

# **Analýza spôsobov hodnotenia odolnosti sietí a prvkov kritickej infraštruktúry vo vybraných štátoch**

The Analysis of a Critical Infrastructure Elements and Networks  
Resilience Evaluation in Selected States

Bc. Lenka Rigáňová

---

Diplomová práce  
2012



Univerzita Tomáše Bati ve Zlíně  
Fakulta aplikované informatiky

---

**Univerzita Tomáše Bati ve Zlíně**

**Fakulta aplikované informatiky**

akademický rok: 2011/2012

# **ZADÁNÍ DIPLOMOVÉ PRÁCE**

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Bc. Lenka RIGÁŇOVÁ**  
Osobní číslo: **A10334**  
Studijní program: **N 3902 Inženýrská informatika**  
Studijní obor: **Bezpečnostní technologie, systémy a management**

Téma práce: **Analýza způsobu hodnocení odolnosti sítí a prvků kritické infrastruktury ve vybraných státech**

Zásady pro vypracování:

1. Vypracujte literární rešerši na téma kritická infrastruktura.
2. Pojednejte o obecných principech vnímání odolnosti kritické infrastruktury.
3. Diskutujte o používaných principech hodnocení odolnosti kritické infrastruktury.
4. Použijte vybraný princip hodnocení odolnosti pro vybraný objekt.
5. Stanovte návrh souboru důležitých entit, které ovlivňují celkovou hodnotu odolnosti ve vybraném objektu.

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **Zákon 45/2011 Zb. o kritické infrastruktuře**
2. **MOZGA, J.; VÍTEK, M.; KOVÁŘÍK, F., Kritická infrastruktura společnosti. 1. Hradec Králové : Gaudeamus, 2008. 156 s. ISBN 978-80-7041-299-2.**
3. **LUKÁŠ, L.; HROMADA, M.; Možnosti hodnocení odolnosti kritické infrastruktury/ Evaluating the Resistance of Critical Infrastructure, Bezpečnost v informační společnosti, Brno, 2009.**
4. **HROMADA Martin, Konceptuálny návrh systému hodnotenia odolnosti prvku kritickéj infraštruktúry, In: Bezpečnostní technologie systémy a management ? mezinárodní konference, Zlín, 2011, ISBN: 978-80-7454-111-7.**
5. **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.**

Vedoucí diplomové práce:

**Ing. Martin Hromada, Ph.D.**

Ústav bezpečnostního inženýrství

Datum zadání diplomové práce:

**24. února 2012**

Termín odevzdání diplomové práce:

**15. května 2012**

Ve Zlíně dne 24. února 2012

prof. Ing. Vladimír Vašek, CSc.  
*děkan*



L.S.

doc. RNDr. Vojtěch Kresálek, CSc.  
*ředitel ústavu*

## ABSTRAKT

Táto práca popisuje ochranu a odolnosť kritickej infraštruktúry. Teoretická časť je zameraná na porovnanie kritickej infraštruktúry v Spojených štátoch amerických, Európskej únii, Českej a Slovenskej republike. Pojednáva o legislatívnych požiadavkách ochrany v menovaných štátoch. V rámci hodnotenia odolnosti kritickej infraštruktúry sa zameriavam na multikriteriálne hodnotenie pomocou procesu RAMCAP Plus, ktorý sa využíva v Spojených štátoch amerických. V praktickej časti aplikujem multikriteriálne hodnotenie odolnosti na objekt kritickej infraštruktúry.

Kľúčová slova: kritická infraštruktúra, ochrana kritickej infraštruktúry, odolnosť kritickej infraštruktúry, hrozba, riziko, zraniteľnosť

## ABSTRACT

This master thesis deals with the protection and resilience of critical infrastructure. The theoretical part is concentrated on the comparison of critical infrastructure in the United States of America, the European Union, the Czech Republic and Slovakia. It discusses the legislative protection in the named states. Within the evaluation of the resilience of critical infrastructure the theoretical part is concentrated on the multicriterial evaluation through the process called RAMCAP Plus, which is mostly used in the USA. In the practical part I have applied this multicriterial evaluation of resilience to the resilience of critical infrastructure.

Keywords: critical infrastructure, protection of critical infrastructure, resilience of critical infrastructure, threat, risk, vulnerability

V prvom rade by som chcela poďakovať svojmu vedúcemu diplomovej práce Ing. Martinovi Hromadovi Ph.D. za odborné vedenie, cenné rady a čas venovaný mojim konzultáciám. Ďalej by som chcela poďakovať svojim rodičom a najbližšej rodine za ich trpezlivosť a dennodennú podporu pri písaní práce.

**Prohlašuji, že**

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

**Prohlašuji,**

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně

.....  
podpis diplomanta

**OBSAH**

<b>ÚVOD.....</b>	<b>9</b>
<b>I TEORETICKÁ ČÁST.....</b>	<b>10</b>
<b>1 KRITICKÁ INFRAŠTRUKTÚRA.....</b>	<b>11</b>
1.1 KRITICKÁ INFRAŠTRUKTÚRA V USA.....	12
1.2 KRITICKÁ INFRAŠTRUKTÚRA V EÚ .....	13
1.3 KRITICKÁ INFRAŠTRUKTÚRA V ČR .....	14
1.4 KRITICKÁ INFRAŠTRUKTÚRA V SR.....	16
<b>2 SEKTOR KRITICKEJ INFRAŠTRUKTÚRY - ENERGETIKA.....</b>	<b>17</b>
2.1 BANÍCTVO .....	17
2.2 ELEKTROENERGETIKA .....	18
2.3 PLYNÁRENSTVO .....	19
2.4 ROPA A ROPNÉ PRODUKTY .....	19
<b>3 OCHRANA KRITICKEJ INFRAŠTRUKTÚRY .....</b>	<b>20</b>
3.1.1 Ochrana kritickej infraštruktúry v USA .....	21
3.1.2 Ochrana kritickej infraštruktúry v NATO.....	22
3.1.3 Ochrana kritickej infraštruktúry v EÚ.....	22
3.1.3.1 EPCIP.....	24
3.1.3.2 CIWIN .....	25
3.1.3.3 Smernica rady 2008/114/ES .....	26
3.1.4 Ochrana kritickej infraštruktúry v ČR.....	28
3.1.5 Ochrana kritickej infraštruktúry v SR .....	30
<b>4 ODOLNOSŤ KRITICKEJ INFRAŠTRUKTÚRY .....</b>	<b>32</b>
<b>5 HODNOTENIE ODOLNOSTI .....</b>	<b>33</b>
5.1 CHARAKTERIZÁCIA AKTÍVA .....	37
5.2 CHARAKTERIZÁCIA HROZBY .....	38
5.3 ANALÝZA DOPADOV .....	40
5.4 ANALÝZA ZRANITELNOSTI .....	41
5.4.1 Priamy expertný odhad .....	41
5.4.2 Even tree analysis (ETA) .....	42
5.4.3 Hybridná kombinácia .....	42
5.5 HODNOTENIE HROZIEB .....	43
5.5.1 Metóda číselného/numerického pomeru .....	44
5.5.2 Porovnanie rizikovej tolerancie s prírodnými rizikami.....	46
5.6 HODNOTENIE RIZIKA .....	47
5.7 RIADENIE RIZIKA A ODOLNOSTI.....	48
5.7.1 Stanovenie kritérií akceptovateľnosti.....	48
5.7.2 Definícia opatrení .....	49
5.7.3 Hodnotenie opatrení .....	49
5.7.4 Akumulácia benefitov vyplývajúcich z každého opatrenia.....	49
5.7.5 Stanovenie siete benefitov a hraničných hodnôt pre každé opatrenie.....	49
5.7.6 Výber a pridelenie zdrojov pre opatrenia.....	50
5.7.7 Riadenie opatrení .....	50
5.7.8 Recyklácia procesu.....	50

<b>II PRAKTICKÁ ČÁST .....</b>	<b>51</b>
<b>6 ZEMNÝ PLYN A JEHO ŤAŽBA.....</b>	<b>52</b>
6.1 PREPRAVA ZEMNÉHO PLYNU .....	54
6.2 DISTRIBÚCIA .....	55
6.3 SKLADOVANIE.....	56
<b>7 POPIS VYBRANÉHO PRVKU KI .....</b>	<b>57</b>
7.1 CHARAKTERIZÁCIA OBJEKTU A AKTÍV .....	62
7.2 CHARAKTERIZÁCIA HROZBY .....	65
7.2.1 Teroristické hrozby .....	65
7.2.2 Prírodné hrozby .....	66
7.2.3 Hrozby zo závislosti a prepojenosti .....	66
7.3 ANALÝZA DOPADOV .....	67
7.4 HODNOTENIE HROZIEB .....	71
7.5 ANALÝZA ZRANITEĽNOSTI .....	74
7.6 HODNOTENIE RIZIKA A ODOLNOSŤ .....	76
7.7 RIADENIE RIZIKA A ODOLNOSTI.....	78
<b>ZÁVER .....</b>	<b>80</b>
<b>ZÁVER V ANGLIČTINE.....</b>	<b>82</b>
<b>ZOZNAM POUŽITEJ LITERATÚRY .....</b>	<b>83</b>
<b>SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....</b>	<b>88</b>
<b>ZOZNAM OBRÁZKOV .....</b>	<b>90</b>
<b>ZOZNAM TABULIEK .....</b>	<b>91</b>



## ÚVOD

Človek je počas celej svojej existencie vystavený veľkému počtu ohrození. K najpodstatnejším aktívam, ktoré človek chráni, patrí život, zdravie, bezpečie, životné prostredie a majetok. S nárastom nových technológií sa súčasná spoločnosť stala závislá od niektorých služieb a zariadení, pri ktorých narušení alebo zlyhaní môže dôjsť k oslabeniu národnej alebo dokonca medzinárodnej bezpečnosti a k ohrozeniu zdravia a životov obyvateľstva. Všetky tieto zariadenia a služby nazývame pojmom kritická infraštruktúra. Ich ochrana musí byť zaistená pomocou preventívnych a zmierňovacích opatrení, pripravenosti zložiek, zdrojov, zariadení a pomôcok na zvládnutie cielených útokov, dopadov živelných pohrôm, zvládnutie kritických situácií a zaistenie rýchlej obnovy systémov.

Problematika ochrany kritickej infraštruktúry sa začala riešiť najmä po tragických udalostiach z 11. septembra 2001 v USA, ale i ďalších teroristických útokoch v Madride a Londýne. Z tohto dôvodu na prvom mieste riešenia danej problematiky sa všetky štáty zameriavajú na terorizmus. Cieľom ochrany kritickej infraštruktúry je znížiť jej potenciálnu zraniteľnosť a zároveň zvýšiť jej odolnosť.

Ochranou a odolnosťou kritickej infraštruktúry sa najskôr začali zaoberať Austrália a USA až neskôr sa pripojili i štáty Európskej únie a NATO. Okrem teroristických útokov môžu nastať mimoriadne udalosti prírodného charakteru alebo z dôvodu nebanlivosti ľudského faktoru a zlyhania zariadení. Pod kritickou infraštruktúrou chápeme energetiku, telekomunikácie, počítačové systémy, internet, prenosové siete a iné dôležité služby, ktoré zabezpečujú základné funkcie štátu a ktoré môžu mať vplyv i na susedné štáty. Z tohto dôvodu je vhodné chápať i riešiť danú problematiku z globálneho hľadiska. Vzhľadom na geografické umiestnenie štátov, každá krajina vlastní osobitné kritické prvky infraštruktúry. Prírodné mimoriadne udalosti, ktoré vznikajú, sa taktiež líšia lokalizáciou a úmyselné útoky najmä politickou stratégiou, či fanatickým náboženstvom. K zdokonaleniu systému ochrany a odolnosti je však vhodné vymieňať si potrebné informácie a komunikovať s ostatnými štátmi. Pomocou všeobecného rozhľadu môže vzniknúť plnohodnotný systém hodnotenia odolnosti prvkov a sietí vo vybraných oblastiach infraštruktúry. V teoretickej časti rozoberám viacero systémov hodnotenia odolnosti, ktoré následne aplikujem na vybraný prvok kritickej infraštruktúry v praktickej časti práce.

## **I. TEORETICKÁ ČASŤ**

## 1 KRITICKÁ INFRAŠTRUKTÚRA

Pod pojmom infraštruktúra chápeme súbor zariadení, ktoré sú potrebné pre fungovanie spoločnosti. Toto slovné spojenie sa začalo využívať začiatkom 19. storočia. Pochádza z latinských slov:

- predpony infra (nižšie, pod),
- structure (stavba, výstavba). [2]

Z obecného hľadiska môžeme povedať, že infraštruktúra je množina prepojených a logicky usporiadaných prvkov, ktoré ju udržiavajú pohromade. Využíva sa v rôznych odvetviach a môžeme ju rozčleniť na:

1. Technickú – doprava, energetika, stroje, vodné a odpadové hospodárstvo.
2. Ekonomickú – zabezpečenie peňažných prevodov, sietí finančných a bankových služieb.
3. Sociálnu – školstvo, zdravotníctvo, kultúra, bývanie, obchodné siete a siete verejnej správy. [6]

Infraštruktúry môžu byť navzájom závislé v prípade, ak sa stav jednej infraštruktúry zakladá na materiálnom výstupe inej infraštruktúry. Vhodným príkladom je plynovod, ktorý poskytuje palivo pre výrobu elektriny tepelných elektrární.

Vzájomný vzťah medzi infraštruktúrou spoločnosti a ľuďmi je veľmi úzky. Infraštruktúra vznikla dlhodobou prácou ľudí, ktorí jej prevádzku neustále kontrolujú a podporujú jej rozvoj. Vznik podnietil fakt zjednodušenia ľudskej práce. Človek ju berie v dnešnej dobe ako samozrejmosť a nevie si bez nej predstaviť život. Pokiaľ infraštruktúra funguje tak ako má, väčšina ľudí sa o ňu nezaujíma. Problémy nastanú v momente, keď nevykonáva prevádzku správne alebo prestane úplne pracovať.

Do tejto skupiny patrí veľký počet odvetví. Chrániť pred hrozbou však nie je možné všetky oblasti. Každá krajina je povinná sústrediť pozornosť na oblasti najväčšieho rizika. V každej spoločnosti existuje časť infraštruktúry označovanej ako životne dôležitá, ktorá má pre fungovanie spoločnosti rozhodujúci význam. Pre štát je nevyhnutná z hľadiska hospodárskej funkcie štátu, kvality života obyvateľov, ale najmä k ochrane života, zdravia, bezpečnosti, majetku a životného prostredia. Nepriamo ale i priamo ovplyvňuje ekonomickú a spoločenskú stabilitu, obranyschopnosť a bezpečnosť. Ide o infraštruktúru, ktorá je pre chod územia veľmi dôležitá a zároveň je značne zraniteľná. Význam objektu závisí na rozmere územia. To, čo je dôležité v malom územnom celku, nemusí mať rovnakú mieru závažnosti v celoštátnom meradle alebo naopak. [2, 3, 6, 8]

## 1.1 Kritická infraštruktúra v USA

Možno povedať, že vznik a základ danej problematiky bol v USA a Austrálii. V Amerike sú rozlišované dva základné pojmy - kritická infraštruktúra a kľúčové prvky.

Pod kritickou infraštruktúrou sa chápu „*systémy a zariadenia ako hmotné tak aj virtuálne, ktoré sú životne dôležité pre USA a neschopnosť alebo zničenie takých systémov, či zariadení by malo vplyv na zníženie bezpečnosti, národnej ekonomickej bezpečnosti, národného verejného zdravia alebo bezpečia alebo na akúkoľvek ich kombináciu.*“ (9)

Kľúčové aktíva alebo zdroje sú ojedinelé prvky zvláštného významu. Ide o miesta s historickou udalosťou alebo miesta so zdržujúcou sa masou ľudí. Nemusia síce ohroziť národnú ekonomiku, ale môžu vzniknúť rozsiahle škody na životoch alebo spôsobiť podkopanie verejného sebavedomia. (9)

Tab. 1. Sektory kritickej infraštruktúry USA. [9]

Sektor	Podsektor
1. Poľnohospodárstvo, potraviny	
2. Bankovníctvo, financie	Banky, sporiteľne
3. Chémia	Základné chemikálie
	Špeciálne chemikálie
	Poľnohospodárske chemikálie
	Farmaceutika
	Spotrebné produkty
4. Obchodné zariadenie	Verejné miesta, športové areály, herne, ubytovanie, vonkajšie udalosti, zábava a médiá, nehnuteľnosti a obchody
5. Komunikácia	Telekomunikácie, satelity, bezdrôtové a drôtové siete
6. Kritická výroba	Primárna kovovýroba
	Strojárstvo
	Elektrovýroba
	Dopravné vybavenie
7. Priehradné nádrže	
8. Ochrana priemyselnej základne	Armádna výroba zbraní, výskum a vývoj
9. Záchranné služby – pohotovosť	Krízový management, zdravotníctvo, hasiči, nebezpečný materiál, výkon práva, pyrotechnici, taktické policajné tímy, pátracie tímy
10. Energia	Elektrina
	Ropa
	Zemný plyn
11. Vládne zariadenie	Federálne budovy, úrady, ambasády, súdy,...
12. Zdravotná starostlivosť a verejné zdravie	Potrúbie pre prepravu nebezpečných chemických látok

13. Informačné technológie	Hardvér, softvér, IT systémy, Internet
14. Národné pamiatky a ikony	Trvalé objekty a geografické miesta, národné dedičstvo, pripomienka významu národa
15. Jadrové reaktory, materiály, odpad	
16. Pošta a preprava zásielok	
17. Doprava	Letecká
	Cestná
	Námorná
	Hromadná verejná
	Potrubná
	Železničná
18. Voda	

## 1.2 Kritická infraštruktúra v EÚ

V dnešnej dobe existuje veľký počet kritických infraštruktúr, ktorých zničenie by malo závažné cezhraničné následky. Z anglického jazyka sa ujala skratka ECI (European critical infrastructure). V smernici 2008/114/ES sú presne zadefinované pojmy KI a ECI.

*„Kritická infraštruktúra je zložka, 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.“* (10)

*„Európska kritická infraštruktúra je kritická infraštruktúra nachádzajúca sa v členských štátoch, ktorej narušenie alebo zničenie by malo závažné dôsledky minimálne v dvoch členských štátoch Európskej únie.“* (10)

Tab. 2. Sektory kritickej infraštruktúry EÚ. [10]

Sektor	Podsektor
1. Energetika	Produkcia ropy a plynu, rafinácia, úprava, skladovanie a distribúcia potrubím
	Výroba elektrickej energie a jej rozvod
2. Jadrový priemysel	Produkcia, skladovanie a spracovanie jadrových látok
3. Informačná a komunikačná technológia (ICT)	Ochrana informačných systémov a sietí
	Automatizácia prístrojov a kontrolných systémov
	Internet
	Poskytovanie pevných telekomunikačných sietí
	Poskytovanie mobilných telekomunikačných sietí
	Rádiová komunikácia a navigácia
	Satelitná komunikácia
	Vysielanie

4. Voda	Zásobovanie pitnou vodou
	Kontrola kvality vody
	Tesenie a kontrola množstva vody
5. Potraviny	Zásobovanie potravinami a zaistenie bezpečnosti potravín
6. Ochrana zdravia	Lekárska a nemocničná starostlivosť
	Lieky, séra, očkovacie látky a liečivá
	Biologické laboratória a biologický činitelia
7. Finančné	Infraštruktúry a systémy zúčtovania a vyporiadanie obchodov s cennými papiermi
	Regulované trhy
8. Doprava	Cestná
	Železničná
	Letecká
	Vnútrozemská vodná
	Zámorská a príbrežná námorná
9. Chemický priemysel	Produkcia, skladovanie a spracovanie chemických látok
	Potrúbie pre prepravu nebezpečných chemických látok
10. Vesmír	Vesmír
11. Výskumné zariadenie	Výskumné zariadenia

### 1.3 Kritická infraštruktúra v ČR

V Českej republike je presne zadaný pojem infraštruktúra v Stavebnom zákone (t.j. zákon č. 183/2006 Sb., o územním plánování a stavebním řádu).

Verejnou infraštruktúrou sú pozemky, stavby, zariadenia a to v podobe:

1. Dopravnej infraštruktúry – stavby pozemných komunikácií, dráh, vodných ciest, letísk a s nimi súvisiace zariadenia.
2. Technickej infraštruktúry – vedenia a stavby a s nimi prevádzkovo súvisiace zariadenia technického vybavenia (vodovody, vodojemy, kanalizácie, čističky odpadných vôd, stavby a zariadenia pre nakladanie s odpadmi), trafostanice, energetické vedenie, komunikačné vedenie verejnej komunikačnej siete a elektronické komunikačné zariadenie verejnej komunikačnej siete.
3. Občianskeho vybavenia – stavby, zariadenia a pozemky slúžiace napríklad pre vzdelávanie a výchovu, sociálne služby a starostlivosť o rodiny, zdravotné služby, kultúru, verejnú správu a ochranu obyvateľstva.
4. Verejného priestranstva. [11]

Definícia kritickej infraštruktúry je sformulovaná v Krízovom zákone (t.j. zákon č. 118/2011 Sb.). Kritickou infraštruktúrou sa rozumejú „výrobné a nevýrobné systémy

*a služby, ktorých nefunkčnosť by mala závažný dopad na bezpečnosť štátu, ekonomiku, verejnú správu a zabezpečenie základných životných potrieb obyvateľstva.“ (12)*

*Tab. 3. Sektory v pôsobnosti ústredných orgánov ČR. [12]*

Sektor	Podsektor
1. Energetika	Elektrina
	Plyn
	Tepelná energia
	Ropa a ropné produkty
2. Vodné hospodárstvo	Zásobovanie pitnou a úžitkovou vodou
	Zabezpečenie a správa povrchových vôd a podzemných zdrojov vody
	Systém odpadných vôd
3. Potravinárstvo a poľnohospodárstvo	Produkcia potravín
	Starostlivosť o potraviny
	Poľnohospodárska výroba
4. Zdravotná starostlivosť	Prednemocničná neodkladná starostlivosť
	Nemocničná starostlivosť
	Ochrana verejného zdravia
	Výroba, skladovanie a distribúcia liečiv a zdravotníckych prostriedkov
5. Doprava	Cestná
	Železničná
	Letecká
	Vnútroštátna vodná
6. Komunikačné a informačné systémy	Služby pevných telekomunikačných sietí
	Služby mobilných telekomunikačných sietí
	Rádiová komunikácia a navigácia
	Satelitná komunikácia
	Televízne a rádiové vysielanie
	Poštovné a kuriérne služby
	Prístup k internetu a dátovým službám
7. Bankový a finančný sektor	Správa verejných financií
	Bankovníctvo
	Poistovníctvo
	Kapitálový trh
8. Núdzové služby	Hasičský záchranný zbor ČR a príslušné jednotky požiarnej ochrany
	Polícia ČR
	Armáda ČR
	Radiačné monitorovanie
	Predpovedná, varovná a hlásna služba
9. Verejná správa	Štátna správa a samospráva
	Sociálna ochrana a zamestnanosť
	Výkon justície a väzenia

## 1.4 Kritická infraštruktúra v SR

Kritická infraštruktúra predstavuje výrobné i nevýrobné systémy a služby, ktorých zničenie alebo znefunkčnenie spôsobí ohrozenie alebo narušenie hospodárskeho a politického chodu štátu, alebo ohrozenie života a zdravia obyvateľstva. Porušenie, poškodenie alebo zničenie infraštruktúry môže byť zapríčinené nedbalosťou, nehodami, prírodnými alebo úmyselnými činmi. Pojem vymedzuje zákon č. 45/2011 Z. z., o kritickej infraštruktúre.

*„Kritickou infraštruktúrou je systém, ktorý sa člení na sektory a prvky.“ (1,s.1)*

*„Prvkom kritickej infraštruktúry je služba vo verejnom záujme a informačný systém v sektore kritickej infraštruktúry, ktorých narušenie alebo zničenie by malo podľa sektorových kritérií a prierezových kritérií závažné nepriaznivé dôsledky na uskutočňovanie hospodárskej a sociálnej funkcie štátu, a tým na kvalitu života obyvateľov z hľadiska ochrany ich života, zdravia, bezpečnosti, majetku, ako aj životného prostredia.“*

*„Sektorom je časť kritickej infraštruktúry, do ktorej sa zaraďujú prvky; sektor môže obsahovať jeden alebo viac podsektorov kritickej infraštruktúry.“ (1,s.1)*

Tab. 4. Sektory v pôsobnosti ústredných orgánov SR. [1]

Sektor	Podsektor
1. Doprava	Cestná doprava
	Letecká doprava
	Vodná doprava
	Železničná doprava
2. Elektronické komunikácie	Satelitná komunikácia
	Siete a služby pevných a mobilných elektronických komunikácií
3. Energetika	Baníctvo
	Elektroenergetika
	Plynárenstvo
	Ropa a ropné produkty
4. Informačné a komunikačné technológie	Informačné systémy a siete
	Internet
5. Pošta	Poskytovanie poštových služieb, poštový platobný styk a obstarávateľská činnosť
6. Priemysel	Farmaceutický priemysel
	Hutnícky priemysel
	Chemický priemysel
7. Voda a atmosféra	Meteorologická služba
	Vodné stavby
	Zabezpečovanie pitnej vody
8. Zdravotníctvo	



## 2 SEKTOR KRITICKEJ INFRAŠTRUKTÚRY - ENERGETIKA

Objekt, ktorý som si vybrala pre praktickú časť spadá pod sektor energetika, preto sa budem v tejto časti venovať jej charakterizácii. Energetika patrí k najzraniteľnejším prvkom kritickej infraštruktúry. Jeho narušenie spôsobuje pre štát rozsiahle následky, preto predstavuje atraktívny cieľ teroristov. Vzniknuté dôsledky majú dva druhy účinkov:

- primárny účinok – narušenie hospodárenia s energiami v štáte,
- sekundárny účinok – vážne narušenie prvkov z ostatných sektorov (kontaminácia vody, ornej pôdy, ožiarenie ľudí pri úniku rádioaktívneho žiarenia).

Ohrozenie môže nastať v podobe technologických havárií, ľudských chýb, prírodných pohrôm, ale i terorizmu, či vojnových udalostí. Nebezpečenstvo hrozí i vadou materiálu, jeho starnutím alebo nedostatočnou údržbou a kontrolou.

Do sektoru energetiky patrí baníctvo, elektroenergetika, plynárenstvo a ropa. Štátnu správu pre tento sektor vykonáva Ministerstvo hospodárstva SR a Úrad jadrového dozoru SR. [13]

### 2.1 Baníctvo

Baníctvo a hutníctvo prispieva do kritickej infraštruktúry:

- ťažbou, úpravou a spracovaním rudných a nerudných surovín,
- vyhľadávaním a prieskumom rádioaktívnych surovín.

Medzi prvky kritickej infraštruktúry patria:

- sklady výbušnín a chemických reagentí<sup>1</sup>,
- ťažby rádioaktívnych surovín,
- sklady poloproduktov a koncentrátov.

Narušenie, poškodenie, či zničenie tohto podsektora sa prejavuje nárastom ceny a nedostatkom surovín. [13]

---

<sup>1</sup>čínidlo, vo všeobecnosti chemická látka, ktorá sa v laboratóriu používa na spúšťanie chemických reakcií.

## 2.2 Elektroenergetika

Elektrická energia je jeden z najdôležitejších článkov národnej ale i európskej kritickej infraštruktúry. Poháňa veľkú časť spotrebičov v každej domácnosti. Osvetľuje mestá, zaisťuje chod škôl, obchodných stredísk, nemocníc, dodáva energiu pre prenos informácií pomocou komunikačných systémov. Táto skutočnosť naznačuje vzájomné prepojenie funkcií viacerých systémov. Je závislá od iných prvkov KI, pretože elektrárne môžu byť poháňané rôznymi druhmi palív (napr. zemným plynom).

Slovensko sa zaraďuje medzi štáty s dobrými zásobami elektrickej energie, ktorú vyrábajú atómové elektrárne v Jaslovských Bohuniciach a Mochovciach. Zásobujú svojím výkonom veľkú časť krajiny. Nie sú jediným poskytovateľom, okrem nich disponuje Slovensko i tepelnými a vodnými elektrárnami. Elektrárne sú cenným objektom KI, ktorého poškodením vznikajú zdrvivúce následky. Najväčšie riziká hrozia práve u jadrových elektrární, kedy výpadok elektrickej energie by bol ten najmenší problém. Kvôli možným nebezpečenstvám, ktoré so sebou jadrové elektrárne prinášajú (najmä výbuch úmyselným alebo i neúmyselným zapríčinením), a znečisťovaniu životného prostredia, je nevyhnutné ustúpiť od jadrovej energie a prijať nové alternatívne spôsoby energie. Na Slovensku sa začala vo veľkej miere využívať slnečná, geotermálna a veterná energia a energia z biomasy.

„Podsektor zahŕňa:

- výrobu, dovoz, vývoz, prenos a distribúciu elektrickej energie,
- nakladanie s jadrovým palivom,
- nakladanie s rádioaktívnym odpadom vzniknutým pri výrobe elektrickej energie v jadrových elektrárnach.“ (13)

Prvkami kritickej infraštruktúry sú objekty:

- jadrových, tepelných, vodných elektrární a elektrární s kombinovanou výrobou elektriny a tepla,
- výrobní elektrickej energie z obnoviteľných zdrojov,
- prenosových a distribučných sústav vrátane transformátorových staníc,
- úložísk rádioaktívnych odpadov a medziskladov vyhoretého paliva. [13]

## 2.3 Plynárenstvo

Zemný plyn sa ťaží spoločne s ropou. Na Slovensko je dovážaný tranzitnými plynovodmi z Ruska. Slúži ako zdroj energie pre vytápanie, varenie a ohrev teplej vody. Stlačený zemný plyn s označením CNG alebo skvapalnený plyn s označením LNG sa využíva ako pohon motorových vozidiel.

Podsektor zahŕňa ťažbu, dovoz, prepravu, distribúciu a uskladnenie zemného plynu. Prvkami KI tohto podsektora sú:

- objekty ťažobnej siete,
- distribučná sieť vrátane regulačných staníc,
- prepravná sieť (tranzitné plynovody, priame plynovody, kompresorové stanice a vnútroštátne prepúšťacie stanice, zásobníky plynu a tuzemské zdroje, v ktorých je vykonávaná ťažba plynu). [13]

## 2.4 Ropa a ropné produkty

Ropa je tmavohnedá až čierna kvapalina, ktorá sa vyskytuje vo veľkých hĺbkach pod zemským povrchom i pod dnom morí. Vznikla rozkladom zvyškov rastlín a živočíchov pri zvýšenom tlaku. Tento proces trvá niekoľko miliónov rokov.

Ropa má rozmanité využitie. S jej koncentráciou sa stretávame predovšetkým v pohonných látkach, brzdovej kvapaline, nemrznúcej zmesi, hnojivách, výbušninách a v asfalte. Nevyhneme sa jej výskytu ani v potrebách denného života ako je oblečenie, farby, laky, plastové výrobky a dokonca i v niektorých kozmetických výrobkoch a liekoch.

„Podsektor zahŕňa:

- dovoz, ťažbu, prepravu, spracovanie, distribúciou a uskladnenie ropy a ropných produktov,
- núdzové zásoby ropy a ropných výrobkov i tvorbu štátnych hmotných rezerv.

Jeho prvky tvoria objekty ropovodov a tranzitných trás, prečerpávacie stanice, skladovacie terminály, sklady nádrží, zásobníky ropy a ropných produktov, spracovateľské závody (rafinérie).“ (13)

### 3 OCHRANA KRITICKEJ INFRAŠTRUKTÚRY

Ochrana KI má zásadný význam pre vnútornú bezpečnosť krajiny. Akékoľvek narušenie alebo zničenie prvku kritickej infraštruktúry môže mať za následok straty na ľudských životoch, vážne poškodenie ľudského zdravia, majetkové škody, zničenie životného prostredia a najmä stratu dôveryhodnosti subjektu.

Úroveň zabezpečenia priamoúmerne súvisí s množstvom investícií, ktoré sú do ochrany vložené. Čím viac peňazí sme schopný investovať, tým máme väčšiu záruku bezpečnej prevádzky daného prvku. Žiadny štát nie je taký bohatý, aby dokázal stopercentne ochrániť svoju národnú kritickú infraštruktúru. Výšku financií určíme po hĺbkovom poznaní objektov KI a vytvorení stratégie. Stratégiu chápeme ako dlhodobý plán k dosiahnutiu vytýčeného cieľa. V tomto prípade ide o dlhodobý zámer ako predchádzať nevídaným udalostiam a stanoviť účinnú prevenciu. Žiadne dočasné ani krátkodobé riešenia nie sú dostatočné. Cieľom každej infraštruktúry je dosiahnuť stav, kedy je pre užívateľov bezpečná a funguje v plnom pracovnom nasadení. Úlohou spoločnosti je udržať funkčnosť kritickej infraštruktúry za akýchkoľvek podmienok, za bežných, mimoriadnych i kritických situácií. Takže nejde len o výnimočné situácie ohrozenia života a štátu, ale i o zachovanie v bežnej prevádzke. Dôležitou súčasťou ako správne ochrániť infraštruktúru je vyhladať stav, kedy neposkytuje služby v požadovanom čase a v požadovanej kvalite, čiže hranicu akceptovateľnej degradácie funkcie.

Bezpečnosťou by sa mal zaoberať predovšetkým štát, pretože má neobmedzený prístup k informáciám, vydáva legislatívne nariadenia, spracováva plány a vlastní niektoré zariadenia kritickej infraštruktúry. Na ochrane sa okrem štátu podieľajú i súkromné subjekty, do ktorých zaraďujeme vlastníkov alebo prevádzkovateľov stavieb a zariadení KI. Na ochrane by sa však malo podieľať i zvyšné obyvateľstvo. Pravidelne a dôkladne musí byť pripravené na obmedzenia alebo výpadky KI a dostávať dostatočné informácie o ochrane.

Ochranou najdôležitejšej infraštruktúry sa začali štáty zaoberať po útoku 11. septembra 2001, kedy došlo k teroristickému útoku v USA.

Pod pojmom ochrana sa skrýva niekoľko dôležitých činností:

- analýza zraniteľnosti základných funkcií spoločnosti, zdravia, ochrany, bezpečnosti a kvality života pred hrozbami,

- identifikácia prvkov kritickej infraštruktúry, určenie protiopatrení a postupov k ochrane,
- vykonávanie ochrany v súlade s legislatívnymi normami, bezpečnostným plánom a inými stanovenými schválenými plánmi. [1, 2, 3, 6]

### 3.1.1 Ochrana kritickej infraštruktúry v USA

USA bol jeden z prvých štátov, ktoré sa problematikou ochrany kritickej infraštruktúry začali zaoberať. V roku 1998 už existoval ucelený dokument v Amerike ako tzv. *Biela kniha* z roku 1998. V tejto smernici 63 chcel prezident Bill Clinton prijať potrebné opatrenia, aby sa znížil počet fyzických i kybernetických útokov na ich KI. Akékoľvek prerušenie alebo manipulácia musí byť zriedkavejšia, zvládnuteľná a mať minimálny dopad na životné podmienky obyvateľov USA. Potrebná je úzka spolupráca a koordinácia s miestnymi štátmi a záchranármi pre flexibilný program ochrany infraštruktúry. Navrhla vytvoriť plán pre varovanie, ktorý by úzko spolupracoval s FBI<sup>2</sup> a FEMA<sup>3</sup>. [14]

Bezprostredne mesiac po teroristickom útoku 2001 bolo prezidentom Bushom vydané *Vládne nariadenie na ochranu kritickej infraštruktúry*. Dokument bol zameraný na ochranu informačných systémov pre KI. V roku 2003 bola vypracovaná *Národná stratégia vnútornej bezpečnosti*, ktorá sa zaoberala predchádzaním teroristických útokov. Jasne špecifikuje potenciálne útoky a ciele, pre ktoré vznikajú. Najvšeobecnejším dokumentom USA sa stala *Národná stratégia fyzickej ochrany kritickej infraštruktúry a kľúčových zariadení* z roku 2003, ktorá opisuje súhrn problematiky ochrany kritickej infraštruktúry.

Identifikáciu prvkov KI popisuje nariadenie prezidenta *Homeland Security Presidential Directive 7*. [9]

---

<sup>2</sup> Federal Bureau of Investigation (Federálny vyšetrovací úrad) slúži nielen ako vyšetrovací úrad ale súčasne ako kontrarozviedka a vedúca agentúra pre krízový management. Pôsobí ako vyšetrovací orgán amerického ministerstva spravodlivosti.

<sup>3</sup> Federal Emergency Management Agency (Federálna agentúra pre zvládanie krízy) odstraňuje následky škôd po živelných pohromách alebo nehodách väčšieho rozsahu.

### 3.1.2 Ochrana kritickej infraštruktúry v NATO

V roku 2004 bol na istanbulskom samite schválený *Program obrany proti terorizmu* (Defence Against Terrorism - DAT). Ochrana kritickej infraštruktúry je jednou z 10 oblastí, ktorou sa projekt zaujíma. V roku 2009 z odporúčaní expertov vznikla *Ochrana pred nekonvenčnými hrozbami*. NATO aktívne pracuje na ochrane KI vo forme vzdelávania personálu, zodpovedných pracovníkov, a obyvateľstva o spôsoboch a metódach ochrany KI v národných podmienkach. Problematika spadá pod kompetenciu Vyššieho výboru NATO pre civilné núdzové plánovanie (NATO Senior Civil Emergency Planning Committee - SCEPC). Riešenie problematiky sa číní s účasťou vládnych a mimovládnych organizácií, Rady Európy, Európskej únie, Medzinárodného výboru Červeného kríža, Medzinárodnej agentúry pre atómovú energiu, Organizácie OSN pre výchovu, vedu a kultúru (UNESCO), Úradu Vysokého komisára OSN (UNICEF), Úradu OSN pre koordináciu humanitárnych záležitostí (UN-OCHA), Svetovej zdravotníckej organizácie (WHO) a iných. [13, 15]

### 3.1.3 Ochrana kritickej infraštruktúry v EÚ

Medzi prvé európske štáty, ktoré sa začali zaoberať problematikou kritickej infraštruktúry, patria Veľká Británia a Nemecko. Vo Veľkej Británii v roku 1999 bolo zriadené *Koordináčne centrum pre bezpečnosť národnej infraštruktúry* (NISCC - National Infrastructure Security Coordination Centre). Organizácia NISCC bola vytvorená ako súčasť Ministerstva vnútra, ktoré malo riadiť a koordinovať vládne podnety pre ochranu KI proti kybernetickým útokom.

Rada Európskej únie<sup>4</sup> požiadala v júni 2004 o spracovanie súhrnnej stratégie na ochranu kritickej infraštruktúry pre posilnenie ochrany kritickej infraštruktúry. Následne na to 20. októbra 2004 prijala európska komisia *Oznámenie o ochrane najdôležitejšej infraštruktúry v boji proti terorizmu*, ktoré predstavuje návrhy k zlepšeniu prevencie teroristických útokov na kritickú infraštruktúru, pripravenosť a reakciu na ne. Do kritickej infraštruktúry zahrnuli:

- energetické zariadenia a siete,

---

<sup>4</sup> Oficiálna inštitúcia, ktorá prijíma právne predpisy, dohody, schvaľuje rozpočet a koordinuje bezpečnostnú a zahraničnú politiku. Skladá sa z ministrov členských štátov.

- komunikačné a informačné technológie,
- financie (bankovníctvo, cenné papiere a investície),
- jedlo,
- vodu (priehrady, skladovanie, úprava a siete),
- dopravu (letiská, prístavy, železničnú a cestnú hromadnú dopravu a systémy riadenia letovej prevádzky),
- výrobu, skladovanie a prepravu nebezpečných materiálov (chemické, biologické a jadrové materiály),
- vládu (kritické služby, zariadenia, informačné siete, majetok a pamiatky).

Oznámenie navrhlo kritériá na určenie kritickej infraštruktúry danej krajiny:

- rozsah geografickej oblasti, ktoré by mohli byť postihnuté,
- rozsah a účinky v závislosti na čase. [16]

Dňa 5. novembra 2004 bol schválený *Haagsky program*, ktorý objasňoval potrebu posilnenia súčasných činností civilnej ochrany.

Európska komisia<sup>5</sup> usporiadala semináre k predloženiu návrhov a pripomienok členských štátov 6. – 7. júna a 12. – 13. septembra 2005 a predložila *Zelenú knihu*, v ktorej sa zaoberá možnosťami pre EPCIP.

Zelené knihy sú dokumenty vydávané Európskou komisiou na zvolené témy s cieľom diskutovať v rámci Európskej únie o svojich predložených návrhoch. Konzultácie môžu vyústiť k praktickým návrhom, k uskutočneniu v publikácii Bielej knihy. Zelená kniha teda slúži ako východiskový dokument pre budúce legislatívne opatrenia.

Záverom všetkých konferencií bol deň 8. december 2008, kedy Rada Európy prijala *Smernicu 2008/114/ES, o identifikácii a označení európskych kritických infraštruktúr a zhodnotení potreby zlepšiť ich ochranu*.

Každý členský štát má zodpovednosť za ochranu kritickej infraštruktúry vo svojej krajine, teda na svojom území. Následky zničenia národnej kritickej infraštruktúry však môžu mať vážne dopady i v ďalších susedných štátoch. [16, 17]

---

<sup>5</sup> Jedna z hlavných inštitúcií EÚ, ktorá pripravuje návrhy nových európskych právnych predpisov, spravuje rozpočet, riadi a kontroluje činnosť politiky Únie. Má 27 členov a to zástupcov z každého členského štátu.

### 3.1.3.1 EPCIP

The European Programme for Critical Infrastructure Protection (Európsky program na ochranu najdôležitejšej infraštruktúry) má za úlohu zaistiť dostatočnú bezpečnostnú úroveň ochrany európskej kritickej infraštruktúry. Ochrana každého prvku KI musí byť riešená samostatne podľa hrozieb, ktoré na danú infraštruktúru môžu pôsobiť. Európsky program musí zminimalizovať všetky negatívne hroziace dopady. Je potrebné zohľadniť všetky riziká rovnako, či už sa jedná o úmyselné útoky alebo prírodné pohromy. Zvýšená pozornosť je zameraná na terorizmus.

V záujme celkovej bezpečnosti je vhodné vypracovať spoločný postup (tzv. akčný rámec), ktorý bude nápomocný všetkým členským štátom za použitia vhodných opatrení v znižovaní nebezpečenstva. Je nevyhnutné zaviesť spoločný rámec na ochranu kritickej infraštruktúry, pretože nie každý členský štát by poskytoval dostatočnú úroveň ochrany a tým by mohol ohroziť zvyšné štáty. Uľahčí sa týmto spôsobom identifikácia, výmena i šírenie najlepších postupov a kontrolných mechanizmov danej problematiky. Zadefinujú sa presné právomoci a zodpovednosť všetkých subjektov. Priamu zodpovednosť za ochranu ECI nesú nielen členské štáty, ale i vlastníci a prevádzkovatelia KI.

Základné princípy:

- **subsidiarita:**
  - zodpovednosť členských štátov, vlastníkov a prevádzkovateľov predovšetkým na národnej úrovni,
  - zodpovednosť komisie na ochranu s cezhraničným dosahom v rámci EÚ,
- **doplňkovosť** – dopĺňanie existujúcich opatrení,
- **dôvernosť** – poskytovanie informácií by zostalo v dôvernom prostredí, aby nemohli byť zneužitú,
- **spolupráca zainteresovaných subjektov** – vzájomná spolupráca v rozvoji EPCIP vlastníkov, prevádzkovateľov, štátu a normalizačných úradov,
- **proporcionálnosť** – vhodnými technikami sústrediť pozornosť na najrizikovejšie oblasti, pretože je nemožné ochrániť všetko. [18, 19]



### 3.1.3.2 CIWIN

Critical Infrastructure Warning Information Network (Varovná informačná sieť najdôležitejšej infraštruktúry) je súčasťou Európskeho programu na ochranu najdôležitejšej infraštruktúry. CIWIN je sieť technicky navrhnutá firmou UNISYS Belgium na podnet Európskej rady. Vznikla pri vypracovaní celkovej stratégie ochrany kritickej infraštruktúry Európskej komisie. Keďže poškodenie národnej infraštruktúry môže mať dopad i na situáciu v iných štátoch Európskej únie, je potrebná dostatočná vzájomná informovanosť členských štátov. Zvyšuje sa tým i vzájomná stabilita a dôvera dotknutých štátov. Hlavným cieľom je pomáhať pri vymieňaní informácií o spoločných hrozbách, zraniteľných miestach, stratégiách, vhodných opatreniach pri zmiernení rizík, či hrozieb. Umožňuje koordináciu a spoluprácu členských štátov týkajúcu sa informácií o ochrane kritickej infraštruktúry. Zaručuje zabezpečenú a štruktúrovanú výmenu informácií medzi zúčastnenými štátmi. Každý štát je zodpovedný za ochranu kritickej infraštruktúry patriacej do jeho pôsobnosti, ale nie je schopný ako samostatný celok uchrániť celú EÚ. Nedokáže ani samostatne zabezpečiť celoeurópsku výmenu informácií a rýchlych varovaní. Pre tieto dôvody je nevyhnutná spolupráca väčšiny, ak nie všetkých členov EÚ. Účasť v CIWIN je umožnená všetkým štátom Európskej únie, avšak platnosť začína až podpísom Memoranda o porozumení. Povinnosť, ktorá vyplýva z daného dokumentu, je zostaviť vlastný tím. Zostavený národný tím bude mať na starosti sledovať a riadiť využívanie siete CIWIN národnými užívateľmi a:

- prideľovať a odnímať prístupové práva,
- schvaľovať zverejnenie dokumentov,
- zabezpečovať technickú podporu. [20]

Najväčší problém vo varovnej informačnej sieti je problematika výmeny informácií a varovaných signálov.

Navrhované možnosti politiky sú:

1. možnosť neprijíma žiadny nový návrh politiky a tým pádom by si členské štáty riešili problémy individuálne.
2. návrh by vyžadoval pre svoju funkciu zmenu existujúcej IT architektúry a i úpravu jej právneho základu k funkcii rýchleho varovania.

3. alternatíva by fungovala formou nezabezpečenej výmeny informácií, kedy by bola prístupná i širokej verejnosti. Informovanosť členských štátov medzi sebou by bola rapídne zvýšená, avšak musel by sa značne selektovať výber informácií.
4. možnosť je navrhnutá v zabezpečenej avšak nepovinnej forme. Obsahovala by 2 funkcie:
  - a. systém rýchleho varovania,
  - b. elektronické fórum na výmenu informácií.

Do prevádzky by musel byť zavedený informačný nástroj, ktorý by tento prenos citlivých údajov bol schopný prevádzkovať a ukladať až po najvyššiu úroveň utajenia.

5. varianta CIWIN slúži ako povinný viacúrovňový komunikačne/varovný systém s rovnakými funkciami ako v predchádzajúcej možnosti. [20]

Členské štáty a Komisia musia prijať tieto bezpečnostné opatrenia:

- zabrániť neoprávnenému prístupu osoby,
- nezneužívanie právomoci oprávnených osôb (prístup len k nevyhnutným údajom),
- znemožniť kopírovaniu, upravovaniu, mazaniu, či čítaniu neoprávneným osobám.

Operatívny cieľ CIWIN je „poskytnúť nástroj IT, ktorý uľahčí spoluprácu členských štátov v oblasti ochrany KI, poskytne efektívnu a rýchlu alternatívu často časovo náročných metód vyhľadávania informácií a poskytne členským štátom možnosť priamo komunikovať a poskytovať informácie, ktoré považujú za dôležité.“ (2)

### 3.1.3.3 Smernica rady 2008/114/ES

Smernica rady 2008/114/ES o identifikácii a označení európskych kritických infraštruktúr a zhodnotená pre potreby zlepšiť ochranu je záväzný dokument EÚ.

Cieľom tejto smernice je určiť a označiť ECI a posúdiť potrebu zvýšiť jej ochranu. Každý členský štát má povinnosť informovať ostatné štáty, na ktoré môže mať potenciálna ECI závažný vplyv o dôvodoch označenia. Až po dohode s týmito štátmi je možné infraštruktúru označiť ako ECI. Každý členský štát predkladá komisii každé dva roky súhrnné údaje o druhoch rizík, hrozieb a zraniteľných miest v jednotlivých sektoroch, vďaka čomu môže komisia vypracovať spoločný vzor.

Ďalej definuje možnosti zaobchádzania s citlivými informáciami. Každá osoba, ktorá prichádza do styku s utajovanými skutočnosťami musí mať minimálne zodpovedajúci alebo vyšší stupeň bezpečnostnej previerky. Poznáme štyri stupne utajenia vyhradené, dôverné, tajné a prísne tajné.

Definuje presný postup pri vytváraní bezpečnostného plánu prevádzkovateľa v rámci európskej kritickej infraštruktúry:

1. presne identifikovať dôležité zariadenia,
2. uskutočniť analýzu rizika z hľadiska možných hrozieb, zraniteľných miest a možných dôsledkov,
3. vybrať, určiť a identifikovať protiopatrenia a postupy. [19]

Komisia môže byť nápomocná pri identifikácii potenciálnych ECI po požiadavke štátu. Inak si každý štát volí ECI sám podľa postupu:

- v 1. kroku vyjadruje prvý výber KI v rámci sektora,
- v 2. kroku na vybranú KI z prvého kroku uplatní definíciu kritickej infraštruktúry,
- v 3. kroku na vybranú KI z druhého kroku uplatní definíciu európskej kritickej infraštruktúry,
- v 4. kroku uplatní prierezové kritériá na potenciálne ECI, ktoré prešlo predchádzajúcimi bodmi. [10]

Potenciálna ECI, ktorá nespĺňa niektoré z daných kritérií sa ďalej nepovažuje za ECI.

Pod prierezovými kritériami, ktoré vychádzajú zo závažnosti dôsledkov sú chápané:

- straty na životoch (počet mŕtvych i zranených osôb),
- hospodársky vplyv (hospodárske straty, zhoršenie výrobkov, služieb a vplyv na životné prostredie),
- vplyv na verejnosť (strata dobrého mena, strata dôvery). [10]

Každý členský štát má povinnosť informovať ohrozené štáty o identifikácii a vytýčiť dôvody jej označenia za potenciálnu ECI. Ohrozené štáty sa zapoja do rokovaní a narozdiel od Komisie musia mať prístup k podrobným informáciám. Štát, ktorý nie je označený a cíti sa byť ohrozený, podá Komisii návrh o zapojení sa do rokovania. Túto požiadavku komisia zváži a oznámi štátu s potenciálnou ECI.

Až po dohode zo všetkými dotknutými štátmi je možné označiť ECI. Členské štáty každoročne informujú Komisiu o počte označených ECI a sektore i o závislých štátoch a každé dva roky o druhoch hrozieb, rizík a zraniteľných miest. Proces sa zakončí informovaním vlastníka alebo prevádzkovateľa označenej infraštruktúry a vydá sa príslušný stupeň utajenia.

Medzi vlastníkom a príslušným orgánom členského štátu je poverený diskutovať o každej označenej ECI styčný úradník pre bezpečnosť. Komisia svoju podporu prejavuje sprístupnením najlepších procesov, metodík, odborným vzdelávaním, výmenou informácií o vývoji v oblasti ochrany kritickej infraštruktúry. [10]

### 3.1.4 Ochrana kritickej infraštruktúry v ČR

Samostatný zákon, ktorý by upravoval ochranu kritickej infraštruktúry zatiaľ v Českej republike neexistuje. Zastávajú ho niektoré zákony o systéme krízového riadenia:

- zákon č. 238/2000 Sb., o Hasičském záchranném sboru České republiky,
- zákon č. 239/2000 Sb., o Integrovaném záchranném systému,
- zákon č. 240/2000 Sb., o Krizovém řízení,
- zákon č. 241/2000 Sb., o Hospodářských opatřeních pro krizové stavy.

Výsledkom práce posúdenia situácie v oblasti riešenia problematiky ochrany KI v ČR bola *Komplexná stratégia ČR k riešeniu problematiky kritickej infraštruktúry*. Nadväzuje na predchádzajúce dokumenty a materiály, ktoré boli predmetom jednaní v rámci schôdzí Výboru pre civilné núdzové plánovanie, Bezpečnostnej rady štátu a vlády ČR. V súlade s platnou Bezpečnostnou stratégiou chráni záujmy ČR, ktoré sa delia na:

- **životné záujmy** – ochrana životných záujmov štátu a jeho občanov,
- **strategické záujmy** – predovšetkým zaistenie ekonomickej bezpečnosti ČR prostredníctvom posilňovania globálnej ekonomickej stability, diverzifikáciu zdrojov strategických surovín, výrobkov, služieb, zdrojov a foriem kapitálových tokov a ochrany strategických infraštruktúr,
- **ostatné záujmy** – ochrana životného prostredia, presadzovanie princípov udržateľného rozvoja, znižovanie kriminality a potlačenie extrémizmu, zaistenie prevencie na nepredvídateľné živelné, ekologické a priemyselné havárie. [21]

Komplexná stratégia predstavuje zhrnutie prejednaných, schválených a budúcich krokov, ktoré budú rozpracované v Národnom programe ochrany KI do konkrétnych úloh pre príslušných nositeľov ich plnenia.

*Národný program ochrany kritickej infraštruktúry* pojednáva problematiku:

- stanovenia zásad určovania prvkov kritickej infraštruktúry – určenie základných kritérií pre určenie prvkov, ktorými sú nenahraditeľnosť, nahraditeľnosť, prierezové kritériá (počet obetí, ekonomický dopad, dopad na verejnosť) a odvetvové kritériá (technické alebo prevádzkové hodnoty) ,
- uskutočnenia legislatívnych úprav – návrh novely krízového zákona,
- stanovenia konkrétnych nositeľov úloh – vláda ČR, ministerstvo vnútra, ministerstvá a iné ústredné správne úrady a subjekty kritickej infraštruktúry,
- vypracovania programu pre ochranu KI – hĺbkové riešenie ochrany KI s ohľadom na konkrétnych účastníkov,
- vytvorenia podmienok pre financovanie – finančné zabezpečenie v potrebnom rozsahu,
- podpory výstupov a výsledkov vedeckého rozvoja – vytváranie bezpečnostných výskumov a programov,
- zaistenia vzdelávania v oblasti ochrany KI – tvorenie vzdelávacích programov v oblasti pripravenosti a zvládania mimoriadnych udalostí či krízových situácií.

[21]

Úprava krízového zákona sa udiala niekoľkokrát. K dnešnému dátumu je platná verzia *zákonu č. 118/2011 Sb.*. Vymedzuje základné pojmy súvisiace s krízovým riadením a ochranou kritickej infraštruktúry. Zaoberá sa finančným zabezpečením krízových opatrení na bežný rozpočtový rok. V Hlave II určuje orgány krízového riadenia a ich povinnosti, ktoré musia vykonávať. Definuje i povinnosti a práva právnických, podnikajúcich osôb a subjektov kritickej infraštruktúry. Každý subjekt je právne povinný viesť plánovaciú, organizačnú alebo technickú dokumentáciu. V pláne krízovej pripravenosti subjektu KI sú identifikované možné ohrozenia funkcie prvku a stanovené opatrenia na jeho ochranu. Kontrolnú činnosť v medziach svojej pôsobnosti vykonávajú orgány krízového riadenia. Nedodržaním pokynov tohto zákona vznikajú správne delikty. Pri menších priestupkoch je pokuta vydaná od 20 000 Kč do 100 000 Kč podľa závažnosti vzniknutého priestupku. Za správne delikty právnických a podnikajúcich fyzických osôb sa môže pokuta vyšplhať až do nemalej čiastky 3 000 000 Kč. [12]

### 3.1.5 Ochrana kritickej infraštruktúry v SR

Jedným z prvých dokumentov, ktorý riešil problematiku ochrany kritickej infraštruktúry je zákon č. 319/2002 Z. z. o obrane Slovenskej republiky v znení neskorších predpisov. Infraštruktúru nepopisoval ako kritickú, ale obrannú, ktorá v čase vojnového stavu slúži k zabezpečeniu obrany štátu.

Po konferenciách v rámci Európskej únie, ktoré sa snažili zlepšiť úroveň ochrany si aj Slovenská republika začala uvedomovať, že v tomto smere má obrovské nedostatky. Nechala sa inšpirovať už skúsenými a vyspelejšími štátmi a v roku 2006 vydala *Koncepciu kritickej infraštruktúry v Slovenskej republike a spôsob jej ochrany a obrany*. Zaoberá sa v prvom rade ochranou pred terorizmom, ale prihliada i na potrebu komplexnej ochrany. Základom koncepcie je zadefinovať terminológiu pre pochopenie daného problému, aby nevznikali zbytočné nedorozumenia. Orientačne vymedzila sektory národnej infraštruktúry, ktoré boli nápomocné v určení sektorov a prvkov kritickej infraštruktúry. Pre uľahčenie uviedla základné kritéria pre tvorbu prvkov:

- pravdepodobnosť ohrozenia prvkov teroristickým útokom,
- riziko narušenia politického chodu alebo obranyschopnosti štátu,
- jedinečnosť/nenahraditeľnosť daného prvkov. [13]

Vymedzila zodpovednosti, kde okrem verejnej správy (vláda, súdy, ministerstvá, ozbrojené sily, bezpečnostné zbory...) zahrnula aj vlastníkov a prevádzkovateľov prvkov KI. Hlavným cieľom koncepcie je konkretizovať spôsob ochrany, akými prostriedkami a nástrojmi je možné sa brániť pred ohrozením. Popisuje krízové riadenie a smerovanie bezpečnostného výskumu v oblasti riešenia ochrany a obrany kritickej infraštruktúry. Určitú časť venuje i ochrane utajovaných skutočností.

Do roka vznikol nový dokument za odobrenia Bezpečnostnej rady *Národný program pre ochranu a obranu kritickej infraštruktúry Slovenskej republiky*, ktorý zhodnotil súčasný stav kritickej infraštruktúry. Oproti predchádzajúcemu dokumentu presnejšie identifikoval a popísal sektory. Pričlenil k nim subjekty, ktorým vytýčil úlohy k plneniu. Podobne ako v iných štátoch bolo hlavnou úlohou vytvoriť:

- harmonogram plnenia opatrení na ochranu a obranu KI,
- medzirezortný program na finančné zabezpečenie,
- a stanoviť národného gestora. [22]

Proces tvorby uceleného legislatívneho nástroja v problematike ochrany a obrany kritickej infraštruktúry sa ukončil minulý rok, kedy bol vydaný zákon č. 45/2011 Zb. o kritickej infraštruktúre. Vychádza zo spomínanej smernice EÚ 2008/114/ES. Je v súlade s Ústavou Slovenskej republiky a súvisiacimi zákonmi:

- zákon č. 261/2002 Z. z. o prevencii závažných priemyselných havárií a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- zákon č. 319/2002 Z. z. o obrane Slovenskej republiky v znení neskorších predpisov,
- zákon č. 541/2004 Z. z. o mierovom využívaní jadrovej energie (atómový zákon) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a ostatnými všeobecne záväznými právnymi predpismi.

Vymedzuje základné pojmy, ktoré sa danej problematiky týkajú. Ustanovuje štruktúru ústredných orgánov štátnej správy k ich priradeným sektorom KI, kde na vrchole pôsobnosti je postavená vláda SR. Určuje postup ústredných orgánov pri identifikácii prvku KI a ECI pomocou sektorových a prierezových kritérií. V sektorových kritériách sa prihliada na charakteristické znaky konkrétneho sektora KI. Pri prierezových kritériách sa zohľadňuje počet ohrozených osôb, hospodársky vplyv a vplyv na verejnosť. Dôležitým krokom zákona je oblasť striktne daných povinností prevádzkovateľa:

- uplatniť účinnú technológiu k ochrane,
- zaviesť bezpečnostný plán do šiestich mesiacov od poverenia,
- priebežne prehodnocovať a prípadne aktualizovať bezpečnostný plán,
- dostatočne oboznámiť svojich zamestnancov s daným bezpečnostným plánom,
- určiť oprávnenú osobu a poskytnúť ústrednému orgánu potrebné materiály,
- každé 3 roky vykonať modelovú situáciu,
- v prípade hrozby postupovať podľa definovaného bezpečnostného plánu. [1]

Základným právnym nástrojom ochrany je bezpečnostný plán. Vo vzniknutých nejasnostiach a hrozbách je kontaktná osoba sprostredkovateľom medzi prevádzkovateľom prvku, príslušným ústredným orgánom a ministerstvom. Za nedodržanie striktne daných povinností alebo vyzradenie citlivých informácií, čo je považované za priestupky, môžu byť udelené pokuty od 200 € až do výšky 200 000 €. [1]

V júni 2011 bol schválený utajovaný dokument *Návrh sektorových a prierezových kritérií na určenie prvkov kritickej infraštruktúry*, ktorý napomáha pri určovaní prvkov KI.

## 4 ODOLNOST KRITICKEJ INFRAŠTRUKTÚRY

Hlavnou úlohou ochrany kritickej infraštruktúry je zaistiť bezpečnosť. Odolnosť je schopnosť štátu zaistiť plnenie funkcie štátu v krízových situáciách. Ochrana výrazným spôsobom ovplyvňuje celkovú úroveň odolnosti použitím ochranných opatrení. Základnými vlastnosťami kritickej infraštruktúry sú:

- **výkonnosť** – miera dosahovaných výsledkov kritickej infraštruktúry,
- **ekonomická efektívnosť** – stav, kedy výkon KI prekonal ekonomické náklady na ich dosiahnutie,
- **zraniteľnosť** – vyjadruje podmienky, za akých príde k nesplneniu cieľovej funkcie systému,
- **odolnosť** – schopnosť prevádzkovať systém i v nepriaznivých podmienkach. [3]

Z uvedeného vyplýva, že zraniteľnosť je svojím spôsobom opakom odolnosti. Čím nižšia je zraniteľnosť, tým väčšou odolnosťou prvok KI oplýva a naopak, čím je zraniteľnejší prvok, tým ľahšie je vyradený z prevádzky. Činitele, ktoré ovplyvňujú funkciu KI delíme na vnútorné a vonkajšie. K vnútorným patrí spoľahlivosť odolnosti systému voči vplyvom technických porúch a nesprávnej manipulácie. Vonkajšie činitele ovplyvňujúce odolnosť sú predovšetkým živelné pohromy, kybernetické a fyzické útoky.

Stanoviť mieru odolnosti je možné pomocou ukazovateľov:

- **robustnosť** – vnútorná odolnosť systému voči vonkajším faktorom bez zmeny funkcie systému,
- **redundancia** – vlastnosť systému využiť v rámci riešenia mimoriadnych udalostí alternatívne zdroje, náhrady a miesta,
- **reakciaschopnosť** – schopnosť využiť a zmobilizovať všetky dostupné sily a prostriedky v prípade vzniku kritickej situácie. [4]

Pre vnútornú bezpečnosť každého podniku je dôležité určiť štyri strategické ciele odolnosti, ktoré zahŕňajú akcie pre zvládanie dôsledkov akejkoľvek udalosti a jej rýchlej opätovnej prevádzky:

- posilnenie pripravenosti,
- účinná reakcia na mimoriadne udalosti,
- rýchle zotavenie,
- zmiernenie nebezpečenstva. [24]



## 5 HODNOTENIE ODOLNOSTI

Po vydaní zákonov o ochrane KI si štáty začínajú uvedomovať ďalšiu problematiku v danej oblasti. Je nemožné uvažovať o obecnom modeli v rámci KI, ale vznikajú pokusy, ktoré by mohli byť veľmi významné a nápomocné. Jedným z nich je i RAMCAP Plus (Risk Analysis and Management for Critical Assets Protection) metóda, ktorá bola vyvinutá americkou spoločnosťou ASME<sup>6</sup> začiatkom roka 2009 v New Yorku. Výsledok sa vyvinul v spolupráci a značného úsilia mnohých dobrovoľníkov, vedcov, inžinierov pre dané oblasti, akademikov, štátnych úradníkov a iných. Proces trval nejaký čas od prvotných stretávok cez schôdze výborov až po presné štúdiá a prezentácie. Vznik podmienili udalosti zo septembra 2001 i iné teroristické útoky a mnohé prírodné katastrofy v Spojených štátoch amerických, z ktorých najzávažnejší bol hurikán Katrina<sup>7</sup>. V roku 2005 zachvátilo Ameriku hneď niekoľko hurikánov (Dennis, Emily, Ophelia, Rita a Wilma), ale Katrina mala najväčšiu intenzitu a najničivejší charakter v celej histórii USA. Ďalším vplyvným faktorom boli aj odporúčania z konferencie Bieleho domu v roku 2002 k ochrane KI. [5]

Príručka popisuje postup pre analýzu a riadenie rizík a odolnosti kritickej infraštruktúry a systémov. Program zahŕňa 7 odvetví pre ktoré je použiteľná:

- jadrová energia,
  - jadrový odpad, doprava a skladovanie,
  - chemický priemysel,
  - rafinácia ropy,
  - zemný plyn,
  - priehrady,
- 

<sup>6</sup> American Society of Mechanical Engineers spoločnosť založená v roku 1880 ako Americká spoločnosť strojníkov. Profesionálne združenie podporuje výskum a vzdelávanie, vyvíja normy a štandardy, ktoré zvyšujú bezpečnosť obyvateľstva a poskytuje celoživotné vzdelávanie.

<sup>7</sup> Tropický cyklón, ktorý sa objavil 24. augusta 2005 nad Bahamami. Svoju silu nabral o 5 dní neskôr, kedy dosiahol 5. stupeň intenzity na juhovýchode USA a spôsobil enormné škody. Najviac zasiahnuté mesto bolo New Orleans, kde prelomil hrádzu, čoho následkom bolo zatopenie 80% územia mesta. Následok bol katastrofálny. Počet obetí bol zhruba 1800, milión ľudí sa v okamihu stalo bezdomovcami a vzniknuté škody presahovali 26 miliárd dolárov.

- voda a odpadové systémy. [5]

Cieľom je vytvoriť spoločný mechanizmus pre komparáciu rizík a ich riadenie. Vývojom procesu sa rozšíril pôvodný zámer zníženia rizika terorizmu o posilnenie organizácie odolnosti a schopnosti rýchlej obnovy plnej funkčnosti po nežiaducej udalosti. Bol vyvinutý pre uľahčenie analýzy a riadenia rizík a odolnosti kritických zariadení a infraštruktúr. RAMCAP Plus postup je určený pre neustále vyvíjanie sa na základe skúseností alebo prispôbením sa novým odvetviam a meniacim sa potrebám národa. Patrí medzi kvantitatívne metódy, pretože odhaduje číselné hodnoty rizika, odolnosti, zhodnotenie zraniteľnosti, možnej pravdepodobnosti vzniku nepriaznivých udalostí a možné následky. Taktiež vyžaduje popisy nekvantifikovateľných následkov, do ktorých patria psychologické dôsledky, dôvera verejnosti a vojenská pripravenosť. Výsledkom je úsudok o hodnote možností ako znížiť riziká a zvýšiť odolnosť kritickej infraštruktúry:

- pravdepodobnosť, zraniteľnosť a následky prírodných katastrof,
- zvýšená pozornosť na bezprostrednú závislosť dodávateľských reťazcov,
- meranie odolnosti,
- analýza nákladov,
- hrozba kontaminácie produktu.

V národnom pláne pre ochranu infraštruktúry a rovnako tak v rámci RAMCAP je riziko definované ako súčin pravdepodobnosti hrozieb, možnej zraniteľnosti a spôsobených následkov.

Pre potreby ďalšej práce tohto procesu boli zadefinované základné terminologické pojmy:

**Riziko** - potenciálna strata alebo poškodenie v dôsledku nežiaducich udalostí a ich dopadov. Meria sa kombináciou pravdepodobnosti a možných dopadov nežiaducich udalostí. Ak sú tieto hodnoty vyjadrené numerickým odhadom, očakávané riziko sa vypočíta ako súčin oboch hodnôt. V prípade využitia RAMCAP Plus procesu alebo aj iných relevantných analýz, je riziko výsledkom hrozby, zraniteľnosti a dopadu nežiaduceho vzniknutého incidentu.

**Hrozba** – náznak, okolnosť alebo udalosť, ktorá má potenciál spôsobiť stratu alebo poškodenie majetku, či ľudských životov. V prípade ohrozenia prírodnými katastrofami sa hrozba vníma a popisuje historickou frekvenciou naplnenia konkrétnej prírodnej hrozby. U hrozby uvažujeme o pravdepodobnom vzniku udalostí.

**Zraniteľnosť** – chyba zabezpečenia, teda slabý bod aktíva alebo štruktúry infraštruktúry. V analýze rizík ide o podmienenú pravdepodobnosť, že vzhľadom k útoku alebo prírodnej katastrofe budú odhadované dôsledky a škody.

**Dopady** – dôsledky, ktoré vyplynú z udalosti. Môžeme ich rozdeliť na krátkodobé, dlhodobé, priame a nepriame straty či dopady. K najpodstatnejším kvantitatívnym následkom patria ľudské straty na životoch, zranenia, finančné a ekonomické škody a dopad na životné prostredie. Výsledkom však môžu byť z hľadiska nehmotného a nemerateľného politické následky, znížená morálka i dôvera a zníženie prevádzkovej efektívnosti alebo vojenskej pripravenosti.

Ďalším kľúčovým pojmom je odolnosť, ktorá síce nie je prvkom rovnice analýzy ale pre účely RAMCAP Plus procesu je veľmi dôležitá.

**Odolnosť** – schopnosť fungovať a prevádzkovať bezproblémovo a v dostatočnej miere doterajšiu činnosť po útoku alebo prírodnej katastrofe a v čo najkratšom čase vrátiť aktívum do počiatočného stavu. Dôležitú úlohu hrá parameter času, ktorý sa meria od začiatku udalosti až po návrat k plne funkčnej prevádzke.

Samotný proces realizácie prístupu a procesu RAMCAP Plus je koncipovaný a rozdelený do siedmych analytických oblastí. Ako celok poskytujú presný, objektívny a transparentný základ zberu dát, výklad dát, analýzu a proces rozhodovania. Výsledok tvorí cenný nástroj pre pochopenie, porozumenie a efektívnu alokáciu zdrojov v procese riadenia rizík a odolnosti. Prvých päť krokov tvorí základný nástroj pre vybudovanie stanovenia hodnoty rizika v organizácii. Posledné dva kroky pojednávajú o zhodnotení, analýze a rozhodovacích krokoch, ktoré sú založené na údajoch zhromaždených v predchádzajúcich krokoch. Spomínanými procesnými krokmi sú:

1. Charakterizácia aktív – vymedzuje, ktoré zariadenia a aktíva sú nevyhnutné pre plnenie poslania alebo funkciu organizácie.
2. Charakterizácia hrozby – definuje aké konkrétne hrozby pre každé aktívum hrozia.
3. Analýza dopadov – je odhadom najhoršieho možného výsledku dopadu konkrétnej hrozby na konkrétne aktívum.
4. Analýza zraniteľnosti – je odhadom pravdepodobnosti, že konkrétny útok na konkrétne aktívum vzniká do odhadovaného dopadu a to aj vo vzťahu k efektívnosti existujúcich bezpečnostných opatrení.

5. Hodnotenie hrozieb – je odhadom alebo pravdepodobnosťou, že nastane očakávaná udalosť.
6. Hodnotenie rizika a odolnosti – odhad rizika a odolnosti je určený posudzovaním pre každú udalosť a každé aktívum.
7. Riadenie rizika a odolnosti – posúdenie rizík i odolnosti a spôsoby zníženia rizík spolu s možnosťou zvýšenia odolnosti.

Vo väčšine prípadoch je proces spracovávaný vyškolenými pracovníkmi z oblasti analýzy rizík do 3 alebo 4 dní. Nevyžaduje sa žiadna odborná poradenská pomoc. Tím, ktorí sa zaoberá touto problematikou sa skladá poväčšine z vedúceho pracovníka, zamestnancov, bezpečnostného pracovníka a pracovníka požiarnej alebo núdzovej ochrany. Výnimku tvorí iba vodný sektor, kde sa používajú podstatne podrobnejšie a komplexnejšie nástroje na hodnotenie rizík, čo môže trvať až niekoľko týždňov.

Výsledky sú priamo porovnateľné s podnikmi rovnakého odvetvia a ďalších kritických infraštruktúr. RAMCAP Plus proces je vhodný k pravidelnému opakovaniu merania pokroku, znižovaniu rizík a zvyšovaniu odolnosti. Pravidelné opakovanie pomáha popisovať správy o pokroku. Môžu sa vykonávať trebárs raz do roka alebo podľa potreby na základe meniacej sa okolnosti hrozieb. [5]



Obr. 1. Sedem krokov procesu RAMCAP. [5]

## 5.1 Charakterizácia aktíva

Prvá fáza sa zaoberá výberom aktív, ktoré sú dôležité v rámci ochrany. Bolo by zbytočné míňať čas a peniaze na menej významné aktíva. Vybrané zariadenia pre ďalšiu analýzu sú tie, ktoré môžu mať veľmi závažné dôsledky alebo sú dôležité pre systémy, ktoré by mohli mať nežiaduce následky. Aktíva zahŕňajú celú škálu materiálnych i nemateriálnych zdrojov, ktoré umožňujú prevádzku. Čím podrobnejšie poznatky majú hodnotitelia o každom aktíve, tým majú väčšiu pravdepodobnosť úspechu splnenia požadovaného cieľu. Je dobré predpokladať, že protivník je veľmi informovaný a zručný a tomuto faktoru treba vhodne prispôbiť svoje hodnotenie.

Druhá fáza výberu sa skladá zo šiestich úloh:

- **Identifikácia kritických funkcií** – hodnotiaci tím identifikuje kritické funkcie v organizácii z pohľadu dôležitosti, ktoré dosahujú stanovené ciele spoločnosti.
- **Identifikácia kritických aktív** – môžeme chápať ako majetok organizácie, vrátane ľudí, zariadení, systémov, produktov a informácií potrebných pre udržanie kritických funkcií organizácie.
- **Identifikácia kritickej infraštruktúry a kritických vzájomných závislostí** – identifikácia kritických interných a externých infraštruktúr a ich vzájomných prepojení. Môžu zahŕňať elektrickú energiu, pohonné hmoty, zemný plyn, telekomunikácie, dopravu, počítačové systémy a iné systémy, ktoré vstupujú a sú oporou kritických operácií a funkcií každého aktíva. Niektoré môžu byť mimo kontrolu vlastníka alebo prevádzkovateľa, avšak treba pochopiť a identifikovať závislosti a vzájomné prepojenie zariadení, rovnako ako dôsledky vyplývajúce zo straty týchto systémov.
- **Identifikácia existujúcich protiopatrení** – hodnotiaci tím identifikuje a dokumentuje súčasný stav zabezpečenia (vrstiev bezpečnostného systému). To môže zahŕňať fyzickú bezpečnosť, kybernetickú a operačnú bezpečnosť i administratívnu kontrolu. Cieľom je zhromaždiť informácie o type zabezpečenia a bezpečnostnej stratégii a splňanie stavebných predpisov a noriem. Mnohé zo štandardov sa vzťahujú k bezpečnostnej ochrane zdravia zamestnancov a verejnosti a tým nepriamo tvorí protiopatrenia voči niektorým hrozbám, najmä prírodným.

- **Identifikácia potenciálnych dopadov** – Prípadné následky môžu byť určujúcim faktorom pri rozhodovaní, či konkrétne aktívum je dostatočne kritické a má byť zahrnuté do ďalších krokov. Odhad možných následkov poškodenia alebo straty majetku, bez ohľadu na spôsob útoku, je spoľahlivý spôsob ako rýchlo a účinne odfiltrovať aktíva, ktoré si nezaslúžia väčšiu pozornosť. Pod ekonomickými dôsledkami chápeme priame náklady na opravu, prerušenie prevádzky, náklady na likvidačné práce a obnovu.
- **Vyjadrenie cieľov pre ďalšie analýzy** – pomocou predchádzajúcich bodov tím vypracuje zoznam kritických funkcií a aktív, ktoré sú najviac ohrozené z hľadiska útokov a ktoré majú drvivé následky. [5]

## 5.2 Charakterizácia hrozby

V tomto kroku sú dostatočne podrobne odhadnuté riziká a dôsledky, ktoré daná hrozba môže spôsobiť. RAMCAP Plus proces sa zaoberá tromi typmi ohrozenia:

- teroristické hrozby,
- prírodné hrozby,
- hrozby zo závislosti a prepojenosti. [5]

### 1. Teroristické hrozby

Jeden alebo viac útočníkov sa snaží poškodiť alebo zničiť aktíva, zariadenia alebo systémy, pričom bráni jej schopnosti plniť svoje poslanie alebo funkciu a spôsobuje značné hospodárske škody alebo straty na životoch. Terorizmus je priamy útok na práva a slobodu občanov, útokom na demokraciu a právny charakter štátu. Je plánované, premyslené a politicky motivované násilie, ktoré sa zameriava proti nezúčastneným osobám, slúžiace k dosiahnutiu vytýčených cieľov. V dnešnej dobe sa jedná o najviac rozšírenú hrozbu, preto vznikajú protiteroristické medzinárodné skupiny. Terorizmus zostáva aj v roku 2012 fenomén, proti ktorému sme bezmocný. Jedná sa o atentáty, únosy ľudí, lietadiel, lodí, rôzne bombové, chemické, biologické, radiačné a kybernetické útoky, či útoky pomocou zbraní hromadného ničenia. Pre terorizmus je charakteristické vytýčenie určitej ideológie, či už sa jedná o ekonomické, politické alebo náboženské ciele národného, medzinárodného alebo svetového charakteru k dosiahnutiu definovaných cieľov fanatickým spôsobom, aby zanechal po sebe silnú stopu v podobe paniky a strachu. Kritická infraštruktúra je vďaka svojmu charakteru dôležitej súčasťou života spoločnosti jeden z najlákavejších cieľov pre útočníkov.

## 2. Přírodní hrozby

Udalosti vyplývajúce z extrémov prírodných procesov, ktoré negatívne ovplyvňujú ľudskú spoločnosť a jej záujmy. Nebezpečenstvo, ktoré je natoľko významné, že podstatne znižuje schopnosť aktíva, zariadenia alebo systému vykonávať svoju funkciu. Za základné prírodné katastrofy považuje RAMCAP Plus hurikán, tornádo, záplavy a zemetrasenie. Riziko každej z nich sa odhaduje na základe stanovenia predpokladanej frekvencie udalostí a odhadu dôsledkov. Ostatné prírodné katastrofy sú zahrnuté v prípade, ak pravdepodobnosť výskytu alebo následky sú rovnaké alebo aj vyššie ako u spomínaných štyroch. Patria k nim napríklad lavíny, tsunami, snehové kalamity, búrky a požiare. Závažnosť a frekvencia prírodných katastrof závisí od zemepisnej polohy aktíva alebo objektu. Zatiaľ čo sú zemetrasenia objavované na západnom pobreží Ameriky a na Aljaške, tak hurikány trápia pobrežie Atlantiku. V našich zemepisných šírkach sú každoročne opakované zväčša len záplavy, požiare a snehové kalamity. Zvyšné sa objavujú málokedy alebo sa u nás ešte ani nevyskytli. Údaje o prírodných kalamitách sú presne zaznamenávané, čo umožňuje pomerne presný odhad frekvencie opakovania. Historický záznam obsahuje základnú líniu pre porovnanie. Zmenou globálnej klímy sa dnešné rozpätia katastrof mierne líšia.

## 3. Hrozby zo závislosti a prepojenosti

Hrozby, ktoré by mohli brániť výkonu funkcie celého zariadenia, nie len konkrétneho aktíva. Životne dôležité závislosti majú zariadenia na verejné služby, dodávky, dopravné zariadenia, zamestnancov i zákazníkov. Na rozdiel od predchádzajúcich hrozieb, tieto riziká spracovávajú ušlý zisk na majetku a službách. Len málo z nich môže spôsobiť fyzické poškodenie zariadení. Problém nastáva v prípade, keď sa zariadenie nachádza v blízkosti iného zariadenia, na ktorom je realizovaná teroristická alebo prírodná hrozba. Príkladom by mohol byť útok na tunel alebo most, ktorého cieľom je narušiť dopravu, avšak zároveň poruší i iné prvky infraštruktúry (vodu, plyn, telekomunikačné a elektrické vedenie). Dĺžka trvania útoku je priamoúmerná dôsledkom. Pri kratšej dobe nemusia vzniknúť žiadne negatívne následky, alebo vznikajú také, ktoré sú prijateľné. Čím dlhšie útok trvá, tým horšie dopady spôsobí. Táto časť dopĺňa predchádzajúce hrozby o ďalšie relevantné scenáre, ale nemali by byť zahrnuté do sčítania rizika.

V neposlednom rade je dôležité pospárovať dvojice aktív a hrozieb. Vynechávajú sa málo pravdepodobné spojenia a ďalej sa pracuje iba s možným prepojením dvojíc. [5]

### 5.3 Analýza dopadov

Bezprostredné nadviazanie na predchádzajúce body spočíva v popise vzniknutých párov (aktíva a hrozby), ktoré sú presne zadefinované v bode 2. Postup odhadu je vhodný zvoliť od najväčších možných drastických dopadov až po najmenej závažné. Zvyšuje sa týmto spôsobom efektívnosť analýzy. K odhadu sa používajú dva účely:

- zameranie sa na miesto s maximálnymi možnými škodami,
- hrozba môže byť uskutočnená na rôznych miestach.

Táto časť sa zaoberá podrobnejším návodom na odhad vykazovania dôsledkov úmrtia či vážnych zranení a finančných i hospodárskych strát.

Závažné zranenia vedú k pracovnej neschopnosti a zdravotnému postihnutiu. Objavia sa okamžite alebo v krátkej dobe narozdiel od zdravotných problémov, ktorých rozpätie odhalenia môže byť aj niekoľko týždňov. V Amerike majú zopár programov, ktoré napomáhajú pri odhadoch počtu zranených osôb. Jedným z nich je aj the U.S. Army Corps of Engineers blast effects simulations.

Ekonomické dopady sú považované za kľúčové ukazovatele následkov v analýze rizík. Odhad finančných a ekonomických strát vyžaduje pohľad dvoch zainteresovaných subjektov:

- vlastníci alebo prevádzkovatelia kritickej infraštruktúry, ktorí sú zodpovední za zaistenie bezpečnosti a spoľahlivosť svojich zariadení,
- široká verejnosť, najmä dodávateľia a zákazníci, pre ktorých je najdôležitejšia kvalita a spoľahlivá prevádzka.

Majiteľ má na starosti finančne zabezpečiť:

- opravy a reprodukčné náklady na poškodenom majetku,
- náklady spojené s prerušením prevádzky,
- nápravu životného prostredia,
- sankcie za nedodržanie dohodnutých požiadaviek,
- ostatné náklady, ktoré priamo súvisia s útokom.

Vytvorí sa vstupno-výstupný model, kde hlavnými vstupmi sú hrubé príjmy v dôsledku prerušenia prevádzky, doba prerušenia a údaje o oblasti, v ktorej sa objekt nachádza. Straty niekoľkonásobne narastajú, v prípade ak sa jedná o kritickú infraštruktúru (zemný plyn, elektrina, voda), pretože nie sú dostupné žiadne alternatívne spôsoby náhrady.



## 5.4 Analýza zraniteľnosti

Analýza zraniteľnosti spočíva v podmienenej pravdepodobnosti predpokladanej hrozby z predchádzajúceho bodu. Posudzovanie prebieha s ohľadom na:

- podrobnú špecifikáciu hrozieb (počet útočníkov, použité zbrane, spôsob prepravy),
- podrobnosti o aktíve (konštrukcia, použité systémy a ich rozloženie),
- stávajúcu ochranu,
- informácie o personálnom obsadení.

Tab. 5. Stanovenie zraniteľnosti. [5]

Stanovenie zraniteľnosti				
Numerická hodnota zraniteľnosti		Decimálna hodnota	Percentuálna hodnota	Úspešnosť uplatnenia danej hrozby
5	A	0,90 - 1,00	90 - 100	$9/10 \leq L \leq 1$
	B	0,75 - 0,89	75 - 89	$3/4 \leq L \leq 9/10$
	C	0,5 - 0,74	50 - 74	$1/2 \leq L \leq 3/4$
4		0,25 - 0,49	25 - 49	$1/4 \leq L \leq 1/2$
3		0,125 - 0,249	12,5 - 24,9	$1/8 \leq L \leq 1/4$
2		0,0625 - 0,124	6,25 - 12,4	$1/16 \leq L \leq 1/8$
1		0,0312 - 0,0624	3,12 - 6,24	$1/32 \leq L \leq 1/16$
0		< 0,0311	< 3,11	$L < 1/32$

V tomto procese realizácie je možné použiť aj iné formy analýzy zraniteľnosti, ktoré sú všeobecne akceptované. Pre stručnosť pojednám len o niektorých.

### 5.4.1 Priamy expertný odhad

Členovia hodnotiaceho tímu odhadujú relevantným spôsobom mieru zraniteľnosti, na základe svojich predošlých skúseností a znalostí.

Jednou z najvyužívanějších metód expertného odhadovania je **DELPHI metóda**. Určuje za akých podmienok môže nastať kritická situácia. Najskôr sa ustanoví 3-5 členná komisia, ktorá riadi celý proces, zadefinuje problém a prevedie ho do formy dotazníku. Ďalej zostaví zoznam možných expertov. Ich počet býva zhruba 10. Spracovaný dotazník spolu s dostatočnými informáciami o probléme rozošle zvoleným expertom, ktorý riadne vyplní dotazník spolu s odôvodením svojich odpovedí a pošlú naspäť. Členovia komisie vyhodnotia zhodné i odlišné názory a podľa toho zostavia ďalší dotazník k prehodnoteniu svojho stanoviska. Nový dotazník opäť rozošle expertom.

Z dôvodu väčšej zhody účastníkov sa postup 2-3krát opakuje, než komisia spracuje konečnú správu o stanovenom výslednom odhade.

Ďalšou spomínanou metódou je **Analytický hierarchický proces (AHP)**. Pomáha zjednodušiť a zrýchliť prirodzený proces rozhodovania v zložitých rozhodovacích situáciách. Rozkladá zložité neštruktúrované situácie na jednoduchšie komponenty. Na každej úrovni hierarchickej štruktúry sa použije metóda kvantitatívneho párového porovnania, z ktorého vyplynie komponent s najvyššou prioritou. Štruktúra pozostáva z niekoľkých úrovní, pričom každá z nich obsahuje niekoľko prvkov. Najvyššiu úroveň hierarchie obsahuje vždy len jeden prvok, ktorý definuje cieľ analýzy. Postupne sa pridávajú ďalšie komponenty podľa vzťahu k danej problematike. Čím obecnnejšie sú prvky vzťahu k danému rozhodovaciemu problému, tým zaujímajú vyššiu úroveň. Na hodnotení sa podieľa viac hodnotiteľov. [5]

#### 5.4.2 Even tree analysis (ETA)

Analýza stromu udalostí je vizuálne zobrazenie všetkých udalostí, ktoré môžu nastať. S počtom udalostí rastie i graf podobne ako koruna stromu. Rozvíja postup sledujúci priebeh procesu od iniciačnej udalosti cez konštruovanie udalosti na základe 2 možností (priaznivých i nepriaznivých). To značí, že ide o binárne rozhodovanie. Patrí medzi graficko-štatistické metódy kvantitatívneho alebo kvalitatívneho charakteru. Postup je nasledovný:

- identifikovať a definovať závažné udalosti, ktoré môžu viesť k nechceným dôsledkom,
- identifikovať prekážky, ktoré môžu spôsobiť náhodné udalosti,
- nakresliť strom udalostí,
- popísať potenciálne výsledky nepredvídateľných udalostí,
- určiť frekvenciu náhodnej udalosti a pravdepodobnosť,
- vypočítať pravdepodobnosť/frekvenciu pre identifikované následky,
- zhrnúť a prezentovať závery analýzy. [5]

#### 5.4.3 Hybridná kombinácia

Krížením prvých troch metód dostávame spoľahlivejší odhad. Používajú sofistikovanejšie hodnotenie expertov spočívajúce v rôznych hodnotiacich tímoch alebo rôznych metódach hodnotenia. Postupy odlišných metód sa porovnávajú a následne vyhodnotia.

## 5.5 Hodnotenie hrozieb

Piaty krok odhaduje pravdepodobnosť vzniku hrozby a jej frekvencie opakovania. V procese je práve tento bod považovaný za veľmi zložitý a zásadný pre ďalšie analýzy. Je rozdelený do štyroch oblastí.

### Terorizmus

V prípade terorizmu sa hodnotenie rizík skladá z dostupných dôkazov o protivníkovi a odhadu pravdepodobnosti, že sa protivník bude zaoberať daným aktívom. Môžu mať jedného, dvoch útočníkov, ale takisto môže útočiť organizovaná skupina o 20-tich alebo viacerých členoch. Je veľký rozdiel chrániť sa pred jedným útočníkom, alebo veľkej skupine. Útok dvadsiatich vyzbrojených a vycvičených páchatel'och zvyšuje výdavky na ochranu.

### Prírodné hrozby

U prírodných pohrôm sa vychádza z historických údajov o frekvenciách daných hrozieb na určenom mieste, hoci nemusia byť do budúcnosti presné kvôli vznikajúcim globálnym klimatickým zmenám.

### Hrozby zo závislostí

Závislosť rizika vyplýva z prerušenia bezprostredného dodávateľského reťazca, takže odhad pravdepodobnosti súvisí s historickými poznatkami o frekvenciách prerušovania daného prvku.

### Hrozby z prepojenosti

Blízkosť nebezpečenstva odráža hodnotu pravdepodobnosti v závislosti od susedného objektu.

V danej problematike sa využívajú 3 metódy:

1. **Číselný pomer** – predpokladaný celkový počet útokov v danom roku v USA. Odhad ovplyvňujú historické údaje, spravodajské informácie alebo predpoklady. Číselná pravdepodobnosť sa ďalej odvíja od počtu dostupných cieľov, cieľovej atraktivity, vnímanie náročnosti úspechu útoku a zložitosti uskutočnenia útoku. Celková úprava spočíva v celkovom spracovaní rozdielov medzi jednotlivými mestami a typmi aktív.

2. **Porovnanie rizikovej tolerancie s prírodnými rizikami** – zrovnáva pravdepodobnosti ohrozenia teroristickými útokmi s prírodnými hrozbami. Ak je nebezpečenstvo terorizmu zhodné alebo nižšie, tak je riziko prijateľné.
3. **Investičný zvrat** – metóda využívajúca sa ako súčasť siedmeho kroku, pretože vyžaduje výpočet na základe rizika, koncepčný návrh a odhad nákladov na investičné varianty podstatne znížiť riziká a posúdiť riziká. Vzhľadom k odhadovaným dôsledkom, ohrozeniam a možnostiam nákladov, môže byť vypočítaný bod nulový, teda pomer medzi nákladmi a prínosmi by tvoril hodnotu 1. Ak je skutočná pravdepodobnosť menšia ako vyrovnaná pravdepodobnosť, tak sa projekt neodporúča.

Je vhodné, aby sa využili aspoň 2 metódy pre porovnanie. Pravdepodobnostné odhady sú založené na predpoklade. Nie je možné určiť frekvenciu každého útoku.

### 5.5.1 Metóda číselného/numerického pomeru

Táto metóda poskytuje priamy výpočet pravdepodobnosti útoku za použitia informácií získaných z rôznych bežne dostupných zdrojov. V najjednoduchšej forme sa odhaduje základná pravdepodobnosť útoku na určité aktívum v určitom zariadení umiestnenom kdekoľvek v krajine USA. Niektoré metropolitné štáty a oblasti majú vyššiu prioritu pre teroristov ako iné, preto sa predpoklad upravuje.

#### Príklad:

Počet útokov  $N$  v kalendárnom roku je 1. V národnom pláne (National Infrastructure Protection Plan) je zahrnutých 18 kritických infraštruktúr spolu s kľúčovými zdrojmi. Predpoklad, že pravdepodobnosť útoku je rovnaká pre všetky oblasti značí, že pravdepodobnosť, že konkrétna oblasť zažije útok je približne 0,0556 podľa nasledujúceho vzorca:

$$\frac{N}{KI} = \frac{1}{18} = 0,0\overline{555}. \quad (1)$$

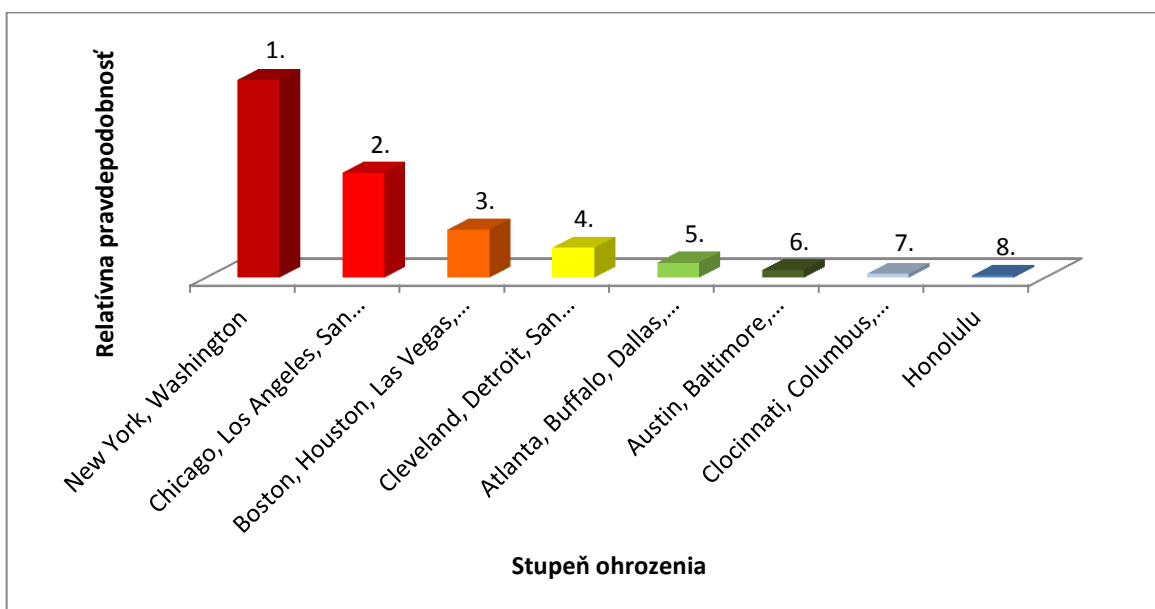
V prípade, ak by spĺňalo kritériá pre výber  $Y=15\ 000$  potenciálnych cieľov v každej oblasti, potom by pravdepodobnosť vyzerala nasledovne:

$$\frac{\frac{N}{KI}}{Y} = \frac{\frac{1}{18}}{15000} = 0,0000\overline{037}. \quad (2)$$

Ak sa predpokladá, že by mohlo dôjsť k maximálne 10 útokom do roka, tak pravdepodobnosť útoku na konkrétny cieľ v danom zariadení bude  $3,7 \cdot 10^{-5}$  akcií za rok. To znamená, že nebezpečenstvo zasiahnutia daného cieľa má veľmi malú šancu spôsobiť škodu podľa vzorca:

$$\frac{N}{\frac{KI}{Y}} = \frac{10}{\frac{18}{15000}} = 0,000037. \quad (3)$$

Predošlé predpoklady, že všetky potenciálne ciele majú rovnakú možnosť napadnutia je príliš zjednodušené a nesprávne. Štúdia dokázali, že niektoré oblasti v krajine majú väčší potenciál napadnutia pred ostatnými. Vyplýva to z grafu na obrázku 2.



Obr. 2. Graf pravdepodobnosti napadnutia miest v USA. [5]

Z obrázka je zrejmé, že najväčšie mestá New York a Washington DC majú oveľa vyššie riziko napadnutia než ostatné. Model RMS bol v rámci vyvinutý predpovedať riziko pre poisťovne. Na základe grafu je možné dospieť k záveru, že pravdepodobnosť útoku na zariadenie umiestnenom v Austine v Texase je oveľa nižšia, než pravdepodobnosť útoku na identické zariadenie vo Washington, DC. Informácie z obrázka majú napomôcť pri úprave vypočítanej pravdepodobnosti z posledného vzorca.

Okrem umiestnenia zariadenia je dôležitým faktorom ovplyvnenia pravdepodobnosti i cieľový typ skupiny. Pravdepodobnosť útoku pre každú skupinu je vyznačovaná číslami 1-8 vzostupne (viz Tab. 6).

Tab. 6. Rozdelenie skupín podľa pravdepodobnosti útoku. [5]

Číslo skupiny	Objekty v danej skupine
1	vládne budovy
2	obchodné centrá, mrakodrapy, burzy, hotely, kasína, letiská, jadrové elektrárne
3	vojenské a vlakové stanice, stanice metra, štadióny, mosty a tunely
4	priemyselné zariadenia, ropa a zariadenie na spracovanie plynu, turistické zaujímavosti, nákupné centrá, reštaurácie, prístavy a lode
5	divadlá, hlavné centrá, plynové stanice
6	lode, bytové domy, zahraničné konzuláty, organizácie USA
7	vodojemy a rozvody, osobné vlaky, lietadlá
8	elektrárne, priehrady, železničná sieť

Ďalšími nemenej dôležitými faktormi sú zložitost' útoku, dostupné zdroje na teroristu a hodnota cieľu. Podľa názoru autorov neistota pri výpočte pravdepodobnosti je väčšia ako číselné hodnoty získané pre pravdepodobnosť. [5]

### 5.5.2 Porovnanie rizikovej tolerancie s prírodnými rizikami

Kým pravdepodobnosť teroristického útoku je rátaná pomocou niektorých faktorov a je tým pádom odhadovaná s možnými veľkými nepresnosťami, tak prírodné hrozby sa opierajú o pravdivé udalosti. S dnešnou vyspelou dobou je tieto riziká možné predpovedať s väčšou presnosťou po dlhodobých výskumoch odborníkov a znalcov. Veľa prírodných katastrof súvisí s intenzitou a rýchlosťou vetra. V dnešnej dobe je pre každú oblasť špecifikovaná najvyššia možná rýchlosť vetra. Všetky infraštruktúry musia byť prispôsobené tejto rýchlosti a bezproblémovo jej odolať.

Vhodným prípadom môže byť porovnanie rizika pri ceste do práce, ktoré môže nastať, s rizikom vzniku teroristického útoku. Ak riziko teroristického útoku je nižšie ako známe tolerované riziko každodenného charakteru, potom je prijateľná miera rizika i vstupné investície. Ak ale vznikne väčšie riziko, potom boli nedostatočné opatrenia a je nevyhnutné zvýšiť vstupné náklady.

Ak je známa úroveň rizika  $R$ , predpokladá sa i zraniteľnosť  $V$  a odhaduje sa konkrétna hrozba, tak pravdepodobnosť dôsledkov  $T$  môže byť určená ako:

$$T = \frac{R}{(C * V)}. \quad (4)$$

Vypočítaná pravdepodobnosť dôsledkov je dôležitá pre rozhodovanie v oblasti investícií do zvýšenia bezpečnosti alebo naopak k zníženiu. [5]

## 5.6 Hodnotenie rizika

V 6. kroku sa zozbierajú výsledky z predchádzajúcich piatich krokov pre ich zosumarizovanie. Z dôvodu, že všetky body vychádzali z odhadu, nie je možné počítať s úplnou presnosťou. Existuje vysoká miera neistoty vo všetkých podmienkach daných rovníc.

Hodnotu rizika vypočítame z nasledujúcej rovnice:

$$\text{Riziko} = \text{Hrozba} \times \text{Zraniteľnosť} \times \text{Dopad}. \quad (5)$$

Kde:

**Riziko** – potenciálna strata v dôsledku pôsobenia nepredvídanej udalosti, ktorá spôsobuje negatívne dôsledky.

**Hrozba** – udalosť, ktorá má potenciál spôsobiť stratu, zničiť aktíva alebo populáciu. Pri analýze rizík sa vyjadruje pravdepodobnosťou, že udalosť nastane.

**Zraniteľnosť** – chyba zabezpečenia a slabé miesto infraštruktúry, ktoré narušiteľ využije. V analýze rizík ide o podmienenú pravdepodobnosť, že vzhľadom k útoku alebo prírodnej katastrofy budú odhadované dôsledky a škody.

**Dôsledky** – výsledok výskytu udalosti. Medzi najzávažnejšie zaraďujeme ľudské straty, zranenia, finančné a ekonomické straty.

Pri tomto kroku však potrebujeme vypočítať i hodnotu odolnosti.

Platí:

$$\text{Odolnosť}^{\text{majiteľa}} = \text{Ušlý zisk} \times \text{Riziko} \times \text{Hrozba}. \quad (6)$$

$$\text{Odolnosť}^{\text{spoločenstva}} = \text{Strata ekonomickej aktivity} \times \text{Riziko} \times \text{Hrozba}. \quad (7)$$

Kde:

**Ušlý zisk** - možno definovať ako to, čo poškodenému ušlo v dôsledku spôsobenia škody, teda ujma spočívajúca v tom, že u poškodeného nedošlo v dôsledku škodnej udalosti k rozmnoženiu majetkových hodnôt, hoci sa to s ohľadom na pravidelný beh vecí dalo očakávať. Neprejavuje sa zmenšením majetku, ale stratou očakávaného prínosu.

**Strata ekonomickej aktivity** – zníženie hodnotenia kvality a efektivity podmienok a výstupov podnikania.

## 5.7 Riadenie rizika a odolnosti

V poslednom kroku sa vykonáva efektívne rozhodovanie o zriadení alebo zlepšení bezpečnostného protipatrenia, zlepšení taktiky zmiernenia následkov, posudzuje a upravuje redundanciu, vytvára havarijné plány, výcviky a cvičenia. Siedmy krok sa zaoberá optimalizáciou pridelovania finančných prostriedkov výberom investičných možností na podporu zvýšenia bezpečnosti a odolnosti na teroristické hrozby, prírodné pohromy a závislosť nebezpečenstva zo vzájomnej prepojenosti a závislosti. Zníženie rizika je výsledkom zníženia niektorej z jej troch častí, t.j. dôsledky, zraniteľnosť alebo pravdepodobnosť. Toto zníženie má za následok i následné zvýšenie odolnosti.

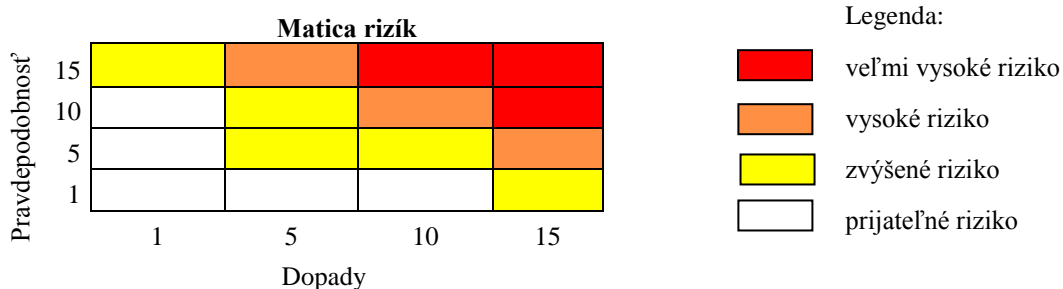
K riadeniu rizík a odolností sú nevyhnutné diskkrétne úlohy:

1. stanovenie kritérií akceptovateľnosti,
2. definícia opatrení,
3. hodnotenie opatrení,
4. akumulácia benefitov vyplývajúcich z každého opatrenia,
5. stanovenie siete benefitov a hraničných hodnôt pre každé opatrenie,
6. výber a pridelenie zdrojov pre opatrenia
7. riadenie opatrení,
8. recyklácia procesu. [5]

### 5.7.1 Stanovenie kritérií akceptovateľnosti

Firma musí rozhodnúť, aká úroveň rizika a odolnosti je pre ňu prijateľná. Rozdeliť si páry do 4 skupín:

- veľmi vysoké riziko – vyžaduje okamžité odstránenie,
- vysoké riziko – nevyžaduje akútne odstránenie, stačí v blízkej dobe,
- zvýšené riziko – vyžaduje zvýšenú pozornosť,
- prijateľné riziko – nedosahuje riziko ohrozujúce firmu.



Obr. 3. Matica rizík. [5]



### 5.7.2 Definícia opatrení

Definovať protiopatrenia na zmiernenie rizika a zvýšenia odolnosti. Z efektívneho hľadiska je vhodné zvoliť poradie riešenia rizikových párov od najvyšších. K ochranným opatreniam a protiopatreniam patria napr. bezpečnostné kontroly, riadenie vstupu a prístupu, overenie spoľahlivosti zamestnancov, CCTV, snímace a detektory, kybernetická bezpečnosť, školenia a cvičenia.

Ďalším spôsobom opatrenia je zmiernenie následkov. K najdôležitejším patrí zálohovanie dôležitých dát, včasná detekcia a upozornenie, evakuačné plány, rozvoj a poskytovanie vzájomnej pomoci a investície do záložných kapacít. [5]

### 5.7.3 Hodnotenie opatrení

Zhodnotiť každé protiopatrenie alebo zmiernovacie opatrenie z hľadiska vyhodnotenia možnosti zvýšenia odolnosti, či zníženia rizika hrozby. Hodnotiť podľa bodov 2-6. Vypočítať si čistý zisk odrátaním nákladov od výnosov a investovať do najväčších čistých výnosov. Dôkladne zhodnotiť a zvážiť, ktorý z prvkov riadenia rizík a odolnosti sa nemení a nemá ani možnosť ovplyvniť dôsledky, zraniteľnosť, pravdepodobnosť alebo nebezpečenstvo. [5]

### 5.7.4 Akumulácia benefitov vyplývajúcich z každého opatrenia

Zbieranie prínosov každej varianty páru aktíva/hrozby, ktoré redukujú riziko a zvyšujú odolnosť. Spísaním do matice, kde riadky tvoria zoznam všetkých párov usporiadaných od najväčšieho rizika a stĺpce sú možnosti vytvorenia čistého zisku daného páru. Musia sa spisovať postupne, aby vznikla v matici uhlopriečka. Každá možnosť sa ďalej preskúma vo vzťahu k ostatným dvojiciam (aktíva/hrozby). Ak existuje súvislosť medzi možnosťami (kombinácia možností dosahuje väčších výnosov ako súčet jednotlivých možností), tak musí byť taktiež napísaná. [5]

### 5.7.5 Stanovenie siete benefitov a hraničných hodnôt pre každé opatrenie

Zdroje sú vždy obmedzené, vyžaduje sa racionálny a starostlivo vytvorený spôsob finančných zdrojov pre maximálny očakávaný zisk v rámci obmedzení. Používajú sa tu dva kľúčové ukazovatele:

- čistý zisk – rozdiel nákladov od prínosov,
- pomer prínosu a ceny. [5]

Možnosti záporného čistého zisku a pomeru menšieho ako 1 nemusíme brať do úvahy. Zvyšné zoradíme od maximálnej výšky čistého zisku alebo pomeru prínosu a nákladov. Skúma neistoty v prospech odhadu nákladov. [5]

#### **5.7.6 Výber a pridelenie zdrojov pre opatrenia**

Vzhľadom k tomu, že RAMCAP Plus proces je navrhnutý pre podporu rozhodovacej právomoci vo verejnom i súkromnom sektore, sú oba pohľady samostatne uvedené. Podrobné informácie je možné získať s rozhodovacou právomocou v oboch odvetviach tým, že skúma oba ukazovatele z predchádzajúceho bodu. Vlastník rozhoduje o maximalizácii hodnoty pre akcionárov, zatiaľ čo verejný činiteľ sa viac zaujíma o maximalizáciu hodnoty pre spoločnosť. Výber je nutné zvážiť nielen podľa predchádzajúceho výberu z ukazovateľov, ale je potrebné zvážiť príslušné nešťastia, úmrtia, zranenia, finančné straty majetku vlastníka, stratenú ekonomickú aktivitu spoločnosti a dôveru verejnosti. Konečný výber nie je len zoznamom, ale konečný krok v oblasti riadenia aktív podniku a preto je potrebné dôkladne svoje rozhodnutie zvážiť. [5]

#### **5.7.7 Riadenie opatrení**

Riadiť opatrenia znamená vykonávať, monitorovať a vyhodnocovať výkonnosť vybraných možností opatrenia. Musia byť detailne naplánované a vykonávané s účinnosťou realizácie prevádzky i jej pravidelné vyhodnocovanie, v prípade nových prvkov. [5]

#### **5.7.8 Recyklácia procesu**

Dodatočné posúdenie a hodnotenie nových rizík a odolnosti by malo byť vykonávané z rôznych dôvodov. Najzávažnejšími príčinami sú zlepšovanie, nové pokroky, poznatky a zmeny. Z hľadiska toho, že RAMCAP Plus proces je relatívne lacný, je vhodné analýzu každoročne alebo aspoň raz za tri roky opakovať. [5]

V teoretickej časti som sa snažila načrtnúť problematiku ochrany a odolnosti kritickej infraštruktúry. V Amerike vznikli pokusy o vytvorenie spoločného procesu v podobe RAMCAP Plus. Keďže u nás nemáme žiadny podobný rámec, vybrala som si práve túto metódu a budem ju používať ako pomocnú metódu v praktickej časti pri vykonávaní hodnotenia odolnosti vybraného objektu kritickej infraštruktúry.

## **II. PRAKTICKÁ ČASŤ**

## 6 ZEMNÝ PLYN A JEHO ŤAŽBA

Zemný plyn je prírodná zmes plyných uhľovodíkov s prevahou metánu  $\text{CH}_4$ . Môže sa ťažiť spolu s ropou alebo uhlím. Vzniká pri rozklade organického materiálu živočíšnych alebo rastlinných zvyškov. Je uložený v pórovitých horninách ohraničených nepriepustnými vrstvami a vodou. Vrty siahajú niekoľko kilometrov pod zem (zhruba 3-8 km), na pevnine i pod morským dnom.

Prírodný zemný plyn sa podľa zloženia delí na štyri skupiny:

- zemný plyn suchý – obsahuje vysoké percento metánu a menšie množstvo vyšších uhľovodíkov (tzv. karbonský zemný plyn, ktorý vzniká pri ťažbe uhlia),
- zemný plyn vlhký – okrem metánu obsahuje väčší podiel vyšších uhľovodíkov (tzv. naftový zemný plyn, ktorý vzniká pri ťažbe ropy),
- zemný plyn kyslý – s vysokým obsahom sulfánu  $\text{H}_2\text{S}$ , ktorý sa odstraňuje,
- zemný plyn s vyšším obsahom inertov – väčší obsah oxidu uhličitého a dusíka.

Najvyužívanejším typom je druhý zmieňovaný druh naftový zemný plyn. [33, 34]

Zemný plyn je vysoko horľavý, bezfarebný, bez chuti a bez zápachu. Z bezpečnostných dôvodov sa pri jeho používaní pridáva chemikália odorant, ktorá spôsobuje charakteristický zápach, podľa ktorého je jednoznačne identifikovateľný. Pre komerčné účely sa musí nevyhnutne upravovať, pretože niektoré jeho látky by mohli negatívne pôsobiť na prepravné systémy.

Zloženie a výhrevnosť výrazne závisia od jeho pôvodu. Jeho vlastnosti sa využívajú pre rôzne účely. K najčastejším patria varenie, ohrev vody, vykurovanie, v elektrárňach, teplárňach, ako pohon motorových vozidiel v doprave i na výrobu ďalších produktov (napr. dusíkatých hnojív, plastických hmôt). [34]

Vyskytuje sa v dvoch formách:

- **CNG** (Compressed Natural Gas) – stlačený zemný plyn,
- **LNG** (Liquefied Natural Gas) – skvapalnený zemný plyn. [33]

Ťažbou plynu v SR sa zaoberá spoločnosť NAFTA, a.s. spolu s podielovým vlastníctvom SPP, a.s.. Na Slovensku sa nachádza niekoľko ložísk, avšak ich spotreba je z hľadiska porovnania s celkovou spotrebou zanedbateľná. Tvorí iba približne 2% z celku. Viac ako 95% celkovej spotreby je prevádzaný plynovodmi z ruskej spoločnosti Gazprom Export.

Slovenský plynárenský priemysel, a.s. sa skladá z dvoch dcérskych spoločností:

- **Eustream, a.s.** – prevádzkovateľ prepravnej siete,
- **SPP – distribúcia, a.s.** – prevádzkovateľ distribučnej siete.

Zemný plyn používaný spotrebiteľmi sa líši od vytiaženého z podzemia. Spracovanie je menej komplikovaný proces ako rafinácia ropy. Odstránením niektorých zložiek (etán, propán, bután, izo-bután) sa získava cenný vedľajší produkt NGL (natural gas liquids). Tie sa ďalej využívajú v ropných rafinériách, petrochemických závodoch a ako zdroj energie. Jeden z najdôležitejších procesov je separácia zemného plynu od ropy a častíc prachu, ktoré by mohli zapríčiniť poruchy kompresorových a regulačných staníc. Pred koróziou pri preprave potrubím sa predchádza pomocou odstránenia vody. Dôležitým procesom je aj odstránenie síry a oxidu uhličitého pre ich nebezpečné, či dokonca smrteľné účinky pri vdychovaní.

Tab. 7. Zloženie zemného plynu v januári 2012. [36]

Zloženie zemného plynu [mol.%]											
Mesiac	Metán	Etán	Propán	izo-Bután	n-Bután	izo-Pentán	n-Pentán	neo-Pentán	Hexán	Oxid uhličitý	Dusík
1/2012	96,597	1,621	0,49	0,071	0,079	0,017	0,013	0	0,017	0,255	0,839

Fyzikálno-chemické vlastnosti uvedené v Tabuľke 8. sa nemerajú priamo, ale stanovujú sa pravidelne každý mesiac výpočtom podľa chemického zloženia a v súlade s technickou normou ISO 6976: Natural gas – Calculation of calorific values, density, relative density and Wobbe index from composition (Zemný plyn – Výpočet tepelných hodnôt, hustoty, relatívnej hustoty a Wobbeho indexu zo zloženia). Výpočtami je kontrolovaná kvalita zemného plynu na vstupe do plynárenskej sústavy.

Tab. 8. Parametre zemného plynu. [36]

Mesiac	Relatívna hustota	Hustota (kg.m <sup>-3</sup> )	Výhrevnosť (kWh.m <sup>-3</sup> )	Spaľovacie teplo (kWh.m <sup>-3</sup> )	Wobbeho číslo zo sp. tepla (kWh.m <sup>-3</sup> )	Obsah celkovej síry (mg.m <sup>-3</sup> )	Emisný faktor CO <sub>2</sub> (tCO <sub>2</sub> /TJ)
1/2012	0,5766	0,7066	0,585	10,627	13,99	0,07	55,43

Hoci energetický mix z uhlia, ropy, zemného plynu, jadrovej energie a alternatívnych zdrojov je na Slovensku celkom vyvážený, môžeme povedať, že dominantnú energetickú surovinu tvorí zemný plyn (necelých 30%).

Spaľovaním plynu nevznikajú žiadne zdraviu škodlivé splodiny a oproti ostatným fosílnym palivám produkuje oveľa menej škodlivín, takže nepoškodzuje životné prostredie. [36]

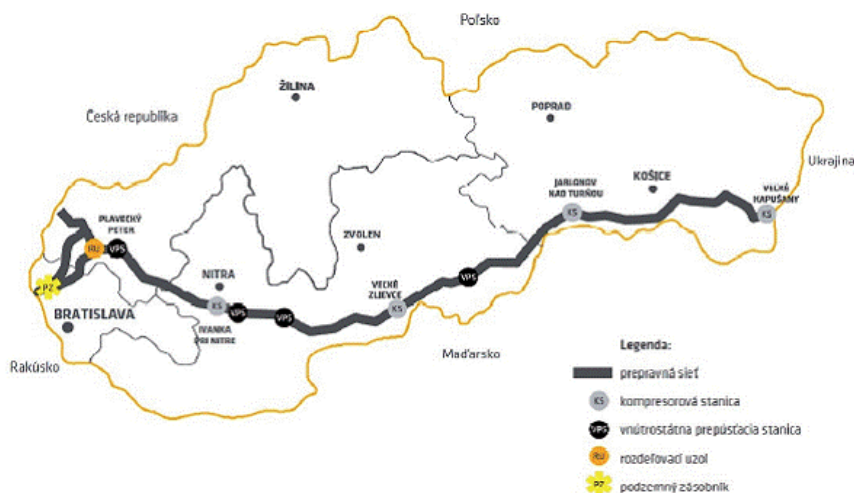
## 6.1 Preprava zemného plynu

Väčšina krajín EÚ je v súčasnosti závislá na dovoze zemného plynu. K jedným z najväčších prepravcov zemného plynu v rámci Európskej únie patrí Eustream, a.s.. Uskutočňuje medzinárodnú prepravu plynu z Ruska pre odberateľov v zahraničí (nielen pre členov EÚ) i pre potreby slovenského trhu. V SR je zatiaľ monopolným podnikom, narozdiel od susedných krajín (napr. Českej republiky). Po krátkodobých ale opakovaných problémoch vedenia plynovodu cez Ukrajinu sa začalo uvažovať o nákupe nórskeho plynu. Zatiaľ je pre obmedzenia dodávky technicky možný reverzný tok z existujúceho spojenia s Českou republikou. Rokovania prebehli aj s inými spoločnosťami, no zatiaľ v tomto procese nemá spoločnosť konkurenciu z dôvodu vysokých finančných nákladov pre nové budovanie.

Preprava zemného plynu je uskutočňovaná dvomi spôsobmi:

- plynovodmi,
- tankermi vo forme skvapalneného plynu.

Dĺžka prepravnej siete Eustream dosahuje zhruba 2270 km s obsahom kapacity 90 miliárd m<sup>3</sup> plynu za rok. Firma má na starosti okrem prevádzky i údržbu kompresorových staníc, ktoré sú znázornené na obrázku (viz. Obr. 4). Vstupným bodom do prepravnej siete sú Veľké Kapušany, ktoré sú blízko hraníc s Ukrajinou. [35, 36, 38]



Obr. 4. Prepravná sieť eustream na SR. [45, 47]

## 6.2 Distribúcia

Posledným krokom poskytovania zemného plynu zákazníkom je distribúcia. Vyššie zmieňovaná preprava prevádza zemný plyn cez územie Slovenska do ďalších európskych krajín. K distribuovaniu ku konkrétnym zákazníkom slúžia iné spoločnosti. Oproti preprave má distribúcia značnú konkurenciu. Hoci všetky firmy majú rovnaký prístup k sieti, najväčšou ešte stále aj po 155 rokoch zostáva SPP – distribúcia, a.s.. Distribúcia zabezpečuje:

- spoľahlivú distribúciu zemného plynu od prepravných sietí až k zákazníkom,
- pripojenie k distribučnej sieti,
- obchodovanie so sieťovými kapacitami,
- údržbu distribučnej siete,
- spracovanie odpočtov spotreby zemného plynu.

Z celkového počtu obcí na Slovensku je plynofikovaných zhruba 77%, vďaka čomu patríme k najviac plynofikovaným krajinám v Európe. Kým väčšie priemyselné podniky môžu mať dohodu priamo s prepravnou sieťou, ostatný podliehajú pod miestne plynárenské distribučné spoločnosti. Firma SPP – distribúcia, a.s. pokrýva 98% zákazníkov s dĺžkou plynovodov 32 500 km. Distribúcia presúva menšie objemy plynu pri oveľa nižších tlakoch na kratšie vzdialenosti do veľkého počtu jednotlivých užívateľov k čomu využíva oveľa menší priemer potrubia i menšie kompresorové stanice na stláčanie plynu. Využívajú sa vysokotlakové, strednotlakové i nízkotlakové plynovody podľa potreby. Tradične sa využívajú pevné oceľové trubky avšak nové technológie umožňujú znížiť náklady a zjednodušiť opravy výmenou za pružné plastové trubky.

Každá spoločnosť musí dodržiavať rovnaké bezpečnostné opatrenia v súlade s požiadavkami legislatívy a internými predpismi:

- sledovať systémami tesnosť potrubia,
- pravidelne uskutočňovať odborné preventívne prehliadky,
- vzdelávať v oblasti bezpečnosti,
- poskytovať 24 hodinovú poruchovú službu,
- poskytovať havarijnú pripravenosť,
- poskytovať zákaznícku službu.

Monitorovanie a prenos údajov do centrálného dispečingu zabezpečujú riadiace systémy SCADA, ktorými sú regulačné a prepúšťacie stanice vybavené. [36, 37, 39]

### 6.3 Skladovanie

Z dôvodu nestabilného záujmu zákazníkov počas roka v závislosti od striedania ročných období je nevyhnutné uskladňovanie plynu v podzemných zásobníkoch. V zimnom období by sa nestíhalo odoberať potrebné množstvo k danej spotrebe kvôli nemožnosti zvýšenia rýchlosti prúdenia zemného plynu a preto sa plyn odoberá celoročne v približne rovnakom množstve a pre navýšenie spotreby sa skladuje vo vopred určených miestach. Výhodné sú vytŕažené plynové a ropné ložiská. Možno povedať, že hlavnou úlohou zásobníkov je vyplniť medzeru medzi dodávkami zemného plynu a jeho skutočnou spotrebou alebo zabezpečiť plynulú prevádzku v prípadoch mimoriadnych udalostí, ktoré kvôli nezhodám Ruska z Ukrajinou nie sú ojedinelé.

Uskladňovaním zemného plynu sa na Slovensku zaoberajú dve firmy, ktorých vlastníkom je i SPP, a.s.:

- NAFTA a.s.,
- POZAGAS a.s..

Obe spoločnosti sú napojené rovnako na domácu prepravnú, tak i na distribučnú sieť. Pre možnosť krátkodobého uskladnenia sú k dispozícii i zásobníky v Českej republike v obci Dolné Bojanovice i iných miest v oblasti hraníc ČR a Rakúska. Vhodných lokalít nie je veľa, pretože sú potrebné na uskladnenie vysoké investície a predovšetkým špecifické geologické podmienky. Celková kapacita, ktorú sú zásobníky schopné dohromady obsiahnuť je 2,75 mld. m<sup>3</sup>, čo je takmer polovica ročnej spotreby. Jednu z najväčších úrovní v rámci EÚ a priblížením sa 50 % chcú dosiahnuť budúcoročnou výstavbou nového zásobníka v Gajary-Báden. Pre porovnanie uvediem, že v ČR, Rakúsku a v Maďarsku tvoria zásobníky iba okolo 30 % spotreby.

Investície do nových zásobníkov alebo nových sietí plynovodov je v dnešnej dobe treba zhodnotiť najmä z toho hľadiska, že zemný plyn patrí k vyčerpatelným zdrojom. Pri doterajšej spotrebe sa odhadujú zásoby na necelých 70 rokov. Preto z môjho pohľadu je výhodnejšou možnosťou udržať doterajší chod na čo najlepšej úrovni. Zostáva otázkou, či obrovské náklady vložené do nových sietí sa za túto dobu môže navrátiť. Reálnou možnosťou ostáva prenajímanie stávajúcich potrubí. [35, 36]



## 7 POPIS VYBRANÉHO PRVKU KI

V tejto časti sa budem venovať multikriteriálnemu hodnoteniu odolnosti na vybranom objekte KI. Objekt tvorí centrálny dispečing prepravnej spoločnosti Eustream. Z dôvodu utajovania informácií podľa zákonov č. 45/2011 Z. z., o kritickej infraštruktúre a č. 215/2004 Z. z., o ochrane utajovaných skutočností použijem fiktívnu časť objektu na reálnom území objektu firmy Eustream, a.s..

Základnou úlohou spoločnosti je preprava zemného plynu na Slovensko, cez územie Slovenska a na európske trhy. Toto poslanie plní úspešne od roku 1972 dodnes. Za toto obdobie prepravilo viac ako 2 miliardy m<sup>3</sup> zemného plynu. Firma prešla pribúdajúcim časom rôznymi názvami a pod terajším funguje už štvrtý rok. Historický vývoj:

- 1972 – Tranzitný plynovod, k.p., Praha,
- 1993 – divízia Slovtransgaz, Slovenský plynárenský priemysel, a.s.,
- 2003 – divízia Tranzit, Slovenský plynárenský priemysel, a.s.,
- 2006 – SPP – preprava, a.s.,
- 2008 – Eustream, a.s.. [46]

Firma Eustream sa skladá z niekoľkých oblastí:

- obchod,
- financie a ľudské zdroje,
- informačné a komunikačné technológie,
- korporátne záležitosti,
- manažérstvo rizík a interného auditu,
- riadenie aktív,
- prevádzka a údržba,
  - centralizovaná údržba,
    - údržba a opravy kompresorov,
    - údržba a opravy potrubí,
    - zváranie,
    - TDW a špeciálne služby,
- dispečing.

**Centrálly dispečing** prepravnej plynárenskej spoločnosti spadá pod oblasť prevádzky a údržby firmy Eustream. Má na starosti riadenie a monitorovanie celého prepravného systému plynu na území Slovenskej republiky. Zamestnáva zhruba 80 pracovníkov, ktorí podľa výkonu svojej práce sú zoradení do daných oblastí prevádzky:

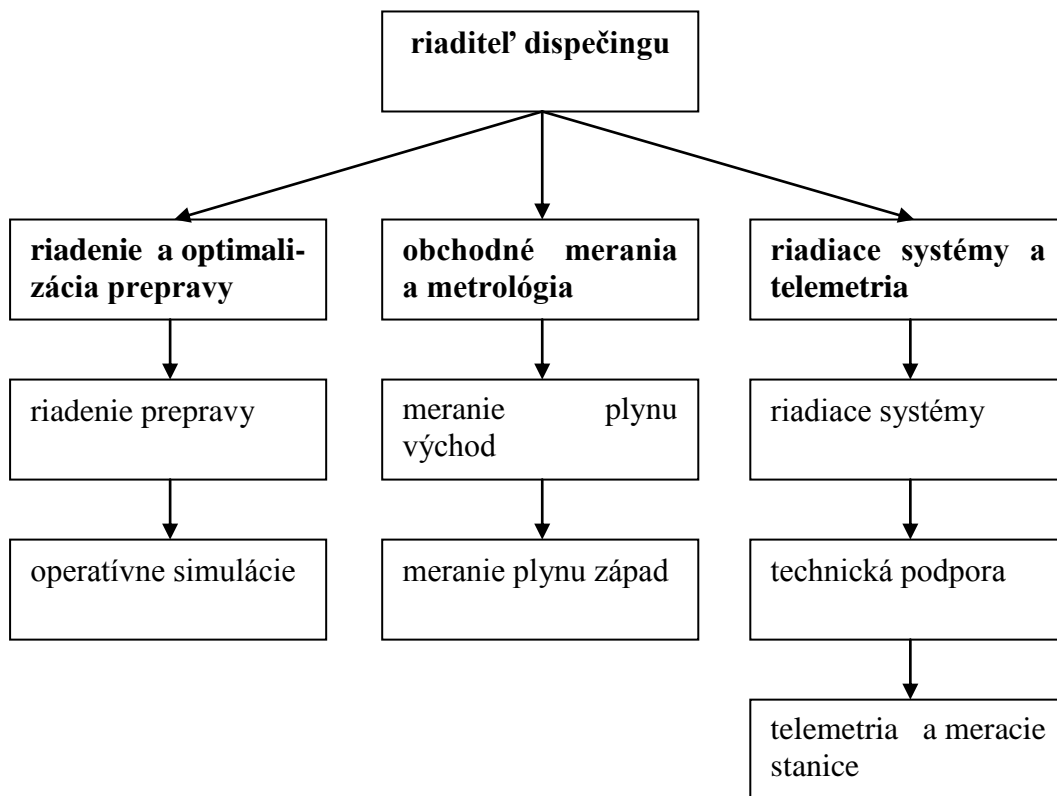
- riadenie a optimalizácia prepravy,
- obchodné merania a metrológia
- riadiace systémy a telemetria.

V prvom rade je potrebné určiť, či objekt naozaj spĺňa podmienky prvku kritickej infraštruktúry. Keďže nový schválený dokument Návrh sektorových a prierezových kritérií na určenie prvkov kritickej infraštruktúry, ktorý napomáha pri určovaní prvkov KI, je utajovaný, vychádzam z predpokladu, že dispečing spĺňa sektorové i prierezové kritéria z hľadiska výkonu jeho práce. Centrálly dispečing zaradíme do podsektoru plynu v sektore energetika, ktoré sú uvedené v prílohe zákona č. 45/2011.



Obr. 5. Mapa prepravnej siete plynu.

## Centrálňy dispečing



Obr. 6. Organizačná štruktúra.

- Riaditeľ dispečingu** riadi a zodpovedá za jednotlivé oblasti dispečingu. Stanovuje ciele pre útvary sekcie a kontroluje ich plnenie. Schvaľuje a vypracováva Plán pohotových výkonov, Plán odstávok zariadenia TS, interné predpisy pre potreby sekcie a uskutočňuje vyhlásenie havarijných stavov TS v ním riadenej oblasti.
- Riadenie a optimalizácia prepravy** ako je z názvu jasné riadi a monitoruje prepravu plynu cez územie Slovenskej republiky pomocou simulačných a optimalizačných programov.
- Odborní pracovníci **obchodného merania a metrológie** pomocou meracích metód kontrolujú množstvo a kvalitu plynu na systémových vstupoch a výstupoch. Zaznamenávajú tieto hodnoty a porovnávajú s normatívnymi hodnotami. Výsledky matematických výpočtov implementujú do riadenia prevádzky.
- Riadiace systémy a telemetria** má na starosti ovládanie systémových prvkov kompresorových staníc, rozdeľovacích uzlov a plynovodu.

Zamestnanci centra zaistujú nepretržitý tok zemného plynu 24 hodín denne každý deň v roku. Aktuálne a presné informácie o jednotlivých častiach siete zemného plynu v potrubí získavajú prostredníctvom počítačového systému SCADA. Tento systém poskytuje prevádzkovateľovi dohľad o stave plynovodu, ovládanie prietokov plynu a diaľkové ovládanie kompresorových staníc v sieti.

Dispečeri v centre vykonávajú viacero úloh:

- hlavnou úlohou je zabezpečiť spoľahlivú a bezpečnú prepravu plynu v požadovanom objeme a čase,
- dohliada na prietok, tlak a teplotu plynu - monitoruje a riadi tok zemného plynu v celej distribučnej sústave potrubia diaľkovo a ovláda prietok plynu,
- uskutočňujú dôležité merania kontrolných stanovísk a kompresorových staníc,
- pomocou zobrazenia dát optimalizujú prevádzku plynárenskej sústavy (možnosť zastavenia v prípade vzniku mimoriadnych udalostí),
- vykonávajú záznam, analýzu a archiváciu dát,
- spolupracujú s ostatnými dispečerskými centrami,
- neustále koordinujú prietok s centrami expedície do Rakúskej a Českej republiky,
- kontaktujú užívateľov o vhodných informáciách na oddelení mimoriadnych udalostí v sieti plynovodu.

Riadenie 2270 kilometrovej tranzitnej sústavy plynovodu poháňanej štyrmi kompresorovými stanicami sa uskutočňuje pomocou softvérovej aplikácie Amadeus Marti Studio. Priemer potrubia je 1200 a 1400 mm s výkonom okolo 250 MW. Keďže každoročná preprava tvorí zhruba 90 miliárd m<sup>3</sup> je zrejmé, že potrubím preteká obrovské množstvo plynu. Prúdenie plynu sa riadi Navierovými-Stokesovými rovnicami, ktoré patria do kategórie najväčších problémoch matematiky riešených najväčšími odborníkmi sveta. Za ich vyriešenie je dokonca písaná vysoká odmena v podobe 1 milióna dolárov. Dispečingu pomáhajú i ďalšie optimalizačné a simulačné programy.

Na riadenie systému je potrebné umiestnenie telemetrického prvku na každý aktívny článok, aby sa dali diaľkovo ovládať prenášaním cez optické káble až do dispečerského centra.

Dispečing začína svoju každodennú pracovnú činnosť vždy od 8:00 hod. a končí nasledovný deň o tom istom čase a opakuje svoj kolobeh každý deň v roku.

Dispečerské centrum je rozdelené na:

- **Komerčný dispečing**, ktorý má za úlohu riešenie administratívnych obchodných vzťahov s užívateľmi prepravnej siete tým, že zbiera požiadavky na prepravu od jednotlivých zákazníkov, kontroluje ich s podpísanými zmluvami a dohodami a v prípade, aj je všetko v poriadku potvrdí pripravenosť objednávky a presunie k prevádzkovému dispečingu.
- **Prevádzkový dispečing** uskutočňuje fyzické riadenie prepravnej siete, teda nastavuje zariadenie ku konkrétnemu priebehu prepravy v zmysle zmluvných podmienok. [46]

Prepravný systém je čiastočne automatizovaný, pretože na starších strojoch 6MW je riadenie uskutočňované na mieste ručne obsluhou. Dispečing musí aktívne komunikovať s pracovníkmi:

- kompresorových staníc ,
- hraničných preberacích staníc (Baumgarten, Lanžhot),
- rozdeľovacieho uzla (Plavecký Peter),
- v prípade opráv i s pracovníkmi, ktorí majú opravu na starosti,
- prevádzkovateľmi zásobníkov plynu,
- dispečingu SPP.

Dispečing má za úlohu i plánovacie činnosti, čo sa prejavuje vytvorením plánu na obdobie od apríla do októbra daného roka, kedy dochádza k odstaveniu zariadení zákazníkov. Tieto plány sa stávajú záväznými po odobrení na konferencii zástupcov dispečingov v Moskve.

Vypracované plány sú v oblasti:

- plán prepravovaného množstva,
- plán spotreby energií na pohon kompresorov,
- plán prevádzkových hodín,
- plán odstávok,
- plán pohotových výkonov.

Dispečing sa snaží udržať rovnováhu medzi požiadavkami obchodníkov a údržbou, kde obchodníci vidia len ideu nepretržitej prevádzky a naopak údržby, ktorá chce čo najviac času pre svoje aktivity v snahe spoľahlivejšieho chodu zariadenia.

## 7.1 Charakterizácia objektu a aktív

Areál fiktívneho dispečingu spoločnosti Eustream, a.s. je umiestnený na Železničnej ulici v Senici v západnej časti Slovenska. V blízkosti areálu sa nachádza železničná stanica, parkovisko autobusov Slovenskej autobusovej dopravy SAD Trnava, niekoľko rodinných domov a čistička odpadových vôd. Územie je ohraničené pletivom vo výške dvoch metrov, nad ktorým sú umiestnené tri kusy ostnatého drôtu. Objekt má jednu oceľovú vstupnú bránu pre nákladnú i osobnú dopravu elektronicky ovládanú vrátnikom, ktorá slúži i ako vchod pre zamestnancov.

Vrátnik zastáva funkciu fyzickej ochrany, ktorá je nepretržitá. Pri výkone práce musí mať oblečenú rovnošatu označenú znakom, aby bolo zrejmé, že ide o bezpečnostnú službu. Jeho výkon je spojený s držaním, nosením a používaním vecných bezpečnostných prostriedkov (zbrane). Plní úlohy, ktoré vyplývajú zo zákona 473/2005 Z.z. o poskytovaní služieb v oblasti súkromnej bezpečnosti (zákon o súkromnej bezpečnosti). Zo svojho preskleného pracoviska na kraji budovy má priamy výhľad na vstupnú bránu, dozerá na správne dodržiavanie režimových a organizačných opatrení a vykonáva strážnu službu. Práca fyzickej ochrany spočíva v:

- zákaze vstupu nepovolaným osobám do chráneného objektu,
- pozornom prezretí osoby vstupujúcej do objektu, či nemá pri sebe zbraň alebo iné predmety, ktorými by mohol spáchať protiprávnu činnosť a v prípade zistenia predmet odobrať alebo zakázať vstup,
- vyžadovaní preukázania sa osôb identifikačnou kartou,
- kontrole všetkých osôb, ktoré sa nachádzajú v dopravnom prostriedku,
- zadržaní páchateľa bezprostredne po spáchaní trestného činu na čas nevyhnutný do príchodu policajného príslušníka.

Objekt je monitorovaný kamerovým systémom, na ktorý vrátnik dozerá. Rozloženie ôsmych kamier mimo budovy stačí na monitorovanie každého miesta chráneného objektu. Záznamy sú uchovávané v záznamovom zariadení 72 hodín. Po 16:00 hodine, keď odíde väčšina zamestnancov, zamkne bránu a pustí vycvičeného strážneho psa. Každý zamestnanec, ktorý po tomto časovom intervale príde do budovy alebo z nej vyjde, musí čakať na vrátnika, než zamkne psa do kletky a odomkne bránu. Pohyblivú pracovnú dobu majú pracovníci od 6:00 hod., kedy vrátnik zamkne psov a odomkne bránu, aby nemusel každého zamestnanca zvlášť púšťať.

Vrátník má informácie o počte zamestnancov v budove vďaka ACCESS systému. Každá návšteva je po predložení občianskeho preukazu označená kartou. Komplex je využitý i ako parkovisko. V budove sú okrem dispečingu umiestnenom na 3 poschodí i kancelárie vedúcich pracovníkov rôznych oddelení v nižších podlažiach. Na prízemí sa nachádza metrologia, centralizovaná údržba a oprava potrubí a kompresorov. Na prvom poschodí sa nachádza oddelenie defektoskopie, ekonomická asistencia a TDW špeciálne služby. Sklady a potrebné prostriedky a nástroje sú umiestnené v neďalekej budove zhruba 500 metrov od budovy dispečingu.

Ochrana budovy spadá pod kritické aktíva firmy. Okrem systému CCTV objekt chráni a pasívne a aktívne detektory, ktoré sú napojené na centrálnu ústredňu. V budove nechýbajú ani požiarné snímáče.

Podobne ako budovu chráni spomínané bezpečnostné prvky i zamestnancov z ohľadom na ich život a zdravie. Ďalším kritériom však zostáva ochrana ich osobných údajov vyplývajúca zo zákona č. 428/2002 Z.z. o ochrane osobných údajov. Keďže dispečing spadá pod ochranu utajovaných skutočností, podľa zákona 215/2004 Z. z. o ochrane utajovaných skutočností, musia využívať vo svojom informačnom a komunikačnom systéme kryptografické prvky pre daný stupeň zabezpečenia. Firma Eustream má rovnako ako všetky ostatné firmy vybudovanú bezpečnostnú politiku informačného systému, kde sa zameriava na tri hlavné oblasti:

- **diskrétnosť** – k údajom a dátam sa nesmú dostať nepovolane osoby,
- **integrita** – údaje a dáta nesmú byť neoprávneným spôsobom modifikované, poškodené alebo zmazané,
- **dostupnosť** – údaje a dáta musia byť dostupné zamestnancom v rámci ich výkonu práce.

V rámci bezpečného užívania informačného systému dodržiavajú zamestnanci zásady bezpečného užívania:

- používať len legálne zakúpený softvér,
- pravidelne softvér aktualizovať,
- inštalovať kvalitný licencovaný antivírusový softvér a pravidelne ho aktualizovať, aby bol odolný voči najnovším druhom vírusov,
- vhodné je využívať i anti-spaware programy a osobné firewaly,

- zakázat přístup na vybrané webové stránky (Skype, facebook, ICQ), nielen z dôvodov spomalenia práce počítača i zamestnanca, ale najmä ohľadom bezpečnosti, pretože tieto stránky sú najviac postihnuté počítačovými vírusmi,
- každý zamestnanec môže do počítača alebo intranetu vstúpiť len pod svojím prihlasovacím menom a heslom,
- heslo musí byť dostatočne dlhé, striedať malé i veľké písmená, dokonca i číslice a interpunkčné znamienka, (min 8 znakov) a nemalo by v žiadnom prípade obsahovať slová a taktiež by pracovník nemal používať toto heslo k prihlasovaniu na iné stránky,
- heslo musí užívateľ každých 10 dní meniť,
- pri akejkoľvek poruche treba okamžite informovať IT zamestnanca, ktorý ak ide o menej závažnú poruchu, dokáže ju spraviť zo svojho počítača, v opačnom prípade musí ísť na miesto vzniku poruchy,
- informovať a pravidelne školiť zamestnancov.

O informačný systém vo firme Eustream sa stará špecifický tím IT pracovníkov v Bratislave, ktorí sú pravidelne školení a preverovaní. V dispečingu v Senici sú iba dvaja IT zamestnanci, a v prípade, že nedokážu chybu opraviť, povolajú posily z Bratislavy, prípadne i odbornú firmu.

Firma využíva najmodernejšie technológie, softvéry a produkty k výkonu práce, čo zvyšuje bezpečnosť a odolnosť voči nežiaducim vplyvom.

V zhrnutí pod kritickými aktívami dispečingu chápeme:

- zamestnancov – na prvom mieste predovšetkým ich život, zdravie a ochranu osobných údajov,
- budovu – pred napadnutím a zničením,
- celkovú prevádzku komerčného dispečingu,
- celkovú prevádzku prepravného dispečingu,
- know-how,
- informačný systém (HW, SW),
- komunikačný systém (komunikačné siete, Internet, Intranet, GSM),
- databázový systém,
- počítače,
- ostatné prístroje a zariadenia, ktoré sú potrebné k uskutočňovaniu prevádzky.



## 7.2 Charakterizácia hrozby

Po identifikácii aktív, je nevyhnutné charakterizovať i možné hrozby, ktoré môžu v dispečingu nastať (viz Tab. 9). Podľa charakteru hrozby ich delíme na tri skupiny.

Tab. 9. Vymedzenie hrozieb dispečingu.

Teroristické hrozby	Prírodné hrozby	Hrozby zo závislosti a prepojenosti
násilné alebo neoprávnené vniknutie cudzej osoby	požiar	prerušenie dodávky elektriny
bombové útoky, použitie zbraní	prívalový dážď	prevádzková porucha
deštrukcia priestoru alebo jeho časti		chybná manipulácia s prvkami
zničenie alebo vyradenie dispečerského pracoviska		nedodržanie pracovných postupov

### 7.2.1 Teroristické hrozby

Ohrozenie teroristickými, bombovými a kybernetickými útokmi sa nedá nijakým spôsobom dopredu predvídať, preto ich zaradujem na prvé miesto. Ich dôsledky môžu spôsobiť značné straty na životoch ale i obrovské hospodárske škody, ktoré môžu mať až zničujúci dopad pre firmu. K najväčším hrozbám patrí **zničenie alebo vyradenie dispečerského pracoviska, deštrukcia priestoru alebo jej časti**. Vznikajú ťažko nahraditeľné ujmy na majetku. Pri ohrození **bombových, chemických, biologických alebo radiačných zbraní** sa berie ohľad najskôr na život a zdravie zamestnancov a ľudí, ktorí by sa mohli stať obeťami pred hodnotou majetku. Ľudský život je narozdiel od iných hmotných a nehmotných aktív nenahraditeľný.

Pod tieto hrozby spadajú aj vyhrážky o umiestnení bomby v objekte, ktoré sa musia prešetriť evakuáciou budovy, čo môže spôsobiť škody nedodania potrebného objemu. Vyhrážky môžu ale i odviezť pozornosť od sledovania dôležitých staníc pre vytvorenie väčšej škody. K nemenej podstatným patrí i **násilné vniknutie cudzej osoby do priestoru**, zničenie bezpečnostných prvkov priestoru a úmyselné poškodenie bezpečnostných prvkov.

Pre zničenie firmy postačí i na prvý pohľad nenásilný avšak neoprávnený prístup cudzej osoby do priestoru podniku, k prvkom technického systému fyzickej ochrany a k získaniu informácií o ochrane priestoru.

### 7.2.2 Prírodné hrozby

Z hľadiska geografického polozenia objektu nehrozia žiadne veterné smršte v podobe tornád a tajfúnov. Zo štatistických údajov sa v danej lokalite nevyskytujú ani silné zemetrasenia, ktoré by mali vplyv na prevádzku dispečingu. Keďže rieka Teplica vyvierajúca z Kunovskej priehrady, ktorá preteká cez mesto Senica je od objektu vzdialená 3 km a hoci niekoľkokrát vyliala svoje koryto a ohrozila veľkú časť mesta i vyvretím spod zemných kanálov, objekt dispečingu nikdy nezasiahla a preto ju nemusíme počítať do daných hrozieb. Problémy záplav však môžu nastať silným **prívalovým dažďom**, kedy kanálové systémy nestíhajú dostatočne splavovať množstvo vody. Hrozbou zaplavenia hrozí i susediaci objekt čističky odpadových vôd, ktorý je vzdialený len 300 metrov. Povodňou sú viac ohrozené kancelárie umiestnené v spodnej časti budovy. Dispečing sa nachádza na 3 poschodí a preto väčšie riziko spôsobí silný dážď, ktorý ľahko zničí rovnú plechovú strechu. Rovnako veľkým ohrozením pre objekt môžu byť vzniknuté **požiare**.

### 7.2.3 Hrozby zo závislosti a prepojenosti

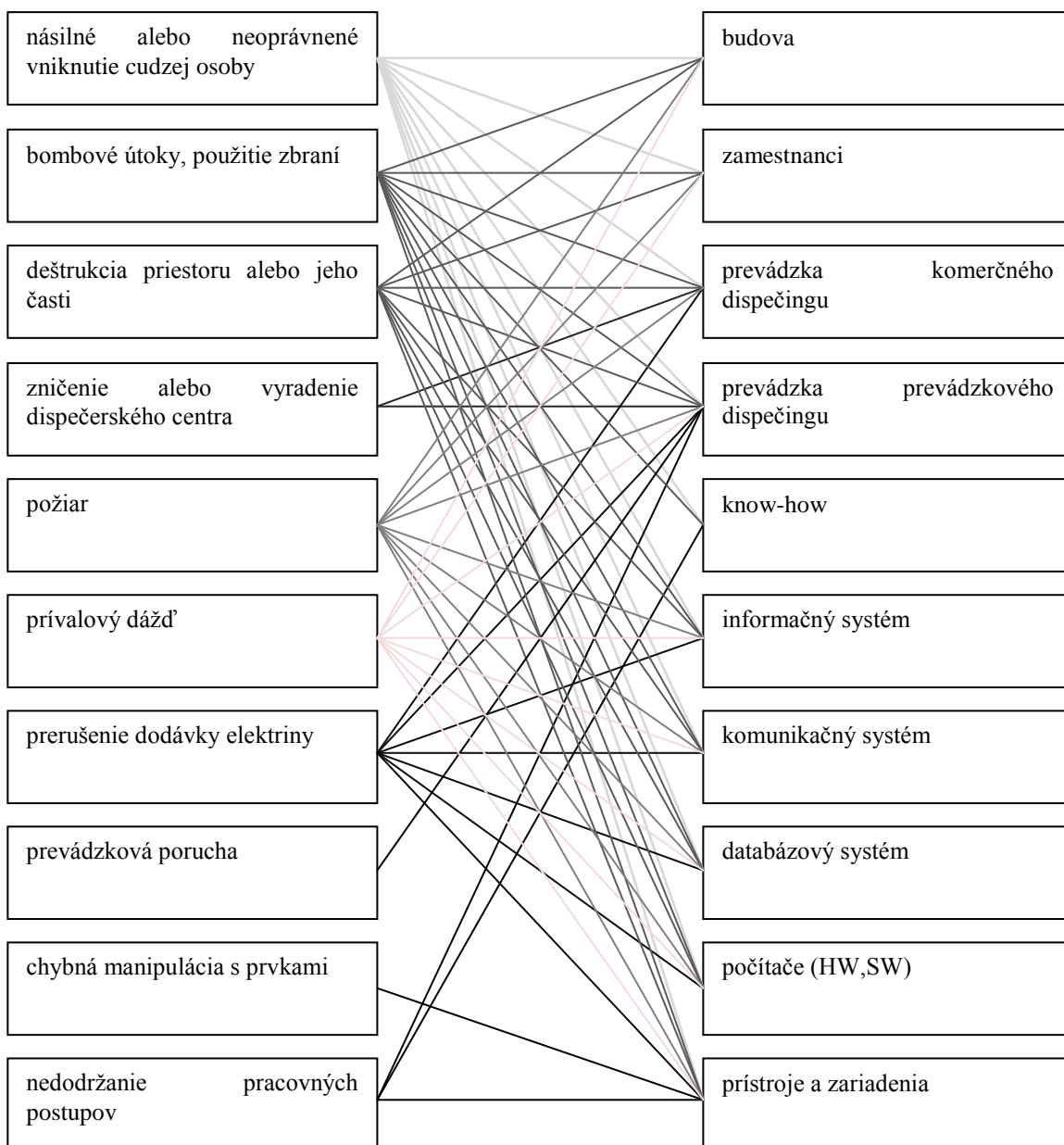
Všetky informačné, komunikačné, databázové i iné systémy sú závislé od dodávky elektrickej energie. **Prerušenie dodávky elektriny** je častým ale nepríjemným javom. Každý objekt kritickej infraštruktúry musí mať záložný zdroj energie, ktorý nahradí okamžite mimoriadny stav prerušenia elektriny bez akýchkoľvek nechcených efektov 60 hodín. Systémy riadenia dispečingu sú závislé nielen od energie ale i od komunikačných sietí (internetu), kedy pri výpadku nie je možné uskutočňovať plynulú prevádzku. Komunikáciu tvorí kombinácia dvoch technológií od mobilného operátora bezdrôtovo a drôtovo - cez optický kábel. Každá firma je závislá od ľudských zdrojov kedy nedostatok, zlyhanie alebo chyby zamestnancov môžu spôsobiť značné problémy. Jedná sa o **chybnú manipuláciu, prevádzkovú chybu alebo nedodržanie striktné daných pracovných postupov**. Zamestnanci musia byť riadne zaškolení a pravidelne preverovaní pracovníci, čím je riziko vymenovaných problémov značne znížené.

Skupiny hrozieb v oblasti výroby, prenosu a distribúcie energetiky delíme na prírodné hrozby, technické zlyhanie a technické zlyhanie systémov fyzickej ochrany.

Skupiny hrozieb z hľadiska fyzickej bezpečnosti (ľudského faktoru) delíme na organizačné zlyhanie, ohrozenie fyzickej povahy a terorizmus.

### 7.3 Analýza dopadov

V tejto časti je dôležité logicky odvodiť všetky možné dopady, ktoré môžu vybrané hrozby spôsobiť daným aktívam (viz Obr. 6). Z Obrázku je zrejmé, že previazanosť hrozieb a aktív je nespočetne veľká. Nie všetky však majú rovnakú váhu z hľadiska následných dôsledkov.



Obr. 7. Analýza dopadov.

Firma Eustream prepraví za rok niekoľko miliárd m<sup>3</sup> plynu. Minulý rok to bolo približne 90 miliárd m<sup>3</sup> plynu. Ročná domáca spotreba tvorí 16% z tohto celku. V roku 2011 prešlo cez Slovensko do Česka a Rakúska dohromady 74 miliárd m<sup>3</sup> plynu, čím docielili zisk z predaja služieb v podobe 229 miliónov €. Podľa týchto údajov si zostavím pomocnú tabuľku pre výpočet ekonomických dopadov na firmu.

Tab. 10. Výpočet ekonomickej degradácie.

degradácia	m <sup>3</sup>	Eur	hodnota	hodnotenie
100%	74 000 000 000	229 276 000	5	veľmi vysoká
80%	59 200 000 000	183 420 800	4	vysoká
60%	44 400 000 000	137 565 600	3	stredná
40%	29 600 000 000	91 710 400	2	málo významná
20%	14 800 000 000	45 855 200	1	nízka
0%	0	0	0	žiadna

#### Príklad výpočtu:

Firma ročne prepraví 74 miliárd m<sup>3</sup> plynu podľa zmluvného kontraktu, ktorý podpísali s ruskou firmou Gazprom. Výnosy z predaja svojich služieb za minulý rok tvoril 802,386 miliónov €, z čoho celkové prevádzkové náklady tvorili 573,110 miliónov €. Zisk teda zodpovedá sume 229,276 miliónov €.

Preprava 1m<sup>3</sup> plynu stojí 1 cent:

$$Cena_{1m^3} = \frac{\text{Výnosy}}{\text{Počet plynu}} = \frac{802\,386\,000}{74\,000\,000\,000} = 0,0108 \text{ €}. \quad (8)$$

Uvažujem o prípade, keď dispečing diagnostikuje poruchu jedného plynového potrubia a guľového uzáveru. Porucha je detekovaná únikom plynu, čo spôsobila prasklina na potrubnom systéme a nefunkčnosť guľového uzáveru. Hoci plyn sa prevádza štyrmi rúrami (v niektorých častiach i piatimi), pri takto závažnej poruche musia uzavrieť trasový uzáver, aby plyn ďalej nepretiekal žiadnym potrubím. Trasové uzávěry sú z týchto dôvodov umiestnené každých 30 km. Oprava trvá niekoľko dní než príde k plynulej prevádzke.

Za 1 deň prepraví firma 200 miliónov m<sup>3</sup> plynu:

$$\frac{74\,000\,000\,000}{365} = 202\,739\,726 \text{ m}^3. \quad (9)$$

V prípade, že oprava trvá 20 dní, tak ide o 4 miliardy m<sup>3</sup> plynu:

$$202\,739\,726 \times 20 = 4\,054\,794\,521 \text{ m}^3. \quad (10)$$

To značí v prepočte necelých 44 miliňov €:

$$4\,054\,794\,521 \times 0,0108 = 43\,966\,356 \text{ €}. \quad (11)$$

Táto suma zodpovedá celkovej strate spôsobenej z nevykonávania činnosti prepravy plynu. Suma však ešte nie je kompletná. V prvom rade je dôležité započítať i výkopové práce. Po uzavretí trasového uzáveru je nutné odčerpanie plynu v potrubí cca do 10 atmosfér (1MPa). Všetok plyn nie je možné odčerpať, preto zvyšný plyn sa musí vypustiť do ovzdušia. Z dôvodu poruchy guľového uzáveru GU DN 1400 mm, musí byť prvok vymenený (viz. Obr. 7). K ďalším hodnotným prácam patrí vyrezanie GU, navarenie a výmena chybného potrubia. Práce v teréne sú ukončené následnou kontrolou, zaizolovaním a zasypaním GU.



*Obr. 8. Výmena potrubia a guľového uzáveru*

Súčet vymenovaných a ďalších nevyhnutných súvisiacich prác spolu s cenou GU DN 1400 mm a iných potrebných nových prvkov, ktoré museli byť počas práce vymenené tvorí zhruba okolo 2 miliónov €.

Počas nedodania plynu do Česka a Rakúska nastávajú firme i ďalšie straty v podobe sankcie 500 000 €.

Celková suma vybranej prevádzkovej poruchy je zhruba 46,5 miliónov € :

$$43\,966\,356 + 2\,000\,000 + 500\,000 = 46\,466\,356 \text{ €}. \quad (12)$$

Podľa Tabuľky 10. ide v prípade prevádzkovej poruchy o 20% degradáciu zisku, čo tvorí nízku hodnotu degradácie.

Podobným spôsobom som ohodnotila degradáciu u pôsobenia každej hrozby. Po analýze ekonomických strát pre firmu z hľadiska hrozieb som zostavila tabuľku (viz Tab. 11), ktorá zhruba zodpovedá percentuálnym finančným dopadom konkrétnej hrozby na aktívum. Výpočty sú zohľadnené z viacerých faktorov, podobne ako tomu bolo v príklade. Pri vyradení dispečerského centra sa okrem nepredaného plynu zarátava taktiež zničený majetok, náklady na jej opravu, náklady na odstránenie škôd a sankcie za nedodanie plynu.

*Tab. 11. Tabuľka finančných dopadov na firmu.*

<b>hrozba</b>	<b>degradácia</b>	<b>hodnotenie</b>
<b>1</b> násilné alebo neoprávnené vniknutie cudzej osoby	20 %	1
<b>2</b> bombové útoky, použitie zbraní	40 %	2
<b>3</b> deštrukcia priestoru alebo jeho časti	20 %	1
<b>4</b> zničenie alebo vyradenie dispečingu	40 %	2
<b>5</b> požiar	40 %	2
<b>6</b> prívalový dážď	30 %	1
<b>7</b> prerušenie dodávky elektriny	20 %	1
<b>8</b> prevádzková porucha	20 %	1
<b>9</b> chybná manipulácia s prvkami	10 %	1
<b>10</b> nedodržanie pracovných postupov	10 %	1

Ako som spomínala v teoretickej časti, dopady sa viažu nielen na finančnú stránku, ale i na straty na životoch, počte zranených osôb a strate dobrého mena. Posledné spomínané kritérium sa nedá relatívne vypočítať, jeho dopad môže a nemusí byť kritický pre firmu a taktiež môže a nemusí nastať. V prípade hociktorého objektu prepravnej spoločnosti nastať určite nemôže, pretože firma tvorí monopol, teda nemá na Slovensku žiadnu konkurenciu. Čo sa týka počtu zranených osôb alebo dokonca strátach na životoch by sa nejednalo o vysoké čísla a z historických štatistík žiadny podobný incident nenastal, preto som si tieto kritéria mohla dovoliť vynechať.

## 7.4 Hodnotenie hrozieb

Na určenie pravdepodobnosti vzniku hrozby nevyužijem metódy popísané v teoretickej časti, pretože tabuľky a grafy, ktoré napomáhajú danému výpočtu sú špecifikované len pre štáty v USA. Pre svoje výpočty využijem kvalitatívnu metódu KARS.

Do Tabuľky 12. vpíšem do riadkov vybrané hrozby z Tabuľky 11. a očísľujem ich v ľubovoľnom poradí. Toto poradie musím zachovať i v stĺpcoch a hľadám súvislosti medzi hrozbami. Existujú len 2 možnosti:

- ak existuje reálna možnosť, že môže ovplyvniť alebo zapríčiniť inú hrozbu, napíšem 1,
- v opačnom prípade napíšem 0.

Napr. požiar môže spôsobiť prerušenie dodávky elektriny (1) avšak v žiadnom prípade nevyvolá prívalový dážď (0). Súčtom jednotiek v riadku dostávam súčet aktivity a súčtom jednotiek v stĺpci získavam súčet pasivity.

Tab. 12. Hodnotenie hrozieb metódou KARS.

	hrozby/hrozby	1	2	3	4	5	6	7	8	9	10	Σ A
1	násilné alebo neoprávnené vniknutie cudzej osoby		0	1	1	0	0	0	0	0	0	2
2	bombové útoky, použitie zbraní	0		1	1	0	0	1	1	0	0	4
3	deštrukcia priestoru alebo jeho časti	0	0		0	0	0	1	1	0	0	2
4	zničenie alebo vyradenie dispečerského centra	0	0	0		0	0	1	1	0	0	2
5	požiar	0	0	1	1		0	1	1	0	0	4
6	prívalový dážď	0	0	1	1	0		1	1	0	0	4
7	prerušenie dodávky elektriny	0	0	0	1	0	0		1	0	0	2
8	prevádzková porucha	0	0	0	1	0	0	1		0	0	2
9	chybná manipulácia s prvkami	0	0	0	0	0	0	1			0	1
10	nedodržanie pracovných postupov	0	0	0	1	0	0	1	1	0		3
ΣP	súčet pasivity	0	0	4	7	0	0	8	8	0	0	

Ďalej si vypočítam koeficient pasivity KP a aktivity KA zo vzorcov:

$$KA = \frac{\Sigma A}{x-1} \times 100 [\%]. \quad (13)$$

$$KP = \frac{\Sigma P}{x-1} \times 100 [\%]. \quad (14)$$

Kde:

x – je počet hrozieb, v tomto prípade 10.

Napr. 5. požiar:

$$KA_5 = \frac{4}{10-1} \times 100 = 44,44 [\%].$$

$$KP_5 = \frac{0}{10-1} \times 100 = 0 [\%].$$

Tab. 13. Výpočet koeficientu aktivity a pasivity.

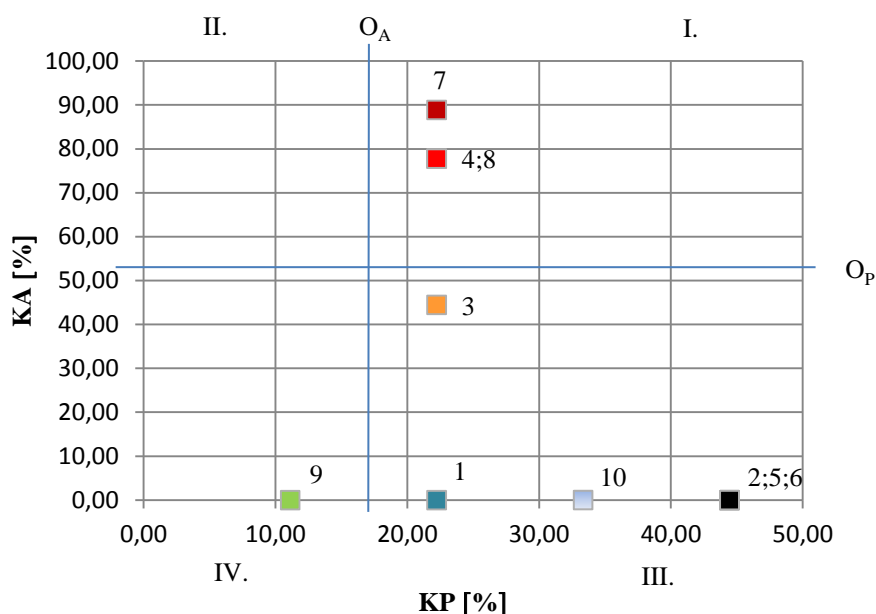
hrozba	KA [%]	KP [%]
1 násilné alebo neoprávnené vniknutie cudzej osoby	22,22	0,00
2 bombové útoky, použitie zbraní	44,44	0,00
3 deštrukcia priestoru alebo jeho časti	22,22	44,44
4 zničenie alebo vyradenie	22,22	77,78
5 požiar	44,44	0,00
6 prívalový dážď	44,44	0,00
7 prerušenie dodávky elektriny	22,22	88,89
8 prevádzková porucha	22,22	77,78
9 chybná manipulácia s prvkami	11,11	0,00
10 nedodržanie pracovných postupov	33,33	0,00

Výsledkom je výstupný graf (viz Obr. 9), kde sú podľa hodnôt koeficientov rozdelené hrozby. Graf rozdelím na kvadranty pomocou dvoch osí ( $O_A$  a  $O_P$ ), čím docielim rozdelenie nebezpečných hrozieb. Výpočet vychádza z maximálneho a minimálneho výsledku koeficientov, kde ale nezapočítavam hodnotu 0:

$$O_A = KA_{max} - \frac{(KA_{max} - KA_{min})}{100} \times 80 = 44,44 - \frac{(44,44 - 11,11)}{100} \times 80 = 17,78. \quad (15)$$

$$O_P = KP_{max} - \frac{(KP_{max} - KP_{min})}{100} \times 80 = 88,89 - \frac{(88,89 - 44,44)}{100} \times 80 = 53,33. \quad (16)$$





Obr. 9. Grafické vyhodnotenie metódy KARS.

- Oblasť I. kvadrantu tvoria primárne i sekundárne nebezpečné riziká: prerušenie dodávky elektriny, zničenie alebo vyradenie a prevádzková porucha.
- V II. kvadrante by mali byť sekundárne nebezpečné riziká, ktoré sa ale v mojom grafe nenachádzajú.
- III. oblasť obsahuje primárne nebezpečné riziká a to: deštrukciu priestoru alebo jeho časti, bombové útoky, požiar, prívalový dážď, nedodržanie pracovných postupov a násilné alebo neoprávnené vniknutie cudzej osoby.
- IV. časť grafu je relatívne bezpečná a v tomto prípade sa jedná o chybnú manipuláciu s prvkami.

Tab. 14. Pomocná tabuľka hodnotenia úrovne hrozby.

bodová hodnota	hodnota hrozby	degradácia
0	nepravdepodobná alebo nehodnotená	0 %
1	veľmi málo pravdepodobná	1 - 20 %
2	málo pravdepodobná	21 - 40 %
3	stredne pravdepodobná	41 - 60 %
4	značne pravdepodobná	61 - 80 %
5	vysoko pravdepodobná	81 - 100 %

Pomocou predchádzajúcich tabuliek určím úroveň hrozby (viz Tab. 15).

Tab. 15. Tabuľka hodnotenia úrovne hrozby.

	hrozba	KA [%]	úroveň hrozby
1	násilné alebo neoprávnené vniknutie cudzej osoby	22,22	2
2	bombové útoky, použitie zbraní	44,44	3
3	deštrukcia priestoru alebo jeho časti	22,22	2
4	zničenie alebo vyradenie	22,22	2
5	požiar	44,44	3
6	prívalový dážď	44,44	3
7	prerušenie dodávky elektriny	22,22	2
8	prevádzková porucha	22,22	2
9	chybná manipulácia s prvkami	11,11	1
10	nedodržanie pracovných postupov	33,33	2

## 7.5 Analýza zraniteľnosti

Zraniteľnosť v objekte dispečingu vyjadrím ako priemernú hodnotu koeficientu aktivity z predchádzajúceho bodu.

### Výpočty:

$$\overline{KA} = \frac{\sum_{i=1}^n x_i x_i}{n} \quad (17)$$

$$\overline{KA} = \frac{x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 + x_8 + x_9 + x_{10}}{n}.$$

$$\overline{KA} = \frac{0,2222 + 0,4444 + 0,2222 + \dots + 0,3333}{10} = 0,2889.$$

### Stredná kvadratická odchýlka:

$$S_n = \sqrt{\frac{\sum_{i=1}^n (x_i - \bar{x})^2}{n-1}}. \quad (18)$$

Kde:

$S_n$  - stredná kvadratická odchýlka spracovania štatistických údajov,

$x_i$  - hodnota  $i$ -tého rizika (koeficientu aktivity),

$x_{pr}$  - priemerná hodnota rizika (koeficientu aktivity),

$n$  - počet rizík.

### Výpočet:

$$S_n = \sqrt{\frac{(x_1 - x_{pr})^2 + (x_2 - x_{pr})^2 + (x_3 - x_{pr})^2 + \dots + (x_{10} - x_{pr})^2}{n - 1}}.$$

$$S_n = \sqrt{\frac{(0,2222 - 0,2889)^2 + (0,4444 - 0,2889)^2 + \dots + (0,3333 - 0,2889)^2}{10 - 1}}.$$

$$S_n = 0,1194.$$

Tab. 16. Pomocná tabuľka stanovenia zraniteľnosti.

bodová hodnota	hodnota hrozby	degradácia
0	nepravdepodobná alebo nehodnotená	0 %
1	veľmi málo pravdepodobná	1 - 20 %
2	málo pravdepodobná	21 - 40 %
3	stredne pravdepodobná	41 - 60 %
4	značne pravdepodobná	61 - 80 %
5	vysoko pravdepodobná až istá	81 - 100 %

Podmienená pravdepodobnosť predpokladaných hrozieb, teda celková zraniteľnosť činí **28,89 ± 11,94 %**, čo spadá pod bodovú hodnotu zraniteľnosti 2, teda málo pravdepodobná možnosť.

## 7.6 Hodnotenie rizika a odolnosť

Zhodnotenie doterajších výsledkov vykonáva výpočet celkového rizika a odolnosti objektu.

### Výpočet rizika:

$$Riziko = \frac{Dopad + Zraniteľnosť + Riziko}{3}^8. \quad (19)$$

Napr.:

$$Riziko_1 = \frac{0,2 \times 0,28 \times 0,2}{3} = 0,237 = 23,7\%.$$

Tab. 17. Hodnotenie rizika

	hrozby	dopady	zraniteľnosť	hrozba	riziko
1	násilné alebo neoprávnené vniknutie cudzej osoby	0,2	0,2889	0,2222	23,7 %
2	bombové útoky, použitie zbraní	0,5	0,2889	0,4444	39,4 %
3	deštrukcia priestoru alebo jeho časti	0,25	0,2889	0,2222	25,37 %
4	zničenie alebo vyradenie dispečerského centra	0,3	0,2889	0,2222	27,03 %
5	požiar	0,4	0,2889	0,4444	37,78 %
6	prívalový dážď	0,4	0,2889	0,4444	37,78 %
7	prerušenie dodávky elektriny	0,2	0,2889	0,2222	23,70 %
8	prevádzková porucha	0,3	0,2889	0,2222	27,03 %
9	chybná manipulácia s prvkami	0,15	0,2889	0,1111	18,33 %
10	nedodržanie pracovných postupov	0,4	0,2889	0,3333	34,07 %
	priemerné riziko				<b>29,43 %</b>
	odchýlka				<b>6,08 %</b>

<sup>8</sup> V procese RAMCAP Plus je hodnota rizika hodnotená násobením parametrov, avšak v tom prípade sa jedná o kumulatívny matematický vzťah, ktorý veľmi skresľuje výsledok a preto som pristúpila k spriemerovaniu parametrov, čo bude objektívnejšie hodnotiť realitu.

**Výpočet odolnosti:**

$$Odolnosť = 1 - \frac{(Ušlý zisk + Riziko + Hrozba)}{3} \quad (20)$$

Napr.:

$$Odolnosť_1 = 1 - \frac{0,2 + 0,1284 + 0,2}{3} = 0,7802 = 78,02\%.$$

*Tab. 18. Výpočet odolnosti objektu.*

	hrozby	ušlý zisk	riziko	hrozba	odolnosť
<b>1</b>	<b>násilné alebo neoprávnené vniknutie cudzej osoby</b>	0,2	0,1284	0,2222	78,02 %
<b>2</b>	<b>bombové útoky, použitie zbraní</b>	0,45	0,6420	0,4444	57,04 %
<b>3</b>	<b>deštrukcia priestoru alebo jeho časti</b>	0,25	0,1605	0,2222	75,80 %
<b>4</b>	<b>zničenie alebo vyradenie dispečerského centra</b>	0,3	0,1926	0,2222	73,58 %
<b>5</b>	<b>požiar</b>	0,4	0,0514	0,4444	59,26 %
<b>6</b>	<b>prívalový dážď</b>	0,4	0,0514	0,4444	59,26 %
<b>7</b>	<b>prerušenie dodávky elektriny</b>	0,2	0,1284	0,2222	78,02 %
<b>8</b>	<b>prevádzková porucha</b>	0,3	0,0193	0,2222	73,58 %
<b>9</b>	<b>chybná manipulácia s prvkami</b>	0,15	0,0048	0,1111	85,19 %
<b>10</b>	<b>nedodržanie pracovných postupov</b>	0,3	0,0385	0,3333	67,53 %
	<b>priemerná odolnosť</b>				<b>70,73 %</b>
	<b>odchýlka</b>				<b>9,53 %</b>

Z predchádzajúcich tabuliek jasne vychádza, že po zhodnotení všetkých vybraných hrozieb je výsledné riziko objektu dispečingu **29 ± 6,08 %** a celková hodnota odolnosti objektu tvorí takmer **71 ± 9,5 %**.

---

<sup>9</sup> V procese RAMCAP Plus je hodnota odolnosti vyjadrená násobením parametrov, avšak v tom prípade sa jedná o kumulatívny matematický vzťah, ktorý veľmi skresľuje výsledok. Hodnota odolnosti je prevrátená hodnota k zraniteľnosti a z aktuálneho poznania, ktoré vyplýva z výskumného projektu, ktorý má táto práca podporiť vychádza vzťah ako priemerná hodnota parametrov odčítaná od hodnoty 1.

## 7.7 Riadenie rizika a odolnosti

V poslednom kroku je nevyhnutné zhodnotiť predchádzajúce body a výsledky, ktoré z nich vyšli a urobiť potrebné opatrenia, ktoré by napomohli k vylepšeniu odolnosti a zníženiu možného vzniku rizika.

Firma musí v prvom rade rozhodnúť, aká úroveň rizika a odolnosti je pre ňu únosná a prijateľná a naopak, čo treba v blízkej budúcnosti upraviť na požadovanú úroveň. K tomuto rozhodnutiu si pripravím maticu, kde na jednej strane rozdelím únosnosť rizika a na druhej strane únosnosť odolnosti (viz Obr. 10). Medzné hodnoty som zvolila podľa vlastného uváženia. V prípade, ak riziko vzniku udalosti je pod 50%, patrí do veľmi vysokého rizika, ktoré firme môže nastať a naopak veľmi vysoké riziko hrozí, keď hodnota odolnosti je menšia ako 50%. Čísllice v matici znamenajú priradené hodnoty hrozieb z predchádzajúcich tabuliek (napr. číslo 1 = násilné alebo neoprávnené vniknutie cudzej osoby do objektu).

		Legenda:			
					veľmi vysoké riziko
					vysoké riziko
					zvýšené riziko
					prijateľné riziko
Riziko	nad 50 %				
	nad 35 %		2,5,6		
	nad 10 %	1,3,7	4,8,10		
	do 10 %	9			
		nad 90 %	nad 75 %	nad 50 %	pod 50 %
		Odolnosť			

Obr. 10. Matica akceptovateľnosti rizík

Z obrázku matice je jasne viditeľné, že pod hrozbou veľmi vysokého rizika, ktoré by muselo byť okamžite odstránené nespadá žiadna oblasť a preto je vhodné predpokladať, že objekt je dostatočne chránený.

V oblasti vysokého rizika sa nachádzajú tri položky, ktoré je vhodné v blízkej dobe odstrániť. Jedná sa o riziko bombových útokov alebo použitia zbraní hromadného ničenia, čo je oblasť, pred ktorou je odolnosť akéhokoľvek objektu takmer vždy prelomená, preto je nevyhnutné sa danou problematikou zaoberať. Z hľadiska ochrany voči požiaru alebo prívalovému dažďu je možné zvýšiť odolnosť a riešenie tohto problému posunúť na prvé miesto v poradí pred ostatnými.

Prívalový dážď robí problémy celému mestu Senica kvôli nedostatočnej úrovne vybudovania kanalizačného systému a blízkosti umelej priehrady, ktorú nestíhajú pri prívalovom daždi vypúšťať.

Zvýšenú pozornosť si vyžadujú i riziká umiestnené v oblasti zvýšeného rizika. Zvýšenie odolnosti nie je v rámci objektu nevyhnutné, ale svojím spôsobom môže byť riešenie nápomocné i k vyššie menovaným vážnejším rizikám.

Prijateľnou akceptovateľnosťou rizika oplýva v tomto objekte chybná manipulácia s prvkami. Predchádzanie rizika spočíva v princípe riadne zaškolených pracovníkov, ktorí prácu so zariadeniami vykonávajú a v dostatočne odvedenej kontrolnej činnosti nad pracovníkmi, ktorú uskutočňujú vedúci oddelení a samozrejme i kvalitnými zariadeniami, ktoré sú ošetrované voči zlej manipulácii (napr. prepäťovou ochranou).

Po zhodnotení stávajúceho stavu objektu, demografického vývoju, lokalite, výskytu protiprávnej činnosti, faktu, že spadá pod kritickú infraštruktúru a predchádzajúcich zistení o stave odolnosti voči vybraným hrozbám a vzniku ich rizika je možné zadefinovať potrebu nových alebo vylepšených opatrení k zvýšeniu odolnosti a zmierneniu rizika.

Z finančného hľadiska nie je možné uskutočniť stopercentnú ochranu a odolnosť objektu. Preto vytýčim len najdôležitejšie opatrenia. V prvom rade by som sa zamerala na kamerový systém. Kamier je síce v objekte umiestnených veľmi veľa, no chránia objekt už niekoľko rokov a ich slabší dosah a nedostatočné nočné videnie môže byť pre objekt nebezpečný kvôli neidentifikácii páchatel'a v objekte.

Ďalšou slabosťou objektu je malý počet aktívnych i pasívnych detektorov umiestnených v objekte, preto by som navrhla zvýšiť ich počet. Tieto vylepšenia môžu mať veľký vplyv na celkový integrovaný zabezpečovací systém, ktorý sa skladá z dochádzkového systému, kamerového systému, elektronických zabezpečovacích systémoch, elektronických požiarnych systémoch, riadení interných systémov (výťahy, klimatizácia, kúrenie) a poplachovému prijímaciemu centru.

## ZÁVER

Hodnotenie odolnosti patrí k významným oblastiam pri zaistení plynulej prevádzky kritickej infraštruktúry. Odolnosť posudzuje objekty kritickej infraštruktúry z hľadiska miery eliminácie účinkov jednotlivých hrozieb. Je vnímaná ako vlastnosť systému prekonať narušenie a znášať negatívne zmeny systému bez toho, aby narušila funkčnosť systému. Medzi najdôležitejšie činitele, ktoré negatívne vplyvajú na funkciu systému, patria živelné pohromy, priemyslové havárie, finančné a ekonomické degradácie, fyzické a kybernetické útoky.

Hodnotenie odolnosti úzko súvisí s ochranou kritickej infraštruktúry. Zvýšením počtu investícií, ktoré sú priamo využité na ochranu kritickej infraštruktúry, priamoúmerne stúpa odolnosť. Ochrana výrazným spôsobom ovplyvňuje odolnosť i zraniteľnosť systému. Nikdy nemôže dosiahnuť stopercentnú účinnosť. Od roku 2001 je ochrana kritickej infraštruktúry rozpracovaná v rôznych štátnych legislatívach. Tvorba ochrany si vyžaduje širokú spoluprácu odborníkov z mnohých odvetví. V dnešnom globalizovanom svete sa daná problematika rieši v širšom meradle. Keďže niektorá kritická infraštruktúra presahuje hranice štátu, musí byť ochrana riešená komplexne. V teoretickej časti porovnávam historický princíp legislatívneho riešenia ochrany a sektorového rozdelenia kritickej infraštruktúry v USA, EÚ, Českej a Slovenskej republike.

K dosiahnutiu presnejších výsledkov je vhodné použiť multikriteriálne hodnotenie. Vo svojej diplomovej práci som sa venovala rôznym faktorom, ktoré môžu ovplyvniť hodnotu odolnosti kritickej infraštruktúry. Medzi najdôležitejšie patria bezpečnostné posúdenie objektu a jeho okolia, charakter hroziaceho útoku, dopady, ktoré môžu spôsobiť, úroveň zraniteľnosti z finančného a ekonomického hľadiska a pravdepodobnosť vzniku mimoriadnej udalosti.

Každá oblasť kritickej infraštruktúry spadá pod ochranu utajovaných informácií a preto som použila rôzne kritériálne hodnotenia na fiktívnom objekte kritickej infraštruktúry. V Slovenskej republike patrí plyn k jedným najviac využívaným energetickým prostriedkom, preto som si vybrala práve dispečing prepravnej plynárenskej spoločnosti. Z dôvodu, že u nás zatiaľ neexistuje žiadny ucelený proces hodnotenia odolnosti alebo zraniteľnosti kritickej infraštruktúry, podkladom k mojim analýzam a výpočtom sa stal americký proces RAMCAP Plus.



Prínosom mojej práce je podpora riešenia projektu bezpečnostného výskumu v ČR VG20112014067 Systém hodnocení odolnosti prvků a sítí vybraných oblastí kritické infrastruktury.

## ZÁVER V ANGLIČTINE

The resilience evaluation belongs to the most significant areas while providing continuous operation of the critical infrastructure. The resilience considers subjects of critical infrastructure from the point of elimination rate of individual threats and their impacts. It is perceived as a characteristic which can overcome the system disruption and it can withstand any negatives of system changes without disrupting the system functionality. The most important factors that negatively affect the function of the system are natural disasters, industrial collisions, financial and economical degradation or physical and cybernetic attacks.

The resilience evaluation is closely related to the protection of critical infrastructure. By increasing the number of investments which are directly used for protection of critical infrastructure, the resilience increases proportionally. The protection strongly influences the resilience and vulnerability of the system. We can never reach 100% effectiveness. Since 2001 the protection of critical infrastructure has been developing in many state legislatures. The formation of protection requires wide cooperation of many specialists from different fields. In this global world this problematic can be solved worldwide. Since some critical infrastructure can exceed the state borders, it must be solved comprehensively.

In the theoretical part the thesis compares the historical principles of legislative protection and sector division of the critical infrastructure in the USA, the European Union, the Czech Republic and Slovakia.

When the specialists want to reach concrete, accurate and specific results, it is appropriate to use multicriterial evaluation. In this master thesis I was dealing with various factors that might influence the value of resilience of the critical infrastructure. In Slovakia natural gas is the most used energy source that's why I have decided to describe the dispatching of transportation gasworks company. Since in Slovakia there exists no self-contained process of resilience evaluation and vulnerability of critical infrastructure, I have decided to use the American process RAMCAP Plus as a base for my analysis and calculation in this thesis.

The main contribution of this thesis is to outline the solution in the project for security investigation in the Czech Republic VG20112014067- The System of Resilience Evaluation of the Elements and Networks in the Chosen Areas of Critical Infrastructure.

## ZOZNAM POUŽITEJ LITERATÚRY

- [1] Slovenská republika. Zákon č. 45/2011 Zb. o kritickej infraštruktúre. In: *Zbierka zákonov*. 8. februára 2011, 45/2011, 19.
- [2] MOZGA, Jaroslav, Miloš VÍTEK a František KOVÁŘÍK. *Kritická infrastruktúra spoločnosti*. Hradec Králové: GAUDEAMUS, 2008. Univerzita Hradec Králové. ISBN 978-80-7041-299-2.
- [3] LUKÁŠ, Luděk a Martin HROMADA. *Možnosti hodnocení odolnosti kritické infrastruktury/ Evaluating the Resistance of Critical Infrastructure, Bezpečnost v informační společnosti*, Brno, 2009.
- [4] HROMADA, Martin. *Konceptuálny návrh systému hodnotenia odolnosti prvku kritickej infraštruktúry*, In: Bezpečnostní technologie systémy a management – mezinárodní konference, Zlín, 2011, ISBN: 978-80-7454-111-7.
- [5] 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.
- [6] ŠENOVSKÝ, Michail, Vilém ADAMEC a Pavel ŠENOVSKÝ. *Ochrana kritické infrastruktury*. Ostrava: Sdružení požárního a bezpečnostního inženýrství, 2007. SPBI Spektrum, 51. ISBN 978-80-7385-025-8.
- [7] ŠENOVSKÝ, Michail a Vilém ADAMEC. *Právní rámec krizového managementu: Management záchranných prací*. 2. aktualizované a rozšířené vydání. Ostrava: Sdružení požárního a bezpečnostního inženýrství, 2007. SPBI Spektrum, 39. ISBN 80-86634-67-1.
- [8] MOZGA, Jaroslav a František KOVÁŘÍK. Několik poznámek k ochraně kritické infrastruktury. In: [online]. [cit. 2012-04-29]. Dostupné z: [http://www.population-protection.eu/attachments/027\\_vol2n1\\_mozga\\_kovarik.pdf](http://www.population-protection.eu/attachments/027_vol2n1_mozga_kovarik.pdf).
- [9] *Homeland Security* [online]. © 2011 [cit. 2012-04-19]. Dostupné z: [http://www.dhs.gov/files/programs/gc\\_1189168948944.shtm](http://www.dhs.gov/files/programs/gc_1189168948944.shtm).
- [10] Európska únia. Smernica rady o identifikácii a označení európskych kritických infraštruktúr a zhodnotení potreby zlepšiť ich ochranu. In: *Úradný vestník Európskej únie*, 23.12.2008, roč. 2008, 2008/114/ES, L 345/75. Dostupné z: <http://eur->

lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:SK:PDF

.

- [11] Česká republika. Zákon o územním plánování a stavebním řádu (stavební zákon). In: *Sbírka zákonů*. 14.3.2006, roč. 2006, 183/2006/2011, 63. Dostupné z: <http://aplikace.mvcr.cz/archiv2008/sbirka/2006/sb063-06.pdf>.
- [12] Česká republika. Úplné znění zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon). In: *Sbírka zákonů*. 6.5.2011, roč. 2011, 118/2011, 44. Dostupné z: [http://www.epravo.cz/\\_dataPublic/sbirky/2011/sb0044-2011.pdf](http://www.epravo.cz/_dataPublic/sbirky/2011/sb0044-2011.pdf).
- [13] Slovenská republika. Konceptia kritickej infraštruktúry v Slovenskej republike a spôsob jej ochrany a obrany, 2007. Dostupné z: [www.minv.sk/?ochrana-kritickej-infrastruktury&subor=10691](http://www.minv.sk/?ochrana-kritickej-infrastruktury&subor=10691).
- [14] USA. White paper, The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63. 22.5.1998. Dostupné z: <http://csrc.nist.gov/drivers/documents/paper598.pdf>.
- [15] MARCHEVKA, Peter. Kritická infraštruktúra v Európskej únii a v Severoatlantickej aliancii. *Krízový Management* [online]. 2011, č. 1 [cit. 2012-04-15]. Dostupné z: <http://fsi.uniza.sk/kkm/files/admincasopis/KM%201%202011/ODBORNE/Marchevka.pdf>.
- [16] Európska únia. Smernica rady 2008/114/ES: o identifikácii a označení európskych kritických infraštruktúr a zhodnotení potreby zlepšiť ich ochranu. In: *Úradný vestník Európskej únie*. Brusel, 8.12.2008. Dostupné z: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:SK:PDF>.
- [17] ŘÍHA, Jozef. Problematika Kritickej infraštruktúry v dokumentech EÚ. *Security Revues* [online]. 2010, č. 4 [cit. 2012-04-15]. Dostupné z: <http://www.securityrevue.com/article/2010/09/problematika-kritickej-infrastruktury-v-dokumenoch-eu/>.
- [18] EU. Green Paper on a European Programme for Critical Infrastructure. In: COMMUNICATION FROM THE COMMISSION. Brusel, 2005. Dostupné z: [http://eur-lex.europa.eu/LexUriServ/site/en/com/2005/com2005\\_0576en01.pdf](http://eur-lex.europa.eu/LexUriServ/site/en/com/2005/com2005_0576en01.pdf).

- [19] EU. European Programme for Critical Infrastructure Protection . In COMMUNICATION FROM THE COMMISSION, 2006. Dostupné z: [http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006\\_0786en01pdf](http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0786en01pdf).
- [20] EU. Rozhodnutie rady o varovnej informačnej sieti kritickej infraštruktúry . In COMMUNICATION FROM THE COMMISSION. Brusel, 2008. Dostupné z: [http://www.europarl.europa.eu/meetdocs/2004\\_2009/documents/sec/com\\_sec%282008%292702\\_/com\\_sec%282008%292702\\_sk.pdf](http://www.europarl.europa.eu/meetdocs/2004_2009/documents/sec/com_sec%282008%292702_/com_sec%282008%292702_sk.pdf).
- [21] Česká republika. Komplexní strategie České republiky k řešení problematiky kritické infrastruktury a Národní program ochrany kritické infrastruktury, dostupné z: <http://krizport.firebrno.cz/file/132>.
- [22] Slovenská republika. Národný program pre ochranu a obranu kritickej infraštruktúry v Slovenskej republike, dostupné z: [http://www.google.com/url?q=http://www.minv.sk/%3Fochranakritickejinfrastruktury%26subor%3D10692&ei=WhUUS\\_X\\_HKLkmwPJ6NHUAg&sa=X&oi=spellmeleon\\_result&resnum=1&ct=result&ved=0CAYQhgIwAA&usg=AFQjCNF2wxySWqBB0Bm5uGLGneBOxe9AGw](http://www.google.com/url?q=http://www.minv.sk/%3Fochranakritickejinfrastruktury%26subor%3D10692&ei=WhUUS_X_HKLkmwPJ6NHUAg&sa=X&oi=spellmeleon_result&resnum=1&ct=result&ved=0CAYQhgIwAA&usg=AFQjCNF2wxySWqBB0Bm5uGLGneBOxe9AGw).
- [23] Európska únia. Critical Infrastructure Protection in the fight against terrorism. In: *Communication from the commission to the council and the european parliament*. Brusel, 2004. Dostupné z: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0702:FIN:EN:PDF>.
- [24] TODD, Keil. Enhancing Critical Infrastructure Resilience. *Homeland Security* [online]. 22.12.2010, [cit. 2012-04-15]. Dostupné z: <http://blog.dhs.gov/2010/12/enhancing-critical-infrastructure.html>.
- [25] Európska únia. Smernica rady 2008/114/ES: o identifikácii a označení európskych kritických infraštruktúr a zhodnotení potreby zlepšiť ich ochranu. In: *Úradný vestník Európskej únie*. Brusel, 8.12.2008. Dostupné z: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:SK:PDF>.
- [26] HODÁSOVÁ, Zuzana. Problematika kritickej infraštruktúry v dokumentoch EÚ. *Security Review* [online]. 28.9.2010[cit. 2012-04-15]. ISSN 1336-9717. Dostupné z: <http://www.securityreview.com/article/2010/09/problematika-kritickej-infrastruktury-v-dokumenoch-eu/>.

- [27] BENEŠ, Ivan. Nejzranitelnější kritickou infrastrukturou je elektroenergetika. *Ekolist* [online]. 21.1.2011[cit. 2012-04-15]. ISSN 1802-9019. Dostupné z: <http://ekolist.cz/cz/publicistika/nazory-a-komentare/ivan-benes-nejzranitelnejsi-kritickou-infrastrukturou-je-elektroenergetika>.
- [28] Ochrana kritickej infraštruktúry. *Ministerstvo vnútra SR* [online]. 2011 [cit. 2012-04-15]. Dostupné z: <http://www.minv.sk/?ochrana-kritickej-infrastruktury>.
- [29] DVOŘÁK, Zdeněk a Mária LUSKOVÁ. Základný výskum v oblasti kritickej infraštruktúry. *Krízový management* [online]. 2011, č. 1 [cit. 2012-04-15]. Dostupné z: [http://fsi.uniza.sk/kritinf/aktuality/publik/01\\_dvorak\\_luskova\\_2011-1-km.pdf](http://fsi.uniza.sk/kritinf/aktuality/publik/01_dvorak_luskova_2011-1-km.pdf).
- [30] MARCHEVKA, Peter. Súčasnosť a budúcnosť kritickej infrastruktúry v Slovenskej republike. *Krízový management* [online]. 2011, č. 2 [cit. 2012-04-15]. Dostupné z: <http://fsi.uniza.sk/kkm/files/admincasopis/KM%202%202011/ODBORNE/Marchevka.pdf>.
- [31] ŘÍHA, Jozef. Kritická infrastruktúra a riziko mimořádné události. *Urbanizmus a územní rozvoj* [online]. 2007, č. 4 [cit. 2012-04-15]. Dostupné z: [http://www.uur.cz/images/publikace/uur/2007/2007-04/08\\_kriticka.pdf](http://www.uur.cz/images/publikace/uur/2007/2007-04/08_kriticka.pdf).
- [32] BENEŠ, Ivan. Procesní model pro ochranu kritické infrastruktúry. *Enviromentální* [online]. 21.1.2011[cit. 2012-04-15]. ISSN 1802-9019. Dostupné z: [http://www.cemc.cz/aspekty/vyber\\_z\\_clanku/legislative/prevence/dokumenty/3.pdf](http://www.cemc.cz/aspekty/vyber_z_clanku/legislative/prevence/dokumenty/3.pdf).
- [33] Zemní plyn. [online]. [cit. 2012-04-18]. Dostupné z: <http://www.zemniplyn.cz/doprava/default.htm>.
- [34] Zemní plyn. [online]. [cit. 2012-04-18]. Dostupné z: <http://www.zemniplyn.cz/plyn/default.htm>.
- [35] Sektorová správa o fungovaní trhu so zemným plynom v SR. In: [online]. Protimonopolný úrad Slovenskej republiky, november 2010 [cit. 2012-04-19]. Dostupné z: [http://www.antimon.gov.sk/files/26/2010/Sprava\\_PMU\\_SR\\_Plyn.pdf](http://www.antimon.gov.sk/files/26/2010/Sprava_PMU_SR_Plyn.pdf).
- [36] *SPP* [online]. © 2012 [cit. 2012-04-19]. Dostupné z: <http://www.spp.sk/>.

- [37] *SPP- distribúcia* [online]. © 2011 [cit. 2012-04-19]. Dostupné z: <http://www.spp-distribucia.sk/>.
- [38] *Eustream* [online]. © 2009 [cit. 2012-04-19]. Dostupné z: <http://eustream.sk/>.
- [39] NaturalGas.org: Natural Gas Distribution. [online]. © 2004-2011 [cit. 2012-04-19]. Dostupné z: <http://www.naturalgas.org/naturalgas/distribution.asp>.
- [40] JANUS, Ján. Dispečing slovenskej prepravnej siete. *Slovgas: Riadiace a informačné systémy* [online]. 2011, č. 2 [cit. 2012-04-23]. Dostupné z: [http://www.szn.sk/Slovgas/Casopis/2011/2/2011\\_2\\_10.pdf](http://www.szn.sk/Slovgas/Casopis/2011/2/2011_2_10.pdf).
- [41] BULÁKOVÁ, Ľudmila. Začiatky ťažby zemného plynu na Slovensku. *Slovgas: Z historie plynárenstva* [online]. 2011, č. 4 [cit. 2012-04-23]. Dostupné z: [http://www.szn.sk/Slovgas/Casopis/2011/4/2011\\_4\\_14.pdf](http://www.szn.sk/Slovgas/Casopis/2011/4/2011_4_14.pdf).
- [42] HORNÍK, Ján. Plánovanie prepravy zemného plynu a jej optimalizácia. *Slovgas: Riadenie prepravy a distribúcie* [online]. 2006, č. 1 [cit. 2012-04-23]. Dostupné z: [http://www.szn.sk/Slovgas/Casopis/2006/1/2006\\_1\\_03.pdf](http://www.szn.sk/Slovgas/Casopis/2006/1/2006_1_03.pdf).
- [43] PRELEC, Rastislav. Dispečerské riadenie distribučnej siete v podmienkach liberalizovaného trhu. *Slovgas: Riadenie prepravy a distribúcie* [online]. 2006, č. 1 [cit. 2012-04-23]. Dostupné z: [http://www.szn.sk/Slovgas/Casopis/2006/1/2006\\_1\\_05.pdf](http://www.szn.sk/Slovgas/Casopis/2006/1/2006_1_05.pdf).
- [44] ZÁHORSKÝ, Peter. Riadenie slovenského tranzitného systému. *Slovgas: Riadenie prepravy a distribúcie* [online]. 2006, č. 1 [cit. 2012-04-23]. Dostupné z: [http://www.szn.sk/Slovgas/Casopis/2006/1/2006\\_1\\_04.pdf](http://www.szn.sk/Slovgas/Casopis/2006/1/2006_1_04.pdf).
- [45] Preprava zemného plynu na území Slovenska. *TZB Portal* [online]. ISSN 1338-3418. © 2010 - 2011 [cit. 2012-04-23]. Dostupné z: <http://www.tzbportal.sk/kurenie-voda-plyn/preprava-zemneho-plynu-na-uzemi-slovenska.html>.
- [46] MINDEK, Milan. Úlohy plynárenského dispečingu na Slovensku. *Slovgas: Plynárenská a energetická legislatíva* [online]. 2011, č. 1 [cit. 2012-04-23]. Dostupné z: [http://www.szn.sk/Slovgas/Casopis/2011/1/2011\\_1\\_11.pdf](http://www.szn.sk/Slovgas/Casopis/2011/1/2011_1_11.pdf).
- [47] Výročná správa 2011. In: [online]. Eustream Slovak Gas TSO, január 2011 [cit. 2012-04-24]. Dostupné z: [http://eustream.sk/sk\\_stiahnut-subor/vyrocnna-sprava-2011](http://eustream.sk/sk_stiahnut-subor/vyrocnna-sprava-2011).

**SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK**

AHP	Analytický hierarchický proces.
ASMF	American Society of Mechanical Engineers.
CCTV	Closed-circuit television.
CIWIN	Critical Infrastructure Warning Information Network.
CNG	Compressed Natural Gas.
ČR	Česká republika.
DAT	Defence Against Terrorism.
ECI	European critical infrastructure.
EPCIP	The European Programme for Critical Infrastructure Protection.
EÚ	Európska únia.
FBI	Federal Bureau of Investigation.
FEMA	Federal Emergency Management Agency.
IT	Information technology.
KI	Kritická infraštruktúra.
LNG	Liquefied Natural Gas.
MW	Megawatt.
NATO	The North Atlantic Treaty Organization.
NISCC	National Infrastructure Security Coordination Centre.
OSN	United Nations Organisation.
RAMCAP	Risk Analysis and Management for Critical Assets Protection.
RMS	Risk Management Solution.
SCADA	Supervisory Control and Data Acquisition.
SCEPS	Senior Civil Emergency Planning Committee.
SPP	Slovenský plynárenský priemysel.



SR Slovenská republika.

USA United States of America.

**ZOZNAM OBRÁZKOV**

Obr. 1. Sedem krokov procesu RAMCAP. [5] .....	36
Obr. 2. Graf pravdepodobnosti napadnutia miest v USA. [5] .....	45
Obr. 3. Matica rizík. [5] .....	48
Obr. 4. Prepravná sieť eustream na SR. [45, 47] .....	54
Obr. 5. Mapa prepravnej siete plynu.....	58
Obr. 6. Organizačná štruktúra.....	59
Obr. 7. Analýza dopadov. ....	67
Obr. 8. Výmena potrubia a guľového uzáveru .....	69
Obr. 9. Grafické vyhodnotenie metódy KARS.....	73
Obr. 10. Matica akceptovateľnosti rizík .....	78

**ZOZNAM TABULIEK**

Tab. 1. Sektory kritickej infraštruktúry USA. [9].....	12
Tab. 2. Sektory kritickej infraštruktúry EÚ. [10] .....	13
Tab. 3. Sektory v pôsobnosti ústredných orgánov ČR. [12].....	15
Tab. 4. Sektory v pôsobnosti ústredných orgánov SR. [1] .....	16
Tab. 5. Stanovenie zraniteľnosti. [5] .....	41
Tab. 6. Rozdelenie skupín podľa pravdepodobnosti útoku. [5].....	46
Tab. 7. Zloženie zemného plynu v januári 2012. [36].....	53
Tab. 8. Parametre zemného plynu. [36].....	53
Tab. 9. Vymedzenie hrozieb dispečingu.....	65
Tab. 10. Výpočet ekonomickej degradácie.....	68
Tab. 11. Tabuľka finančných dopadov na firmu. ....	70
Tab. 12. Hodnotenie hrozieb metódou KARS.....	71
Tab. 13. Výpočet koeficientu aktivity a pasivity. ....	72
Tab. 14. Pomocná tabuľka hodnotenia úrovne hrozby. ....	73
Tab. 15. Tabuľka hodnotenia úrovne hrozby.....	74
Tab. 16. Pomocná tabuľka stanovenia zraniteľnosti.....	75
Tab. 17. Hodnotenie rizika .....	76
Tab. 18. Výpočet odolnosti objektu.....	77