5
5	Zóna 5	0,9	I	?	?
6	Zóna 6	0,9	I	285	85,5
7	Zóna 7	0,9	I	?	?
8	Zóna 8	0	I	0	0
9					
10					
11					
12					

Pravdep. úsp.prerušenia :	#HODNOTA!

Obrázok 18: Model EASI – Bezpečnostná trieda I

Bezpečnostná trieda II:

Estimate of Adversary Sequence Interruption	Pravdepodo. úspešnej komunikácie		Dostup. fyzick. ostrahy:	(v sekundách) Štandardná deviácia
	0,993		?	?

	Zóny	P(Detecie)	Bez.Tr.	Prielom. (v sekundách): Odolnosť:	Štandardná deviácia
1	Zóna 1	0,9	II	?	?
2	Zóna 2	0,9	II	105	31,5
3	Zóna 3	0,9	II	?	?
4	Zóna 4	0,9	II	285	85,5
5	Zóna 5	0,9	II	?	?
6	Zóna 6	0,9	II	290	87
7	Zóna 7	0,9	II	?	?
8	Zóna 8	0,9	II	530	159
9					
10					
11					
12					

Pravdep. úsp.prerušenia :	#HODNOTA!

Obrázok 19: Model EASI – Bezpečnostná trieda II

Bezpečnostná trieda III:

Estimate of Adversary Sequence Interruption

Pravdepodo. úspešnej komunikácie		Dostup. fyzick. (v sekundách) ostrahy:	Štandardná deviácia
0,995		?	?

	Zóny	P(Detecie)	Bez.Tr.	Prielom. (v sekundách): Odolnosť:	Štandardná deviácia
1	Zóna 1	0,95	III	?	?
2	Zóna 2	0,9	III	140	42
3	Zóna 3	0,9	III	?	?
4	Zóna 4	0,9	III	590	177
5	Zóna 5	0,9	III	?	?
6	Zóna 6	0,9	III	590	177
7	Zóna 7	0,9	III	?	?
8	Zóna 8	0,9	III	650	195
9					
10					
11					
12					

Pravdep. úsp.prerušenia :	#HODNOTA!

Obrázok 20: Model EASI – Bezpečnostná trieda III

Bezpečnostná trieda IV:

Estimate of Adversary Sequence Interruption

Pravdepodo. úspešnej komunikácie		Dostup. fyzick. (v sekundách) ostrahy:	Štandardná deviácia
0,998		?	?

	Zóny	P(Detecie)	Bez.Tr.	Prielom. (v sekundách): Odolnosť:	Štandardná deviácia
1	Zóna 1	0,95	IV	?	?
2	Zóna 2	0,95	IV	170	51
3	Zóna 3	0,95	IV	?	?
4	Zóna 4	0,95	IV	890	267
5	Zóna 5	0,95	IV	?	?
6	Zóna 6	0,95	IV	895	268,5
7	Zóna 7	0,95	IV	?	?
8	Zóna 8	0,95	IV	955	286,5
9					
10					
11					
12					

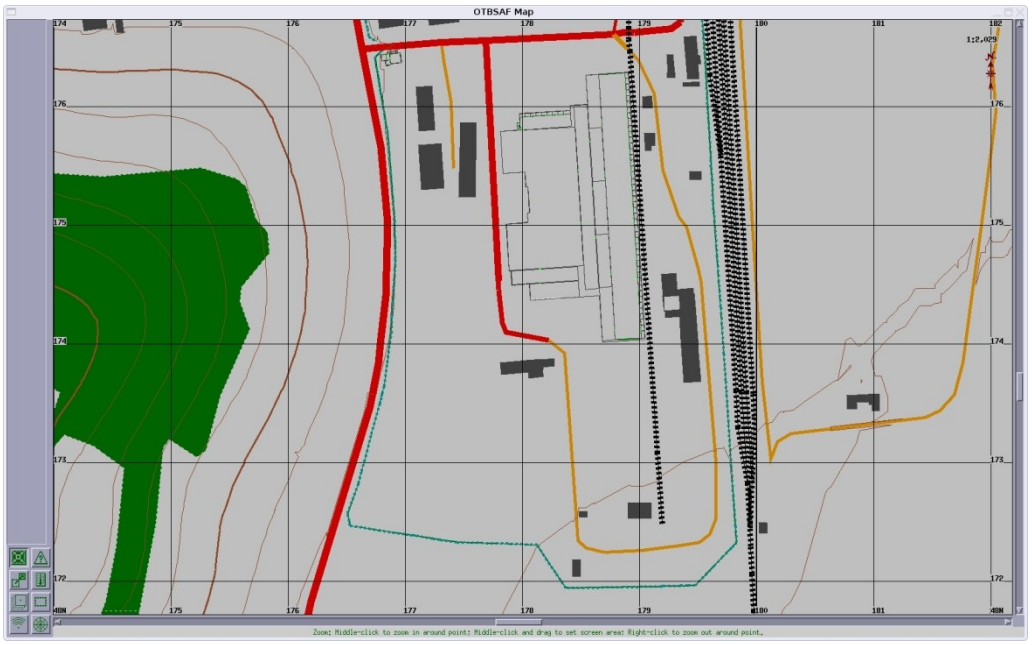
Pravdep. úsp.prerušenia :	#HODNOTA!

Obrázok 21: Model EASI – Bezpečnostná trieda IV

Z uvedených obrázkov je zrejmé, že v zónach, kde sa neboli použité mechanické zábranné systémy je prielomová odolnosť vyjadrená časom potrebným na prekonanie danej zóny, pričom sa bude vychádzať z individuálnosti jednotlivých objektov, čo platí aj pre stanovenie reakčného času fyzickej ostrahy v danom objekte. V tomto smere je potrebné využiť takú formu informačnej podpory, ktorá by bola schopná simulovať a pracovať v reálnych podmienkach, čo by vytvorilo rámec pre relevantné časové údaje použiteľné v súvislosti s prielomovou odolnosťou v modeli EASI.

6.8.3 Stanovenie štandardnej deviácie pomocou simulačného nástroja OTB SAF

Takýmto nástrojom resp. informačnou podporou by mohol byť simulačný nástroj OTB SAF. Tento systém či simulačný nástroj je prioritne používaný v súvislosti s praktickým overením rozhodovacieho procesu a činností veliteľa, plánovacieho procesu, plánovania fáz operácií z časového a priestorového hľadiska. Tento systém simuluje procesy a javy v reálnom alebo špecifikovanom čase a prostredí, s cieľom dosiahnuť najväčšiu mieru reálnosti.



Obrázok 22: Grafické rozhranie OTB SAF

Cieľom tohto systému je simulácia správania spracovaných modelov bojových prostriedkov a jednotiek ozbrojených síl v prostredí virtuálneho bojiska. Simulácia prebieha na základe vopred nadefinovaných parametrov, ktoré zabezpečujú správanie sa systému podľa noriem a zásad používaných v severoatlantickej aliancii. Práve nastavenie správnych parametrov je rozhodujúcim faktorom pri príprave cvičenia či simulácie.

Vzhľadom na určitú zmenu potreby využiteľnosti ozbrojených síl je tento nástroj možné použiť aj v súvislosti s:

- Krízovým manažmentom,
- Kontamináciou osôb,
- Epidémiami a chorobami,
- Logistickou podporou,

- Štatistikou atď.

Zo stručnej charakteristiky systému OTB SAF je zrejmá vhodnosť použitia tohto nástroja aj v kontexte činnosti narušiteľa a príslušníkov fyzickej ostrahy. Tento systém má na základe svojej štruktúry možnosť simulovať časový rámec pohybu narušiteľa a fyzickej ostrahy a tým pádom vytvoriť informačnú a dátovú podporu pre model EASI. Výstupom tohto systému by boli časové údaje, ktoré by boli vnímané jednak ako prielomové odolnosti a súčasne aj ako zdroj informácií pre výpočet štandardnej deviácie, ktorá je vyjadrením strednej kvadratickej odchýlky spracovania štatistických údajov (σ), na základe vzťahu[3]:

$$S_n = \sqrt{\frac{\sum_{i=1}^{n}(x_i - x_{pr})^2}{n-1}} \tag{6.9}$$

Kde:

S_n - štandardná deviácia

x_i - časová hodnota i – tej činnosti

x_{pr} - priemerná časová hodnota danej činnosti

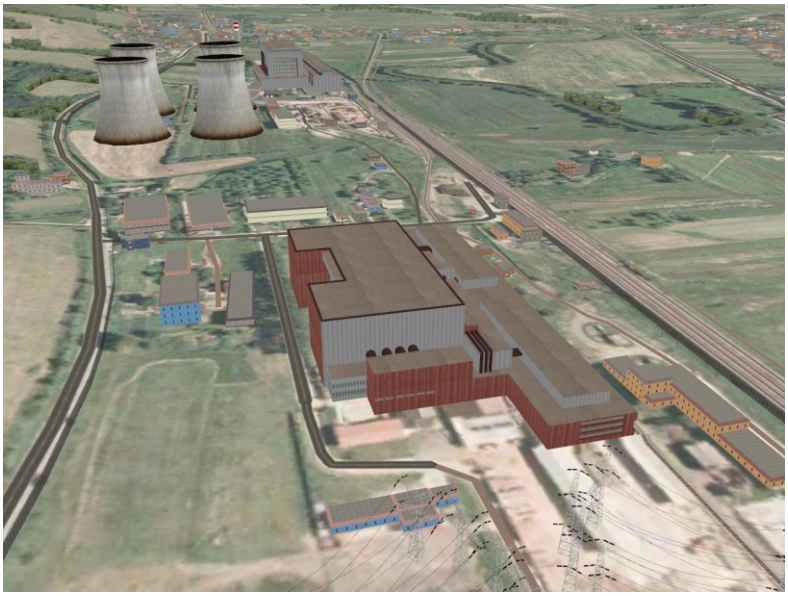
n - počet simulácií

Po dosadení časových závislostí do daného vzťahu je stanovená štandardná deviácia pre konkrétnu bezpečnostnú zónu poprípade deviácia časového vyjadrenia činnosti fyzickej ostrahy, čo vytvorí základ pre kompletizáciu modelu EASI, z čoho vyplýva aj výpočet pravdepodobnosti prerušenia činnosti narušiteľa pre jednotlivé bezpečnostné triedy prvkov kritickej infraštruktúry.

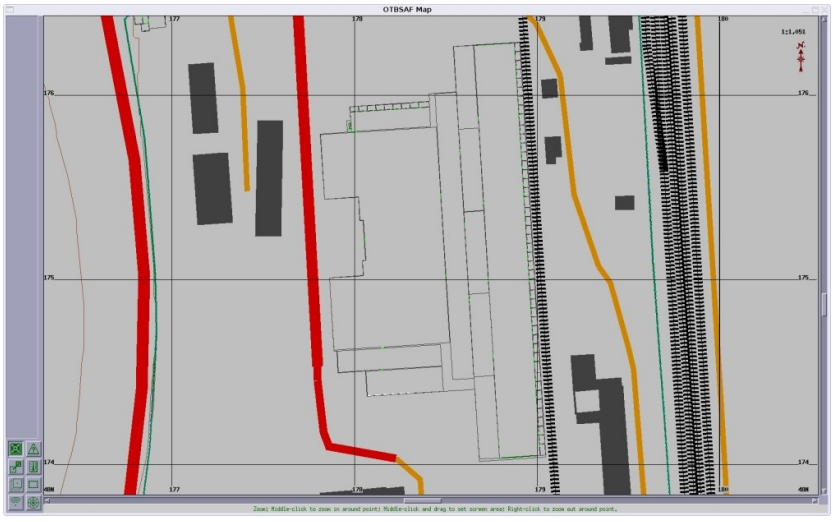
6.8.4 Praktické využitie simulačného nástroja OTB SAF

Pred konkrétnou simuláciou časových závislostí pohybu narušiteľa a fyzickej ostrahy je nutné definovať a aplikovať parametre bezpečnostných zón, ktoré v prípade, kedy je stanovená prielomová odolnosť budú vnímané ako určité checkpointy. Časové hľadisko prekonania týchto bodov bude totožné so stanovenou prielomovou odolnosťou. V zónach kde nie je stanovená prielomová odolnosť sa bude posudzovať nekonštantnosť pohybu narušiteľa a tým pádom rozdielnosť časových parametrov. Tento prístup sa uplatní aj kontexte s činnosťou a reakčným časom fyzickej ostrahy.

V predošlom texte definované parametre bezpečnostných zón boli implementované do vytvoreného fiktívneho objektu, ktorý je svojim charakterom vnímaný ako prvok kritickej infraštruktúry. Pre potreby dizertačnej práce bol v súčinnosti s pracovníkmi simulačného centra Akadémie ozbrojených síl gen. M. R. Štefánika vytvorený model objektu jadrovej elektrárne Obr. 23 a 24 v ktorom boli zohľadnené a implementované prístupy v predošlom texte prezentované.



Obrázok 23: 3D model objektu elektrárne

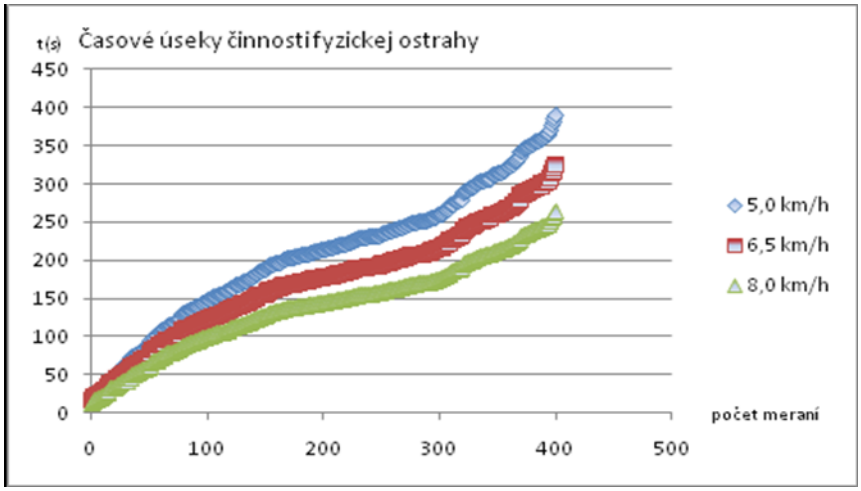


Obrázok 24: 2D model objektu elektrárne

Pre kompletizáciu modelu EASI pre jednotlivé bezpečnostné zóny a triedy bolo potrebné vykonať simulácie v troch rozdielnych oblastiach či úrovniach. Jednalo sa predovšetkým o:

- Simuláciu v oblasti činnosti fyzickej ostrahy, v súvislosti s ktorou bol generovaný určitý počet časových úsekov (1200), pričom sa brala do úvahy nekonštantná rýchlosť pohybu

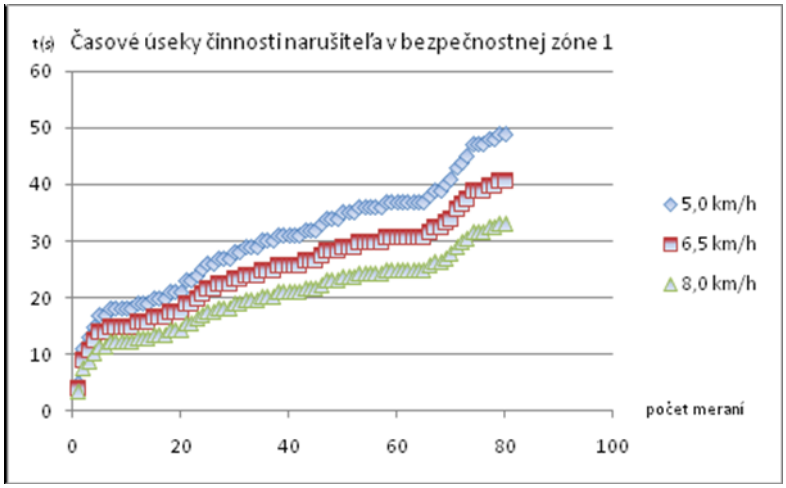
narušiteľa, ktorá vychádzala z obvyklostí simulácie pohybu armádnych jednotiek obr. 25 z ktorých sa následne podľa definovaného vzťahu vypočítala priemerná časová dostupnosť fyzickej ostrahy v danom objekte a štandardná deviácia:



Obrázok 25: Časové úseky činnosti fyzickej ostrahy

$$x_{pr} = 172{,}8s \qquad S_n = \sqrt{\frac{\sum_{i=1}^{n}(x_i - 172{,}8)^2}{1200-1}} \qquad S_n = 78{,}8s \tag{6.10}$$

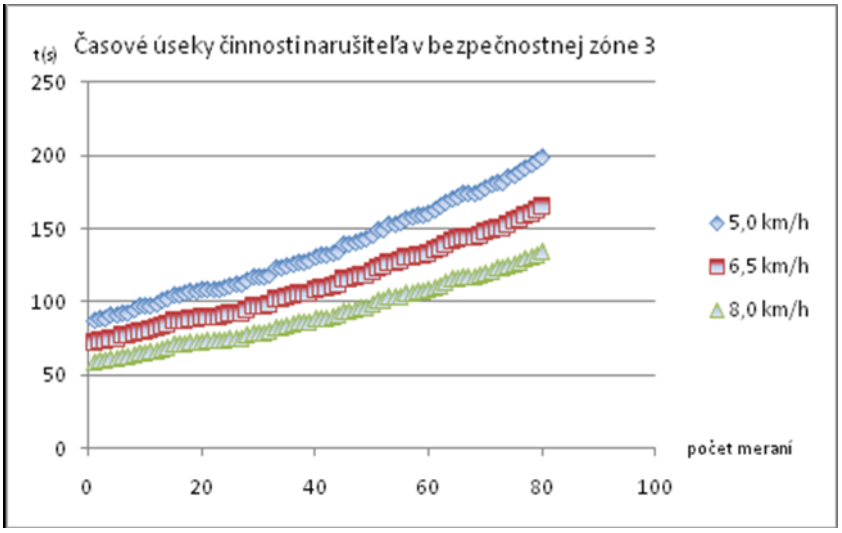
- Simuláciu v oblasti činnosti narušiteľa v súvislosti s ktorou bolo generovaný určitý počet časových úsekov (240 pre jednu bezpečnostnú zónu) obr. 26-29 z ktorých sa následne podľa definovaného vzťahu vypočítala priemerná časová dostupnosť narušiteľa pre jednotlivé bezpečnostné zóny, v ktorých nebola definovaná prítomnosť mechanických zábranných systémov a predpokladalo sa, že narušiteľ bude hľadať najrýchlejšiu cestu v súvislosti s dosiahnutím svojho zámeru:
  - Bezpečnostná zóna 1



Obrázok 26: Časové úseky činnosti narušiteľa v bezpečnostnej zóne 1

$$x_{pr} = 25{,}5s \qquad S_n = \sqrt{\frac{\sum_{i=1}^{n}(x_i - 25{,}5)^2}{240-1}} \qquad S_n = 9{,}2s \tag{6.11}$$

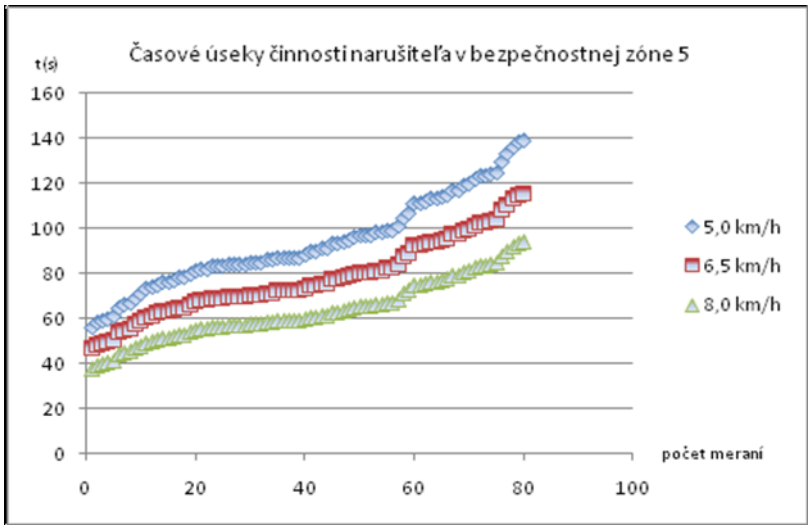
- Bezpečnostná zóna 3



Obrázok 27: Časové úseky činnosti narušiteľa v bezpečnostnej zóne 3

$$x_{pr} = 113{,}4s \qquad S_n = \sqrt{\frac{\sum_{i=1}^{n}(x_i - 113{,}4)^2}{240-1}} \qquad S_n = 32{,}6s \tag{6.12}$$

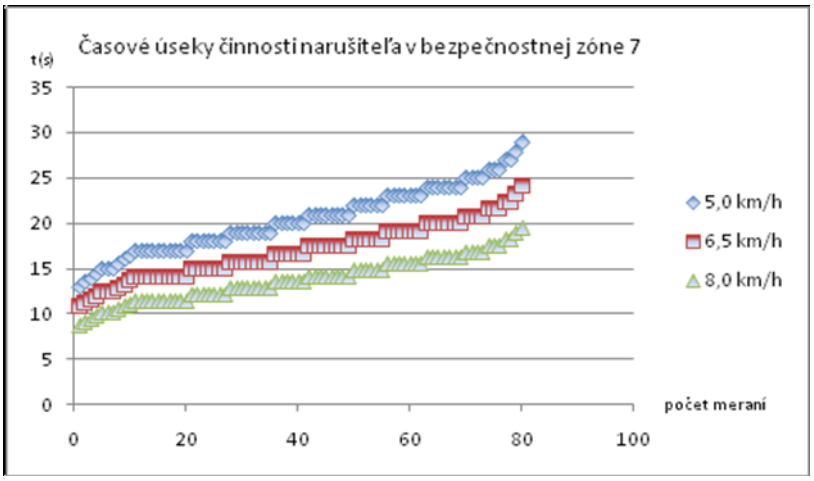
- Bezpečnostná zóna 5



Obrázok 28: Časové úseky činnosti narušiteľa v bezpečnostnej zóne 5

$$x_{pr} = 77{,}7s \qquad S_n = \sqrt{\frac{\sum_{i=1}^{n}(x_i - 77{,}7)^2}{240-1}} \qquad S_n = 22{,}1s \tag{6.13}$$

- Bezpečnostná zóna 7



Obrázok 29: Časové úseky činnosti narušiteľa v bezpečnostnej zóne 7

$$x_{pr} = 17{,}1s \qquad S_n = \sqrt{\frac{\sum_{i=1}^{n}(x_i - 17{,}1)^2}{240-1}} \qquad S_n = 4{,}1s \tag{6.14}$$

- Simuláciu v oblasti tvorby scenárov činnosti fyzickej ostrahy v dôsledku narušenia stráženého priestoru, čo je možné vnímať aj ako formu penetračných testov systému fyzickej ochrany prvku kritickej infraštruktúry a konfrontovanie výstupov z modelu EASI vyplývajúcich a reálnej simulácie na simulačnom nástroji OTB SAF. Tejto časti simulácie sa budem venovať v nasledujúcej časti práce.

6.8.5 Hodnotenie funkčnosti systému fyzickej ochrany prvku kritickej infraštruktúry pre jednotlivé bezpečnostné triedy

Využitie simulačného nástroja nám generovalo vstupné parametre pre model EASI, z ktorého bola následne vyjadrená hodnota pravdepodobnosti úspešného prerušenia činnosti narušiteľa ktorá súčasne vyjadruje aj určitý kvalitatívny parameter navrhnutého systému fyzickej ochrany prvku kritickej infraštruktúry:

- Bezpečnostná trieda I – 0,9699

Estimate of Adversary Sequence Interruption	Pravdepodo. úspešnej komunikácie		Dostup. fyzick. (v sekundách) ostrahy:	Štandardná deviácia
	0,97		172,8	78,8

	Zóny	P(Detecie)	Bez.Tr.	Prielom. (v sekundách): Odolnosť:	Štandardná deviácia
1	Zóna 1	0,9	I	25,5	9,2
2	Zóna 2	0,9	I	75	22,5
3	Zóna 3	0,9	I	113,4	32,6
4	Zóna 4	0,9	I	285	85,5
5	Zóna 5	0,9	I	77,7	22,1
6	Zóna 6	0,9	I	285	85,5
7	Zóna 7	0,9	I	17,1	4,1
8	Zóna 8	0	I	0	0
9					
10					
11					
12					

Pravdep. úsp.prerušenia :	0,969935157

Obrázok 30: Hodnotenie funkčnosti systému FO v bezpečnostnej triede I

- Bezpečnostná trieda II – 0,9929

Estimate of Adversary Sequence Interruption	Pravdepodo. úspešnej komunikácie		Dostup. fyzick. (v sekundách) ostrahy:	Štandardná deviácia
	0,993		172,8	78,8

	Zóny	P(Detecie)	Bez.Tr.	Prielom. (v sekundách): Odolnosť:	Štandardná deviácia
1	Zóna 1	0,9	II	25,5	9,2
2	Zóna 2	0,9	II	105	31,5
3	Zóna 3	0,9	II	113,4	32,6
4	Zóna 4	0,9	II	285	85,5
5	Zóna 5	0,9	II	77,7	22,1
6	Zóna 6	0,9	II	290	87
7	Zóna 7	0,9	II	17,1	4,1
8	Zóna 8	0,9	II	530	159
9					
10					
11					
12					

Pravdep. úsp.prerušenia :	0,99299958

Obrázok 31: Hodnotenie funkčnosti systému FO v bezpečnostnej triede II

- Bezpečnostná trieda III – 0,9949

Estimate of Adversary Sequence Interruption

Pravdepodo. úspešnej komunikácie		Dostup. fyzick. (v sekundách) ostrahy:	Štandardná deviácia
0,995		172,8	78,8

	Zóny	P(Detecie)	Bez.Tr.	Prielom. (v sekundách): Odolnosť:	Štandardná deviácia
1	Zóna 1	0,95	III	25,5	9,23
2	Zóna 2	0,9	III	140	42
3	Zóna 3	0,9	III	113,4	32,6
4	Zóna 4	0,9	III	590	177
5	Zóna 5	0,9	III	77,7	22,1
6	Zóna 6	0,9	III	590	177
7	Zóna 7	0,9	III	17,1	4,1
8	Zóna 8	0,9	III	650	195
9					
10					
11					
12					

Pravdep. úsp.prerušenia :	0,994999895

Obrázok 32: Hodnotenie funkčnosti systému FO v bezpečnostnej triede III

- Bezpečnostná trieda IV – 0,9979

Estimate of Adversary Sequence Interruption

Pravdepodo. úspešnej komunikácie		Dostup. fyzick. (v sekundách) ostrahy:	Štandardná deviácia
0,998		172,8	78,8

	Zóny	P(Detecie)	Bez.Tr.	Prielom. (v sekundách): Odolnosť:	Štandardná deviácia
1	Zóna 1	0,95	IV	25,5	9,2
2	Zóna 2	0,95	IV	170	51
3	Zóna 3	0,95	IV	113,4	32,6
4	Zóna 4	0,95	IV	890	267
5	Zóna 5	0,95	IV	77,7	22,1
6	Zóna 6	0,95	IV	895	268,5
7	Zóna 7	0,95	IV	17,1	4,1
8	Zóna 8	0,95	IV	955	286,5
9					
10					
11					
12					

Pravdep. úsp.prerušenia :	0,997999997

Obrázok 33: Hodnotenie funkčnosti systému FO v bezpečnostnej triede IV

Výstupy EASI modelu nám špecifikovali pravdepodobnosti, ktoré sú vyjadrením funkčnosti systému fyzickej ochrany prvku kritickej infraštruktúry. Navrhnutá štruktúra a funkčné parametre systému fyzickej ochrany z tejto práce vyplývajúce sú dostačujúce v prípade, že nedôjde k zníženiu počtu bezpečnostných zón. Vzhľadom na skutočnosť, že k takémuto prípadu môže dôjsť, v nasledujúcej časti sa budem zaoberať penetračnými testami navrhnutého systému fyzickej ochrany s využitím simulačného nástroja OTB SAF.

6.8.6 Overenie modelu EASI simulačným nástrojom OTB SAF pri penetračných testoch navrhnutého systému fyzickej ochrany prvku kritickej infraštruktúry

Tak ako som v predošlej časti textu naznačil, ďalšia oblasť simulácie bola orientovaná na tvorbu scenárov pre činnosť fyzickej ostrahy v dôsledku narušenia chráneného priestoru v prípade, keď došlo k prekonaniu (penetrácii) niekoľkých bezpečnostných zón.

V tomto kontexte sa uvažovalo o dvoch rovinách plánovanej činnosti narušiteľa a to inicializácia nástražného výbušného systému za účelom úplného zničenia chráneného záujmu, čo sa prejavilo aj dosadením nulovej hodnoty (pre hodnotu prielomovej odolnosti) do 8 zóny modelu EASI a v druhej rovine sa uvažovalo o snahe narušiteľa odcudziť chránený záujem pričom hodnota zóny 8 ostala nezmenená a definovala čas na prekonanie tejto zóny.

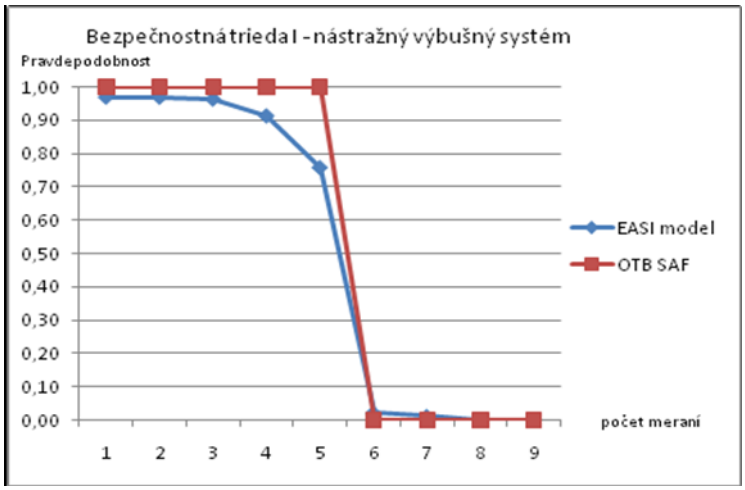
Výstupy generované modelom EASI boli následne overované simuláciou v OTB SAF pre každú bezpečnostnú triedu, pričom samotný proces simulácie je v následných tabuľkách vyjadrený hodnotami 1 v prípade kedy došlo k prerušeniu činnosti narušiteľa a 0 kedy činnosť narušiteľa nebola prerušená a došlo k zničeniu alebo scudzeniu chráneného záujmu tabuľka 24 - 31.

Obrázky 34-41 definujú odolnosť systému fyzickej ochrany prvku kritickej infraštruktúry tak ako bola vyjadrená modelom EASI a simulačným nástrojom OTB SAF pre jednotlivé bezpečnostné triedy so špecifikovanými štrukturálnymi a funkčnými parametrami. Výrazná zmena hodnôt a pokles kriviek poukazuje na prekonanie systému fyzickej ochrany v kontexte s nástražným výbušným systémom a scudzením aktíva, pričom odolnosť systému rastie so zvyšujúcimi sa funkčnými parametrami jednotlivých komponentov systému fyzickej ochrany prvku kritickej infraštruktúry.

Bezpečnostná trieda I – nástražný výbušný systém

Počet prekonaných zón	Výstup z modelu EASI – pravdepodobnosť úspešného prerušenia činnosti narušiteľa	Simulačné overenie modelu EASI nástrojom OTB SAF
0	0,9699	1
1	0,9693	1
2	0,9640	1
3	0,9137	1
4	0,7589	1
5	0,0223	0
6	0,0123	0
7	0	0
8	0	0

Tabuľka 24: Bezpečnostná trieda I – nástražný výbušný systém

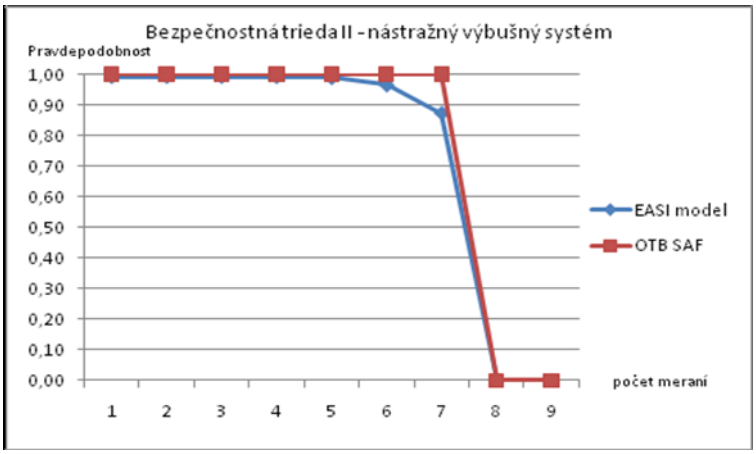


Obrázok 34: Graf overenia EASI modelu nástrojom OTB SAF pre Bezpečnostnú triedu I – nástražný výbušný systém

Bezpečnostná trieda II – nástražný výbušný systém

Počet prekonaných zón	Výstup z modelu EASI – pravdepodobnosť úspešného prerušenia činnosti narušiteľa	Simulačné overenie modelu EASI nástrojom OTB SAF
0	0,9929	1
1	0,9929	1
2	0,9929	1
3	0,9926	1
4	0,9898	1
5	0,9654	1
6	0,8739	1
7	0	0
8	0	0

Tabuľka 25: Bezpečnostná trieda II – nástražný výbušný systém

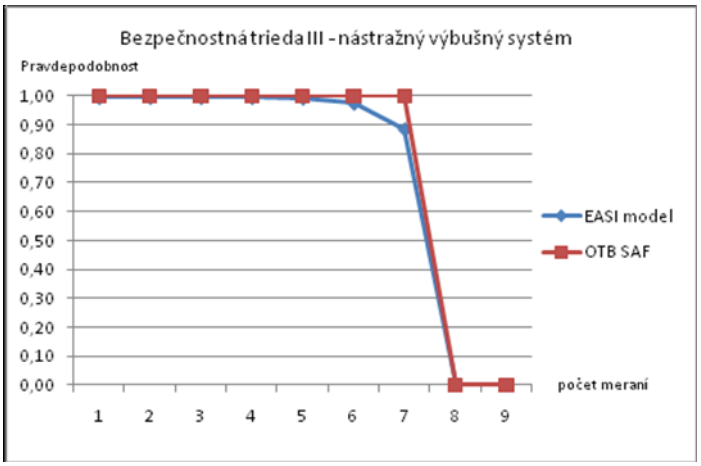


Obrázok 35: Graf overenia EASI modelu nástrojom OTB SAF pre Bezpečnostnú triedu II – nástražný výbušný systém

Bezpečnostná trieda III – nástražný výbušný systém

Počet prekonaných zón	Výstup z modelu EASI – pravdepodobnosť úspešného prerušenia činnosti narušiteľa	Simulačné overenie modelu EASI nástrojom OTB SAF
0	0,9949	1
1	0,9949	1
2	0,9949	1
3	0,9947	1
4	0,9930	1
5	0,9755	1
6	0,8850	1
7	0	0
8	0	0

Tabuľka 26: Bezpečnostná trieda III – nástražný výbušný systém

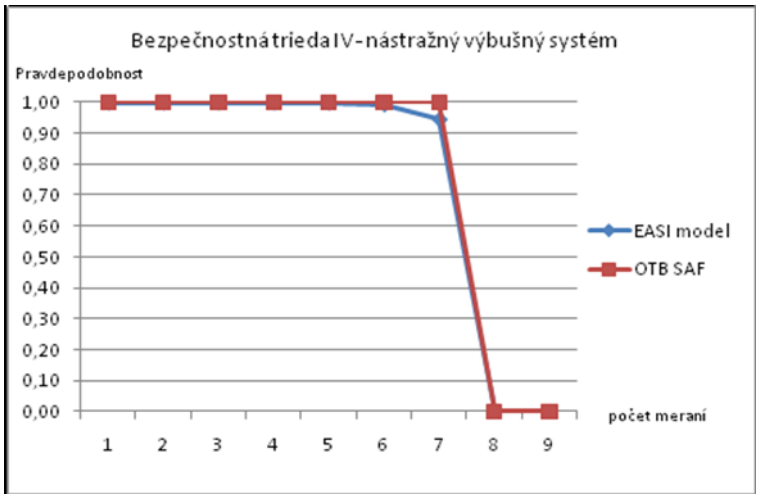


Obrázok 36: Graf overenia EASI modelu nástrojom OTB SAF pre Bezpečnostnú triedu III – nástražný výbušný systém

Bezpečnostná trieda IV – nástražný výbušný systém

Počet prekonaných zón	Výstup z modelu EASI – pravdepodobnosť úspešného prerušenia činnosti narušiteľa	Simulačné overenie modelu EASI nástrojom OTB SAF
0	0,9979	1
1	0,9979	1
2	0,9979	1
3	0,9979	1
4	0,9976	1
5	0,9919	1
6	0,9440	1
7	0	0
8	0	0

Tabuľka 27: Bezpečnostná trieda IV – nástražný výbušný systém

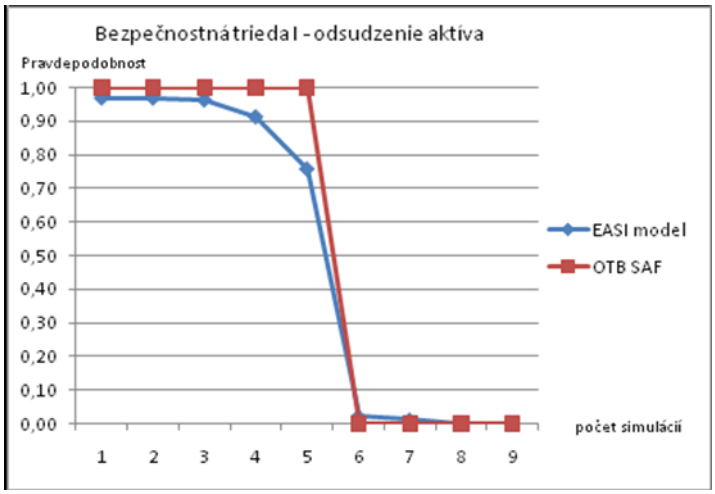


Obrázok 37: Graf overenia EASI modelu nástrojom OTB SAF pre Bezpečnostnú triedu IV – nástražný výbušný systém

Bezpečnostná trieda I – odcudzenie aktíva

Počet prekonaných zón	Výstup z modelu EASI – pravdepodobnosť úspešného prerušenia činnosti narušiteľa	Simulačné overenie modelu EASI nástrojom OTB SAF
0	0,9699	1
1	0,9693	1
2	0,9640	1
3	0,9137	1
4	0,7589	1
5	0,0223	0
6	0,0123	0
7	0	0
8	0	0

Tabuľka 28: Bezpečnostná trieda I – odcudzenie aktíva

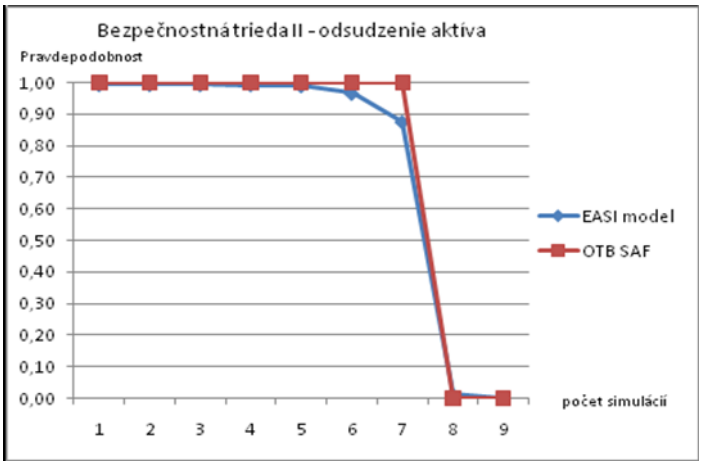


Obrázok 38: Graf overenia EASI modelu nástrojom OTB SAF pre Bezpečnostnú triedu I – odcudzenie aktíva

Bezpečnostná trieda II – odcudzenie aktíva

Počet prekonaných zón	Výstup z modelu EASI – pravdepodobnosť úspešného prerušenia činnosti narušiteľa	Simulačné overenie modelu EASI nástrojom OTB SAF
0	0,9929	1
1	0,9929	1
2	0,9929	1
3	0,9926	1
4	0,9899	1
5	0,9655	1
6	0,8752	1
7	0,0126	0
8	0	0

Tabuľka 29: Bezpečnostná trieda II – odcudzenie aktíva

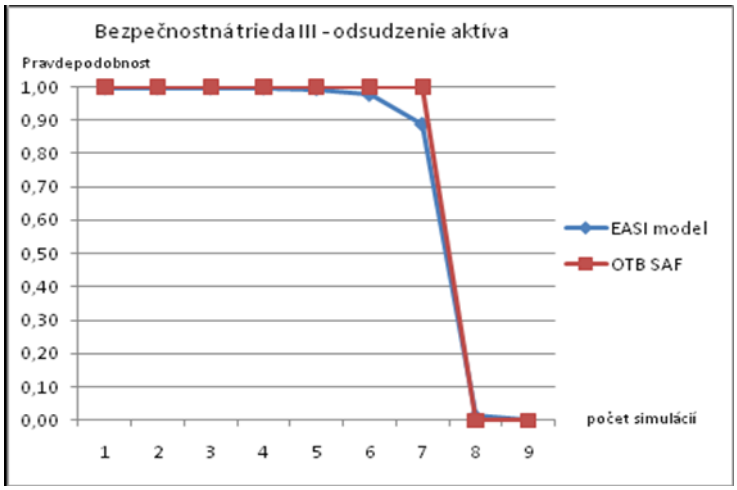


Obrázok 39: Graf overenia EASI modelu nástrojom OTB SAF pre Bezpečnostnú triedu II – odcudzenie aktíva

Bezpečnostná trieda III – odcudzenie aktíva

Počet prekonaných zón	Výstup z modelu EASI – pravdepodobnosť úspešného prerušenia činnosti narušiteľa	Simulačné overenie modelu EASI nástrojom OTB SAF
0	0,9949	1
1	0,9949	1
2	0,9949	1
3	0,9947	1
4	0,9930	1
5	0,9757	1
6	0,8863	1
7	0,0126	0
8	0	0

Tabuľka 30: Bezpečnostná trieda III – odcudzenie aktíva

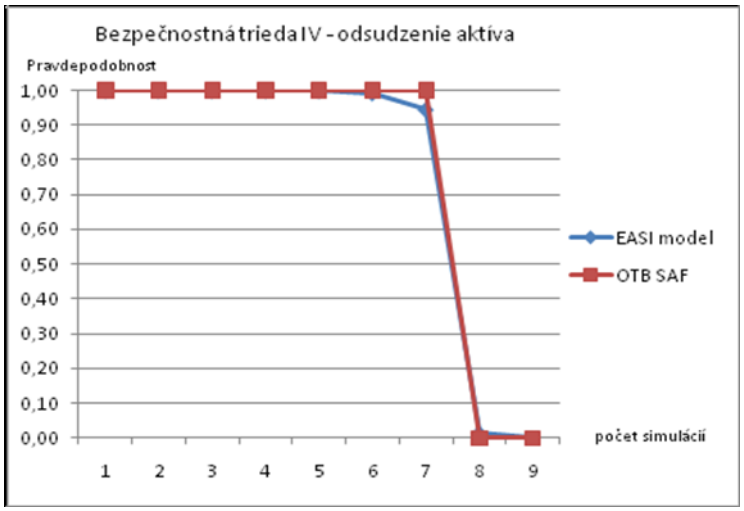


Obrázok 40: Graf overenia EASI modelu nástrojom OTB SAF pre Bezpečnostnú triedu III – odcudzenie aktíva

Bezpečnostná trieda IV – odcudzenie aktíva

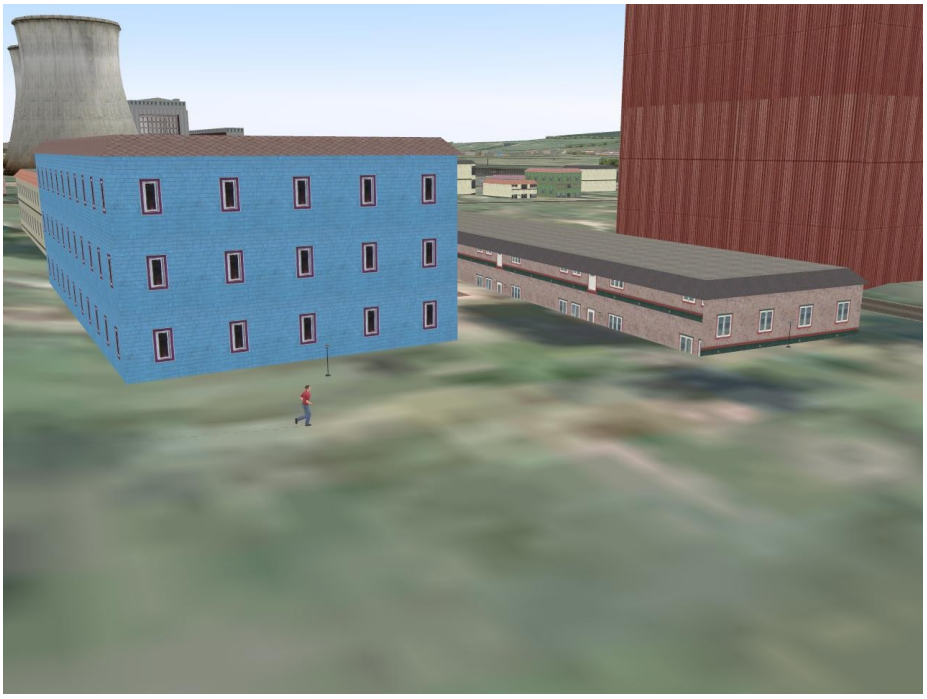
Počet prekonaných zón	Výstup z modelu EASI – pravdepodobnosť úspešného prerušenia činnosti narušiteľa	Simulačné overenie modelu EASI nástrojom OTB SAF
0	0,9979	1
1	0,9979	1
2	0,9979	1
3	0,9979	1
4	0,9976	1
5	0,9919	1
6	0,9447	1
7	0,0134	0
8	0	0

Tabuľka 31: Bezpečnostná trieda IV – odcudzenie aktíva



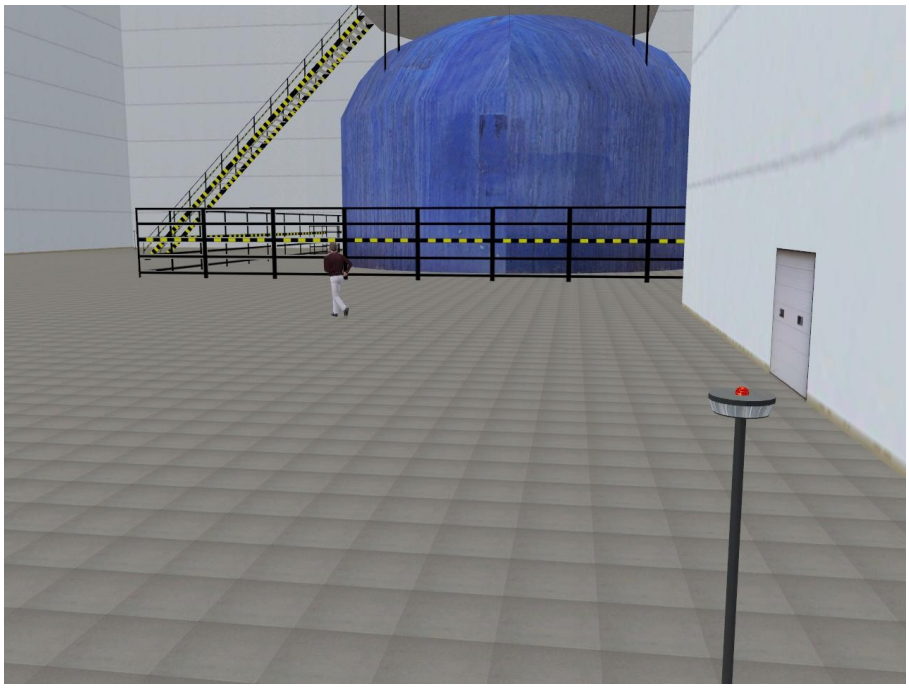
Obrázok 41: Graf overenia EASI modelu nástrojom OTB SAF pre Bezpečnostnú triedu IV – odcudzenie aktíva

Z predošlých tabuliek a grafov vyplynulo, že v prípade keď došlo k prekonaniu 2 bezpečnostných zón, nebola výrazne ovplyvnená funkčnosť systému fyzickej ochrany viz. obr. 42, čo potvrdili aj výstupy z modelu EASI – 0,9460 a aj samotná simulácia .



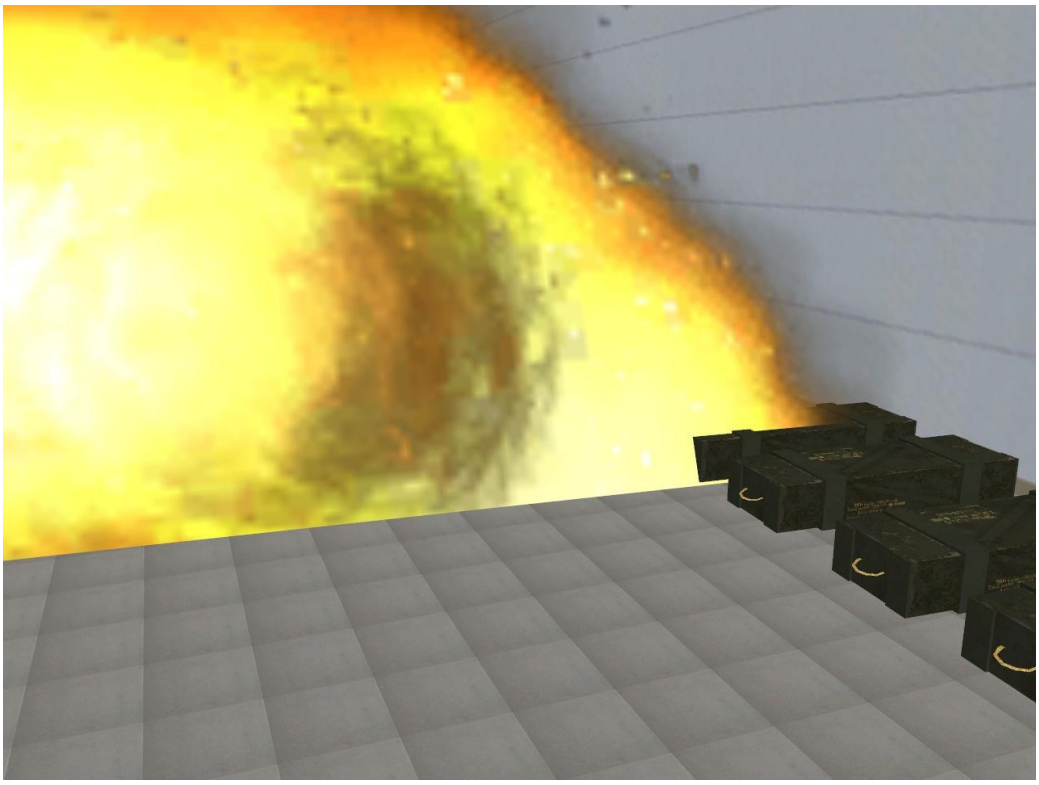
Obrázok 42: Penetračné testy navrhnutého systému FO

Keď došlo k prekonaniu 4 bezpečnostných zón obr. 43 klesla pravdepodobnosť na úroveň 0,7597 a v určitých krajných prípadoch došlo k čiastočnému prelomeniu systému fyzickej ochrany.



Obrázok 43: Činnosť narušiteľa v chránenom objekte

Až v prípade keď došlo k prekonaniu 5 bezpečnostných zón bola pravdepodobnosť úspešného prerušenia činnosti vyjadrená modelom EASI na úroveň 0,0227 čo potvrdili aj simulácie, ktorých výstupom bola inicializácia nástražného výbušného systému a zničenie chráneného záujmu obr.44.



Obrázok 44: Inicializácia nástražného výbušného systému a zničenie chráneného záujmu

Ak by sme brali do úvahy snahu narušiteľa odcudziť chránený záujem tak v podmienkach, ktoré boli v predošlom texte špecifikované z pohľadu štrukturálnych a funkčných požiadaviek by bol navrhnutý systém schopný odolať narušiteľovi aj v prípade prekonania 6 bezpečnostných zón v objektoch zaradených do bezpečnostnej triedy II a vyššie pričom v menovanej zóne bola pravdepodobnosť úspešného prerušenia činnosti narušiteľa vyjadrená na hodnotu 0,875 čo sa potvrdilo aj simuláciou.

7 ZÁVER

V experimentálnej časti práce bola navrhnutá štruktúra a funkčné parametre systému fyzickej ochrany prvku kritickej infraštruktúry, čo vytvorilo rámec pre špecifikáciu a vytvorenie prístupu k hodnoteniu štruktúry systémov fyzickej ochrany prvkov a sektoru kritickej infraštruktúry, čo naplnilo niektoré ciele dizertačnej práce. Akceptovateľnosť definovanej štruktúry, funkčných požiadaviek ako aj prístupu k hodnoteniu štruktúry systémov fyzickej ochrany je vnímaná hlavne v kontexte uskutočnenej verifikácie pomocou modelu EASI a simulačného nástroja OTB SAF, ktorá bola akceptovaná ako syntéza existujúcich prístupov k ochrane majetku a osôb v civilnom a armádnom sektore.

Z predchádzajúcich záverov vyplynulo, že práve použitie simulačného nástroja OTB SAF pre verifikáciu funkčnosti a štruktúry systému fyzickej ochrany prvku kritickej infraštruktúry, bolo rozhodujúcim aspektom overenia teoretickej základne a to nie len v súvislosti s generovaním vstupných parametrov do zvoleného modelu EASI, ale aj so samotným overovaním výstupov z modelu EASI vyplývajúcich, čo je možné vnímať ako overenie štruktúry a funkčnosti systému fyzickej ochrany objektov kritickej infraštruktúry pomocou vhodnej formy informačnej podpory. Tento fakt prispel k vyjadreniu vzťahu štruktúry systému fyzickej ochrany a úrovne ochrany prvku a sektoru kritickej infraštruktúry.

Významný prínos simulačného nástroja OTB SAF vidím hlavne v možnosti verifikovať definovaný systém v kontexte s viacerými významnými hrozbami a to odcudzením či manipuláciou s chráneným záujmom či jeho zničenie pomocou nástražného výbušného systému.

Pri konkrétnych simuláciách v súvislosti zo zámerom použitia nástražného výbušného systému bola jednou s možných alternatív zastavenia narušiteľa jeho fyzická likvidácia, no v súvislosti s povahou a charakterom činnosti súkromných bezpečnostných služieb bolo od tejto formy zastavenia narušiteľa upustené.

Je možné konštatovať, že navrhnutý systém fyzickej ochrany, jeho parametre a stanovenie prístupu k jeho hodnoteniu či overenie jeho funkčnosti pomocou informačnej podpory vytvára predpoklady, aby výstupy z práce vyplývajúce boli využité aj v praxi.

7.1 Využiteľnosť výsledkov dizertačnej práce v praxi

Využiteľnosť vytvorenej metodiky či stanovených štrukturálnych a funkčných požiadaviek na systém fyzickej ochrany prvku kritickej infraštruktúry je vnímané v troch hlavných oblastiach:

- Legislatívny proces,
- Implementácia výstupov dizertačnej práce do realizovaných výskumných projektov,
- Implementácia výstupov dizertačnej práce do pripravovaných výskumných projektov.

7.1.1 Legislatívny proces

Aktuálne legislatívne prostredie v oblasti ochrany kritickej infraštruktúry je formované potrebou implementácie smernice 2008/114/ES, ktorá vytvorila rámec pre tvorbu legislatívnych, normatívnych a inštitucionálnych nástrojov pre optimalizáciu ochrany tejto skupiny infraštruktúr. V kontexte so Slovenskou republikou je možné hovoriť o tvorbe zákona o ochrane kritickej infraštruktúry, ktorý má túto problematiku riešiť a je vnímaný ako forma implementácie smernice. V tomto smere môžem konštatovať, že znalostná základňa, prezentovaná v tejto práci, prispela k implementácii systémov fyzickej ochrany, vnímaných ako významný aspekt ochrany kritickej infraštruktúry, do návrhu zákona, kde sa poukázalo na nevyhnutnosť kategorizácie technických prostriedkov bezpečnostného priemyslu nie len podľa ich skupinovej príslušnosti, ale aj podľa funkčného určenia. Prejavilo sa to kategorizáciou týchto prostriedkov v §2 pism. m, n. Tento fakt vytvára priestor pre tvorbu metodík pre ochranu kritickej infraštruktúry s prepojením na systémy fyzickej ochrany, ktoré budú nasledovať po ukončení legislatívneho procesu. V súvislosti s týmto faktom bude vytváraná snaha o použitie vytvorenej metodiky a tvorbu všeobecne záväznej vyhlášky resp. vládneho nariadenia, ktoré by malo vyriešiť otázku štandardov fyzickej ochrany prvkov kritickej infraštruktúry v konkrétnych oblastiach.

7.1.2 Implementácia výstupov dizertačnej práce do realizovaných výskumných projektov

V súvislosti s programom bezpečnostného výskumu Českej republiky v rokoch 2010-2015 (BV II/2-VS), je nutné konštatovať, že výstupy z dizertačnej práce vyplývajúce sú reálne využívané spoločnosťou Deloitte vo vzťahu k projektu „Metodika ochrany kritické infrastruktury v oblasti výroby, přenosu a distribuce el. energie“, kde vytvorená metodika bude významnou časťou realizovanej metodiky v súvislosti s potrebou vnímania ochrany z komplexnejšieho hľadiska. Využiteľnosť sa predpokladá aj v súvislosti s faktom, že

metodika vytvorená v dizertačnej práci obsahuje reálne prístupy k štandardom fyzickej ochrany, ktoré vychádzajú z realizovaných štandardov fyzickej ochrany spoločnosti ČEZ a.s., s ktorou pre potreby realizácie tejto práce bola podpísaná zmluva o ochrane obchodného tajomstva. V súvislosti s významom spoločnosti Deloitte v bezpečnostnom výskume a formuláciou v dokumente „Komplexní strategie České republiky k řešení problematiky kritické infrastruktury“, ktorá hovorí „Vlastní konkrétní výzkum, vývoj a inovace dotýkající se bezpečnosti kritické infrastruktury budou realizovány prostřednictvím průřezového programu „Bezpečnostní výzkum pro potřeby státu v létech 2010 až 2015“ BV II/1“ sa vytvára priestor do implementácie vytvorenej metodiky to legislatívneho prostredia aj v Českej republike.

Vo vzťahu spomínanému programu bezpečnostného výskumu je potešiteľné konštatovať, že výstupy v práci prezentované budú využité aj v súvislosti s projektom Univerzity Tomáše Bati ve Zlíne a Institutu ochrany obyvatelstva Lázně Bohdaneč „Systém hodnocení odolnosti prvků a sítí vybraných oblastí kritické infrastruktury“, kde sa predpokladá s ich využitím v procese tvorby agregovaných koeficientov integrovaného bezpečnostného systému. Tento fakt vytvára rámec pre prepojenie oboch realizovaných projektov a zosúladenie prístupov a to hlavne v súvislosti s potrebou vytvorenia totožných prístupov a metodík, čo bude zvyšovať potenciál využitia výstupov z oboch projektov vyplývajúcich v ďalšom legislatívnom procese v ČR.

7.1.3 Implementácia výstupov dizertačnej práce do pripravovaných výskumných projektov

Samotná finalizácia a verifikácia výstupov dizertačnej práce bola postavená na využití simulačného nástroja OTB SAF a modelu EASI, pre potreby ktorých bol v súčinnosti so simulačným centrom Akadémie ozbrojených síl gen. M. R. Štefánika v Liptovskom Mikuláši vytvorený čiastočne nový modul simulačného nástroja OTB SAF. Myšlienky, ktoré vyplynuli z tvorby tohto modelu, boli základom pre prípravu projektu v rámci dotačného programu Ministerstva školstva SR, ktorý bude zameraný na transformáciu simulačného centra pre potreby krízového manažmentu a riadenia v civilnom sektore. V súčasnej dobe sa spracováva štúdia realizovateľnosti a cieľom štúdie je pripraviť návrh ďalšieho budovania a rozvoja Simulačného centra AOS v oblasti profesionálneho zamerania špecializovaného pracoviska a materiálno-technickej podpory neakreditovaných a akreditovaných vzdelávacích aktivít, alebo výcviku personálu na tomto pracovisku, pre plnenie úloh v rámci použitia síl a prostriedkov na území Slovenskej republiky a v zahraničí, v rámci operácií národného a medzinárodného krízového manažmentu. Vedomostný základ prezentovaný v tejto práci bude významným

spôsobom ovplyvňovať samotnú transformáciu a kompletizáciu potrebných modulov pre simulačný nástroj OTB SAF.

Tak ako z predošlého textu vyplynulo transformácia simulačného centra je vnímaná aj v kontexte s víziou vytvorenia kurzu pre prevádzkovateľov prvkov kritickej infraštruktúry, ktorý by bol rozdelený do dvoch modulov, pričom teoretický modul by bol realizovaný na Univerzite Tomáše Bati ve Zlíně a praktický modul na Akadémii ozbrojených síl gen. M. R. Štefánika v Liptovskom Mikuláši. V praktickom module by bol práve použitý transformovaný nástroj OTB SAF a pripravovaný simulačný modul pre ochranu vojsk a kritickej infraštruktúry, kde by dochádzalo k simulácii rozhodovacieho procesu v prípade vzniku krízovej situácie a to nie len v kontexte s činnosťou narušiteľa. Overovanie funkčnosti a štruktúry systémov fyzickej ochrany penetračnými testami v reálnom prostredí je nerealizovateľný proces, ktorý zvyšuje motiváciu prevádzkovateľov kritickej infraštruktúry využiť tento modul simulačného centra pre penetračné testy, ktoré budú čo najväčšou mierou korešpondovať s reálnymi podmienkami v objektoch, ktoré sú v ich pôsobnosti. Zo štruktúry tohto pripravovaného kurzu je možno vydedukovať, že ide perspektívne o medzinárodný kurz, preto bude snaha certifikovať tento kurz aj s výhľadom na Európsku úniu, čo by zvýšilo význam kurzu aj z pohľadu eurozóny. V prípade úspešnej realizácie by bol kurz zameraný aj na prevádzkovateľov európskej kritickej infraštruktúry. Táto spolupráca a vytvorenie spomínaného kurzu by zvýšilo význam Univerzity Tomáše Bati ve Zlíně a Akadémie ozbrojených síl gen. M. R. Štefánika v Liptovskom Mikuláši pri tvorbe a formovaní medzinárodného bezpečnostného prostredia.

Zoznam skratiek

AIR	Active Infrared - Aktívny infračervený detektor
BMW	Bistatic Microwave – Bistatický mikrovlnný detektor
CCTV	Closed-circuit television – Uzavretý televízny okruh
ECI	European Critical Infrastructure
ECIP	European Critical Infrastructure Protection contact points
EKI	Európska kritická infraštruktúra
EPCIP	European Program for Critical Infrastructure Protection
ETA	Event Tree Analysis
EZS	Elektrický zabezpečovacia systém
FBI	Federal Bureau of Investigation
FMEA	Failure Mode and Effects Analysis
FO	Fyzická ochrana
FTA	Fault Tree Anylysis
HAZOP	Hazard and Operability Study
HDP	Hrubý domáci produkt
HRA	Human Reliability Analysis
IZS	Integrovaný záchranný systém
KI	Kritická infraštruktúra
MMW	Monostatic Microwave – Monostatický mikrovlnný detektor
MZS	Mechanické zábranné systémy
OSP	Operator Security Plan
PCO	Pult centralizovanej ochrany
PD	Pravdepodobnosť detekcie
PO	Prielomová odolnosť
QRA	Quantitative Risk Analysis
RAS	Rapid Alert System
SCEPT	Senior Civil Emergency Planning Committee
SLO	Security Liason Officer
TZP	Technické zabepečovacie prostriedky
WTC	World Trade Centre

Zoznam obrázkov

Zoznam tabuliek

8 LITERATÚRA

Monografie

[1] ASME INNOVATIVE TECHNOLOGIES INSTITUTE, LLC, . *All-hazard risk and resilience : Prioritizing Critical Infrastructures Using the RAMCAP Plus Approach.* 1. New York : ASME, 2009. 155 s. ISBN 978-0-7918-0287-8.

[2] A. COLLINS, P.; K. BAGGETT, R. *Homeland Security : and Critical Infrastructure Protection.* 2. Westport : Praeger, 2009. 267 s. ISBN 978-0-313-35147-1.

[3] GARCIA, M. L. *The Design and Evaluation of Physical Protection Systems*. 2. USA : Butterworth-Heinemann, 2008. 351 s. ISBN 978-0-7506-8352-4.

[4] LAUCKÝ, V. *Řízení technologických procesů v průmyslu komerční bezpečnosti*. 1. Zlín : UTB - Academia Centrum Zlín, 2005. 101 s. ISBN 80-7318-329-3.

[5] LEE, E. *Homeland Security and Private Sector Business : Corporations´ Role in Critical Infrastructure Protection*. 1. USA : Taylor & Francis Group, 2009. 281 s. ISBN 978-1-4200-7078-1.

[6] MACAULAY, T. *Critical Infrastructure : Understanding Its Component Parts, Vulnerabilities, Operating Risks and Interdependencies*. 1. USA : Taylor & Francis Group, 2009. 320 s. ISBN 978-1-4200-6835-1.

[7] MOZGA, J.; VÍTEK, M.; KOVÁŘÍK, F., *Kritická infrastruktura společnosti*. 1. Hradec Králové : Gaudeamus, 2008. 156 s. ISBN 978-80-7041-299-2.

[8] MURRAY, Alan T.; GRUBESIC, Tony. *Critical Infrastructure : Reliability and Vulnerability.* 1. USA : Springer, 2010. 311 s. ISBN 978-3642087738.

[9] ŠEBESTA, M.; SCHWARZ, R., *Management rizik : s pravdepodobnostním prístupem ke stanovení rizik.* 1. Brno : Vojenská akademie v Brne, 2003. 63 s.

Príspevky so zborníkov

[10] GOŇA, S.; LOVEČEK, T. *Detekcia narušiteľa poplachovými systémami a nové bezpečnostné technológie zvyšujúce jej pravdepodobnosť*. In . Zlín : Univerzita Tomáše Bati ve Zlíně, 2008. 21 s. s.2,

[11] GOŇA, S.; LOVEČEK, T. *Detekcia narušiteľa poplachovými systémami a nové bezpečnostné technológie zvyšujúce jej pravdepodobnosť*. In . Zlín : Univerzita Tomáše Bati ve Zlíně, 2008. 21 s. s.10,

[12] HORÁK R.; SALINGER T.; NAVRÁTIL J.; *Řešení kritické infrastruktury s možností využití nástrojů EU*, Ochrana obyvatel 2007, Ostrava, 2007, ISBN 80-86634-51-5

[13] LONGSTAFF, P.; MERGEL, I.; ARMSTRONG, N.; Insitute for National Security and Counterterrorism, Workshop Report: *Resilience in Post-Conflict Reconstruction and Natural Disasters*, Syracuse University, 2009, Syracuse

[14] LUKÁŠ, L.; HROMADA, M.; *Možnosti hodnocení odolnosti kritické infrastruktury/ Evaluating the Resistance of Critical Infrastructure*, Bezpečnost v informační společnosti, Brno, 2009

Legislatívne zdroje

[15] EU. Critical Infrastructure Protection in the fight against terrorism. In *Communication from the commission to the council and the european parliament.* 2004, 345, s. 1-11. Dostupný také z WWW: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0702:FIN:EN:PDF>.

[16] EU. Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. In *Council directive 2008/114/EC*. 2008, 345, s. 75-82. Dostupný tiež z WWW: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:en:PDF>.

[17] EU. European Programme for Critical Infrastructure Protection . In COMMUNICATION FROM THE COMMISSION. 2006, s. 1-13. Dostupný tiež z WWW: <http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0786en01.pdf>.

[18] MINV SR, *Koncepcia kritickej infraštruktúry v Slovenskej republike a spôsob jej ochrany a obrany*, dostupné tiež z WWW: < www.minv.sk/?ochrana-kritickej-infrastruktury&subor=10691>

[19] MINV SR, Národný program pre ochranu a obranu kritickej infraštruktúry v Slovenskej republike, dostupné tiež z WWW: http://www.google.com/url?q=http://www.minv.sk/%3Fochranakritickejinfrastruktury%26subor%3D10692&ei=WhUUS_X_HKLkmwPJ

6NHUAg&sa=X&oi=spellmeleon_result&resnum=1&ct=result&ved=0CAYQhgIwAA&usg=AFQjCNF2wxySWqBB0Bm5uGLGneBOxe9AGw

[20] Non-Binding Guidelines - For Application of the Council Directive on the Identification and Designation of European Critical Infrastructure and the Assessment of the Need to Improve Their Protection. 2008, JRC48985, Dostupný tiež z WWW: <http://publications.jrc.ec.europa.eu/repository/handle/111111111/13328>. ISSN 1018-5593,

[21] SR. Zákon č. 45/2011 o kritickej infraštruktúre. In *45/2011*. 2011, 19, s. 434-442. Dostupný tiež z WWW: <http://www.zbierka.sk/zz/predpisy/default.aspx?PredpisID=210111&FileName=zz2011-00045-0210111&Rocnik=2011>.

[22] SR. Zákon č. 333/2007 ktorým sa mení a dopĺňa zákon č. 319/2002 Z. z. o obrane Slovenskej republiky v znení neskorších predpisov a o zmene niektorých zákonov. In *333/2007*. 2007, 147, s. 2279-2281. Dostupný tiež z WWW: http://www.mod.gov.sk/data/files/616.pdf

[23] USA. George W. Bush, Vládne nariadenie na ochranu kritickej infraštruktúry, 2001, Dostupný tiež z WWW: http://www.iwar.org.uk/cip/resources/bush/executive-order.htm

[24] USA. National strategy for Homeland security. In *Homeland security council*. 2007, s. 1-53. Dostupný tiež z WWW: <http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf>.

[25] USA. Secure cyberspace. In *The national strategy*. 2003, s. 1-59. Dostupný tiež z WWW: <http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf>

[26] USA. The Clinton Administration´s Policy on Critical Infrastructure Protection. In *Presidential Decision Directive 63*. 1998, s. 1-14. Dostupný tiež z WWW: http://csrc.nist.gov/drivers/documents/paper598.pdf

[27] USA. The Physical Protection of Critical Infrastructures and Key Assets. In *National strategy*. 2003, s. 1-82. Dostupný tiež z WWW: <http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf>.

[28] SR. Vyhláška Národného bezpečnostného úradu : o fyzickej bezpečnosti a objektovej bezpečnosti. In *Vyhlášky NBU*. 2004, 1, s. 1-34. Dostupný tiež z WWW: <http://www.nbusr.sk/ipublisher/files/408/336_2004.pdf>.

[29] SR. Vyhláška úradu jadrového dozoru Slovenskej republiky : ktorou sa ustanovujú podrobnosti o požiadavkách na zabezpečenie fyzickej ochrany. In *Zbierka zákonov č. 51/2006*. 2006, 24, s. 477-482. Dostupný tiež z WWW: <http://www.ujd.gov.sk/files/legislativa/51.pdf>.

Internetové zdroje

[30] *A Nuclear and radiation accidents* [online]. 2004. A European Informational Website. Dostupné z WWW: <http://radiationshielding.eu/list_of_nuclear_accidents_en.html>.

[31] *Avalange* [online]. 2009 [cit. 2010-03-23]. Avalange centers. Dostupné z WWW: <http://www.avalanche.org/>.

[32] *Bezpečnost a prevence* [online]. 2008. Organizovaný zločin. Dostupné z WWW: <http://aplikace.mvcr.cz/archiv2008/bezpecnost/ozlocin.html>.

[33] *Extreme dry weather worsens food situation in Zimbabwe* [online]. 2008 [cit. 2011-04-13]. FAO Newsroom. Dostupné z WWW: <http://www.fao.org/newsroom/en/news/2008/1000825/index.html>.

[34] Federal Ministry of the Interior. *Protecting Critical Infrastructures – Risk and Crisis Management : A guide for companies and government authorities* [online]. Berlin : Ministry of the Interior, 2008 [cit. 2011-04-13]. Dostupné z WWW: <http://www.bmi.bund.de/SharedDocs/Downloads/EN/Broschueren/Leitfaden_Schutz_kritischer_Infrastrukturen_en.pdf?__blob=publicationFile>

[35] FEMA, California Extreme Fire Hazards, Dostupné on-line:< http://www.fema.gov/news/event.fema?id=413>

[36] Hasičský záchranný sbor Ústeckého kraje, dostupné on-line: < http://www.hzsoul.cz/index.php?option=com_content&task=view&id=255&Itemid=111>

[37] HOFREITER L., LOVEČEK T., VEĽAS A., zásady a princípy analýzy rizík v oblasti fyzickej a objektovej bezpečnosti, Žilinská univerzita v Žiline, Fakulta špeciálneho inžinierstva, Žilina, 2006, dostupné on-line: http://www.nbusr.sk/ipublisher/files/nbusr.sk/oblasti-bezpecnosti/objektova-afyzicka/docs_of/analyza/zasady_metodika.

[38] JELEMENSKÝ, Ľ., MARKOŠ, J., HAZOP metóda na identifikáciu možných nebezpečných stavov a prevádzkových problémov, AT&P Journal 1/2004 - http://www.scribd.com/doc/7338001/ManazmentRizikprezentacieAkoTahakKomplet

[39] LAML R., Zraniteľnosť, Mepoforum, dostupné on-line http://www.mepoforum.sk/media/kniznica/media/documents/pdf/Zranitelnost.pdf

[40] Mesto Vsetín [online]. 2000. Zbraně hromadného ničení. Dostupné z WWW: <http://www.mestovsetin.cz/bezpeci/brevir/static/dokumenty/prestupky_a_trestne_ciny/chranime_zdravi_a_zivot/zbrane_hromadneho_niceni.htm>.

[41] Resilience Alliance, Assessing and managing resilience in social-ecological systems: Volume 2 supplementary notes to the practitioners workbook, 2007, dostupné on-line: < 1190318371_practitioner_workbook_suppl_notes_1.0.pdf >

[42] *Security and society* [online]. 2009, Extremism in general. Dostupné z WWW: <http://www.security-society.org/?q=taxonomy/term/29>

[43] *Seismology* [online]. 2005. Zemetrasenia na slovensku. Dostupné z WWW: <http://www.seismology.sk/index_S.php>.

[44] *Výkladový slovník : Mechanické zábranné prostriedky* [online]. 2005. Terminológia bezpečnostného manažmentu. Dostupné z WWW: <www.securityrevue.com/tbm/part2_p.html#tab-7>.

[45] *The Dartmouth Flood Observatory* [online]. 2008. Space-based Measurement of Surface Water. Dostupné z WWW: <http://www.dartmouth.edu/~floods/>.

[46] *Terrorism. In Policy and Guidelines.* [online].USA. 1999. Dostupné z WWW: <http://www.highbeam.com/doc/1G1-120349151.html>.

[47] *Terrorism Research Center*. [online]. USA. Dostupné z WWW: < http://www.terrorism.com/ >

[48] *Volcano Hazards Program* [online]. 2009. U.S. Volcanoes and Current Activity Alerts. Dostupné z WWW: <http://volcanoes.usgs.gov/>

[49] WALKER, B. *Section 1.5 to practitioner : Resilience Alliance* [online]. 2009 Specified and General Resilience. Dostupné z WWW: <http://1255615042_walker _general_resilience _short_form.pdf>

Normy

[50] ČSN CLC/TS 50131-7 príloha E

[51] ČSN/P CEN/TS 14383-3

[52] EN 356

[53] EN 1143

[54] EN 1303

[55] EN 1906

[56] EN 12209

[57] ENV 1627

[58] STN 01 0380

Akademické práce

[59] HROMADA, M. *Analýza rizík a havarijné plánovanie vo výrobnom závode SHP Harmanec a.s.*. Zlín, 2008. 110 s. Diplomová práce. Univerzita Tomáše Bati ve Zlíně.

9 ZOZNAM VLASTNÝCH PUBLIKÁCIÍ Z DANEJ PROBLEMATIKY

PETZ, I., NECAS, P., KELEMEN, M., ANDRASSY, V., HROMADA, M., SOUSEK, R., *Constructive simulation entities behaviour modelin in realm of blended simulation.* In. Brno, ICMT ,2011, 1211-1214, 4 s, ISBN 978-80-7231-787-5

KELEMEN, M., HROMADA, M., NECAS, P., ANDRASSY, V., SOUSEK, R., PETZ, I., *The ONESAF OTB modeling and simulation tool for the defence and critical infrastructure component physical and technical protection system verification,* In. Brno, ICMT, 2011, 1215-1223,9 s, ISBN 978-80-7231-787-5

HROMADA, M., LUKAS, L., 2009, *Porovnanie ochrany kritickej infraštruktúry na Slovensku, v Čechách a v EU / The Comparison of critical infrastructure protection in Slovakia, Czech Republic and EU*, WSPÓŁCZESNE DYLEMATY BEZPIECZEŃSTWA - TEORIA I PRAKTYKA, Warszava, Poland,Wyższej Szkoły Bezpieczeństwa i Ochrony w Warszawie,

HROMADA, M., *Implementácia technológií inteligentných budov do problematiky ochrany kritickej infraštruktúry/ Inteligent Building Technologies Implementation to Critical Infrastructure Protection* , Vliv technológií inteligentních budov na zajištění bezpečnosti objektů, Praha, 2009,

LUKÁŠ, L., HROMADA, M., *Možnosti hodnocení odolnosti kritické infrastruktury/ valuating the Resistance of Critical Infrastructure,* In: Bezpečnost v informační společnosti, Brno, 2009, p. 56, ISBN 978-80-7231-653-3

HROMADA, M., *Technologické prístupy k ochrane kritickej infraštruktúry na Slovensku*, Bezpečnostné technológie systémy a management – medzinárodná konferencia, In: Zlín, 2009, ,

HROMADA, M., *Ochrana kritickej infraštruktúry a jej technologické aspekty/Critical infrastructure Protection and Its Technological Aspects*, In: Security Magazín, Číslo 93, 2010, ISSN – 1210-8723,

HROMADA, M., *Stanovenie odolnosti kritickej infraštruktúry/The Critical Infrastructure Vulnerability Determination*, In: Security Magazín, Číslo 93, 2010, ISSN –1210-8723,

HROMADA, M., *Stanovení odolnosti kritickej infraštruktúry – teoretický rámec/Critical Infrastructure Resilience Determination – Theoretical Framework* ,In: Security Magazín, Číslo 93, 2010, ISSN – 1210-8723

HROMADA, M., *Stanovení odolnosti kritickej infraštruktúry – praktický příklad/Critical Infrastructure Resilience Determination – Practical Example*, In: Security Magazín, Číslo 93, 2010, ISSN – 1210-8723

HROMADA, M., *Kritická infraštruktúra – úvod do problematiky/Critical Infrastructure – Problematic Introduction*, In. Security Magazín, Číslo 93, 2010, ISSN –1210-8723

HROMADA, M., *Organizácia ochrany kritickej infraštruktúry v SR, EU, a USA/The Critical Infrastructure Protection Organization in SR, EU and USA*, In: Security Magazín, Číslo 93, 2010, ISSN – 1210-8723

HROMADA, M.,*Povinnosti prevádzkovateľa Európskej kritickej infraštruktúry/The European Critical Infrastructure Operator Duties*, In: Security Magazín, Číslo 95, 2010, ISBN – 1210-8723

HROMADA, M.,*Využitie modelovania v problematike ochrany kritickej infraštruktúry/The modeling use in area of Critical Infrastructure protection,* In: Security Magazín, Číslo 96, 2010, ISBN – 1210-8723

HROMADA, M., *Inteligent Building Technologies as an important aspect of Critical Infrastructure Protection*, In: odborný vedecký časopis Trilobit, FAI, UTB ve Zlíně, 2010, ISSN 1804 – 1795