

Tvorba nástroje pro multikriteriální hodnocení odolnosti kritické infrastruktury

Multi-criteria Evaluation of Critical Infrastructure Resilience Tool
Development

Bc. Aleš Venclík

Diplomová práce
2013



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2012/2013

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Bc. Aleš VENCLÍK**
Osobní číslo: **A11341**
Studijní program: **N3902 Inženýrská informatika**
Studijní obor: **Bezpečnostní technologie, systémy a management**
Forma studia: **prezenční**

Téma práce: **Tvorba nástroje pro multikriteriální hodnocení
odolnosti kritické infrastruktury**

Zásady pro vypracování:

1. Vypracujte literární rešerši na téma kritická infrastruktura.
2. Pojedejte o obecných principech vnímání odolnosti kritické infrastruktury.
3. Diskutujte o používaných principech hodnocení odolnosti kritické infrastruktury.
4. Stanovte kriteria pro potřeby hodnocení odolnosti kritické infrastruktury.
5. Navrhněte nástroj pro multikriteriální hodnocení odolnosti kritické infrastruktury.

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. Vztažná legislativa, příslušné evropské, vnitrostátní, resortní a další normy.
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 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.

Vedoucí diplomové práce:

Ing. Martin Hromada, Ph.D.

Ústav bezpečnostního inženýrství

Datum zadání diplomové práce:

8. února 2013

Termín odevzdání diplomové práce:

3. června 2013

Ve Zlíně dne 8. února 2013

prof. Ing. Vladimír Vašek, CSc.

děkan



doc. RNDr. Vojtěch Křesálek, CSc.

ředitel ústavu

ABSTRAKT

Tato práce se věnuje tématu ochrany a odolnosti kritické ochrany. Teoretická část je zaměřena především na porovnání vývoje kritické infrastruktury v ČR, USA, EU a NATO. Zabývá se vzájemnou propojeností prvků kritické infrastruktury a popisuje a srovnává metody pro vyhodnocení odolnosti prvku kritické infrastruktury. V praktické části se práce věnuje použití a aplikaci metody KARS při hodnocení odolnosti prvku kritické infrastruktury a využití těchto poznatků k vytvoření nástroje pro multikriteriální hodnocení prvku kritické infrastruktury Křížák.

Klíčová slova: kritická infrastruktura, ochrana kritické infrastruktury, odolnost kritické infrastruktury, hodnocení odolnosti kritické infrastruktury, KARS, Křížák

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 the North Atlantic Treaty Organisation. It deals with the the interconnectedness between critical infrastructure elements and describes and compares the methods for evaluation of the resistance of critical infrastructure elements. In the practical part thesis deals with the use and application of the KARS method for evaluating the resistance of the critical infrastructure element and using this knowledge to create a multi-criteria evaluation tool for critical infrastructure element Crusader.

Keywords: critical infrastructure, protection of critical infrastructure, resilience of critical infrastructure, evaluation of critical infrastructure resilience, KARS, Crusader

Děkuji panu Ing. Martinu Hromadovi, Ph.D. za vedení, rady a připomínky ohledně diplomové práce.

Dále děkuji svým blízkým a přátelům za podporu při studiu. Děkuji také všem svým přátelům a kolegům za čas stráveným při studiu, bez nichž by studentská léta nebyly to pravé. Největší dík však patří mé rodině za podporu po celou dobu studia

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

OBSAH	7
ÚVOD	9
TEORETICKÁ ČÁST	10
1 KRITICKÁ INFRASTRUKTURA	11
1.1 ZÁKLADNÍ POJMY TÝKAJÍCÍ SE KRITICKÉ INFRASTRUKTURY	11
1.2 LEGISLATIVNÍ ZDROJE	12
2 VÝVOJ OBORU KRITICKÁ INFRASTRUKTURA	14
2.1 VÝVOJ V ČESKÉ REPUBLICE	14
2.1.1 VÝVOJ PŘED ROKEM 1989	14
2.1.2 VÝVOJ PO ROCE 1989	14
2.2 VÝVOJ V EVROPĚ A EVROPSKÉ UNII	17
2.2.1 ZÁKLADNÍ PRINCIPY EPCIP	18
2.2.2 CÍLE EPCIP	19
2.2.3 DEFINICE A OBLASTI EVROPSKÉ KRITICKÉ INFRASTRUKTURY	19
2.3 VÝVOJ V RÁMCI SEVEROATLANTICKÉ ALIANCE	20
2.4 VÝVOJ VE SPOJENÝCH STÁTECH AMERICKÝCH	21
2.4.1 DEPARTMENT OF HOMELAND SECURITY	23
2.4.2 ROZDĚLENÍ ODPOVĚDNOSTI ZA KRITICKOU INFRASTRUKTURU V RÁMCI USA	24
3 VÝZNAM KRITICKÉ INFRASTRUKTURY	25
4 PRVKY KRITICKÉ INFRASTRUKTURY	27
4.1 PROCES URČOVÁNÍ PRVKŮ KRITICKÉ INFRASTRUKTURY	27
4.2 ZDRAVOTNÍ PÉČE	28
4.2.1 PŘEDNEMOCNIČNÍ NEODKLADNÁ PÉČE.....	29
4.2.2 NEMOCNIČNÍ PÉČE.....	29
4.2.3 OCHRANA VEŘEJNÉHO ZDRAVÍ.....	30
4.2.4 VÝROBA, SKLADOVÁNÍ A DISTRIBUCE LÉČIV A ZDRAVOTNICKÝCH PROSTŘEDKŮ	30
5 OHROŽENÍ KRITICKÉ INFRASTRUKTURY	31
5.1 KRITICKÁ INFRASTRUKTURA JAKO KOMPLEXNÍ SYSTÉM	31
5.2 PROPOJITELNOST KRITICKÉ INFRASTRUKTURY	31
5.3 KRITIČNOST KRITICKÉ INFRASTRUKTURY	32
5.4 HROZBY OHROŽUJÍCÍ KRITICKOU INFRASTRUKTURU	33
5.4.1 BLACKOUT	33
6 ODOLNOST KRITICKÉ INFRASTRUKTURY	34
6.1 HODNOCENÍ ODOLNOSTI KRITICKÉ INFRASTRUKTURY	35
6.1.1 MODELOVÁNÍ ZMĚN V ČASE – DIFERENCIÁLNÍ ROVNICE	35
7 OCHRANA KRITICKÉ INFRASTRUKTURY V ČR	37
8 PRINCIPY HODNOCENÍ ODOLNOSTI KRITICKÉ INFRASTRUKTURY	39
8.1 SYSTÉMY A METODY PRO HODNOCENÍ A ANALÝZU	41

PRAKTICKÁ ČÁST	44
9 MULTIKRITERIÁLNÍ HODNOCENÍ ODOLNOSTI KRITICKÉ INFRASTRUKTURY.....	45
9.1 KARS.....	45
9.2 APLIKACE METODY KARS PŘI HODNOCENÍ ODOLNOSTI KRITICKÉ INFRASTRUKTURY.....	45
9.2.1 SOUPIS RIZIK	45
9.2.2 SESTAVENÍ TABULKY RIZIK	46
9.2.3 VYPLNĚNÍ TABULKY SOUVZTAŽNOSTI RIZIK	47
9.2.4 VÝPOČET KOEFICIENTŮ AKTIVITY A PASIVITY	48
9.2.5 GRAFICKÉ VYHODNOCENÍ	48
9.2.6 STANOVENÍ HODNOTY RIZIKOVOSTI	49
9.2.7 STANOVENÍ KOEFICIENTU ZÁVISLOSTI	51
9.2.8 STANOVENÍ KOEFICIENTU ROBUSTNOSTI.....	52
9.2.9 VÝPOČET HODNOTY KOEFICIENTU PŘIPRAVENOSTI K_{PR}	56
9.2.10 VÝPOČET HODNOTY ODOLNOSTI PRVKU KRITICKÉ INFRASTRUKTURY	59
10 KŘÍŽÁK.....	61
10.1 MENU.....	61
10.2 R.....	61
10.3 R2.....	62
10.4 A, P.....	62
10.5 HRZI.....	62
10.6 KS.....	62
10.7 KRZ	62
10.8 KSR.....	63
10.9 KPR.....	63
10.10 ODP.....	63
10.11 HELP	63
ZÁVĚR	65
ZÁVĚR V ANGLIČTINĚ.....	66
SEZNAM POUŽITÉ LITERATURY.....	67
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....	69
SEZNAM OBRÁZKŮ	71
SEZNAM TABULEK.....	72
SEZNAM GRAFŮ	73
SEZNAM PŘÍLOH.....	74

ÚVOD

Lidstvo jako takové již od pradávna muselo zápasit o přežití, o záchranu hmotných zdrojů a kulturních hodnot. S postupem času, díky zdokonalování vědy a techniky, ve společnosti vznikly nová rizika a možná ohrožení. Současná společnost je závislá na bezproblémovém chodu řady prvků a služeb.

Problematika kritické infrastruktury si právem zaslouží naši pozornost. Zvyšující se zranitelnost moderní společnosti se stává důležitým tématem jak na úrovni České Republiky, Evropské Unie či v rámci celosvětového měřítka. V rámci zranitelnosti moderní společnosti si musíme začít klást otázky související s ohrožením obyvatelstva, zachováním základních funkcí státu, zvyšováním prevence, připravenosti a zvládnání následků jakékoliv mimořádné události. Téma ochrany proti útokům vůči společnosti je stále aktuální. To dokazuje nedávný teroristický útok na Bostonský maraton, který se stal 15. dubna 2013. Okolo 14:45 lokálního času, cca 12 sekund po sobě, vybuchly v cíli maratonu dvě bomby vyrobené z tlakových hrnců naplněných hřebíky a kuličkami z ložisek. Událost se odehrála u ulice Boylston Street, nedaleko Copley Square.

Z hlediska ochrany KI je důležité provést hodnocení řady jejích vlastností, zejména odolnosti kritické infrastruktury a jejích prvků. Cílem práce je ukázat možnosti a způsoby hodnocení odolnosti prvků kritické infrastruktury s využitím matematických metod, modelování a simulace.

Jak však naznačuje téma, má práce se zabývá především odolností kritické infrastruktury a možnostmi jejího hodnocení. Odolnost je vnímána jako vlastnost systému absorbovat narušení, snášet negativní změny systému a přitom zabezpečit základní funkce, strukturu, identitu a zpětnou vazbu systému. Pro potřeby určení hodnoty odolnosti existuje mnoho způsobů, metod a postupů. Za nejkompexnější nástroj pro identifikaci či kvantifikaci rizik je všeobecně považována analýza rizik, jejíž součástí je výběr vhodné metody pro získání měřitelných ukazatelů. A právě touto cestou se ubírá i má diplomová práce. Jako vhodnou metodu jsem si vybral, na doporučení mého vedoucího pana Ing. Martina Hromady Ph.D., jím vyvíjenou metodiku určování hodnoty odolnosti kritické infrastruktury postavenou na metodě KARS (Kvalitativní analýza rizik s použitím jejich souvztažnosti).

I. TEORETICKÁ ČÁST

1 KRITICKÁ INFRASTRUKTURA

Pojem kritická infrastruktura (KI) byl poprvé použit v americkém článku z roku 1977, který se touto problematikou zajímal. Ochranu KI lze ale datovat již od roku 1962, kdy došlo k tzv. Kubánské krizi. Právě po takto závažné události se začala řešit problematika bezpečnosti telekomunikační sítě. A také se poprvé vyskytla otázka možné zranitelnosti tohoto systému.

Společnost si v průběhu dalších asi pěti let začala postupně uvědomovat svou závislost na určitých službách a zařízeních, které v současné době spadají právě do kategorie KI. Většina z těchto zařízení je zranitelná. To způsobuje nárůst zranitelnosti jako celku. Podle zkušeností jednotlivých států s mimořádnými událostmi, které způsobily narušení KI, se odvíjí i pohled na její ochranu.

Nejvýznamnějším milníkem moderního vnímání problematiky ochrany KI byly události týkající se 11. září 2001. Právě po událostech spojených s tímto datem, teroristickým útokem na světové obchodní centrum v New Yorku, věnovaly Spojené státy americkému výzkumu bezpečnosti výraznou část celkových výdajů. Útok totiž ukázal, že hlavní prioritou pro stát je bezpečný prostor.

1.1 Základní pojmy týkající se kritické infrastruktury

Podle zákona číslo 240/2000 Sb. o krizovém řízení ve znění pozdějších předpisů jsou definovány tyto základní pojmy:

Kritickou infrastrukturou se rozumí prvek kritické infrastruktury nebo systém prvků kritické infrastruktury, narušení, jehož funkce by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu [1].

Prvkem kritické infrastruktury se rozumí zejména stavba, zařízení, prostředek nebo veřejná infrastruktura, určené podle průřezových a odvětvových kritérií. Je-li prvek kritické infrastruktury součástí evropské kritické infrastruktury, považuje se za prvek evropské kritické infrastruktury [1].

Evropskou kritickou infrastrukturou nebo evropskými kritickými infrastrukturami se rozumí kritická infrastruktura nacházející se v členských státech, jejíž narušení nebo zničení by mělo závažný dopad pro nejméně dva členské státy [1].

Ochranou kritické infrastruktury se rozumí všechny činnosti zaměřené na zajištění funkčnosti, nepřetržitosti a celistvosti kritické infrastruktury s cílem zabránit hrozbě, riziku nebo zranitelnosti, zmírnit je a neutralizovat [1].

Subjektem kritické infrastruktury se rozumí provozovatel prvku kritické infrastruktury; jde-li o provozovatele prvku evropské kritické infrastruktury, považuje se tento za subjekt evropské kritické infrastruktury [1].

1.2 Legislativní zdroje

Zákon č. 239/2000 Sb., o integrovaném záchranném systému a o změně některých zákonů, ve znění doplňků

Zákon vymezuje působnost a strukturu integrovaného záchranného systému. Určuje pravomoc, práva a povinnosti právnických a fyzických osob při přípravě na mimořádné události a při záchranných a likvidačních pracích, při ochraně obyvatelstva před, během a po vyhlášení stavu nebezpečí, nouzového stavu, stavu ohrožení státu a válečného stavu, kterým se všeobecně říká krizové stavy [2].

Zákon č. 240/2000 Sb., o krizovém řízení a změně některých zákonů (krizový zákon)

Zákon stanovuje působnost a pravomoc státních orgánů a orgánů územních samosprávných celků, práva a povinnosti právnických a fyzických osob při přípravě na krizové situace, které nesouvisí se zajišťováním obrany České republiky před vnějším napadením, a při jejich řešení [1].

Zákon č. 241/2000 Sb., o hospodářských opatřeních pro krizové stavy a o změně některých souvisejících zákonů

Zákon upravuje přípravu hospodářských opatření pro stav nebezpečí, nouzový stav, stav ohrožení a válečný stav a přijetí hospodářských opatření po vyhlášení krizových stavů. Dále stanoví pravomoc vlády a správních úřadů, práva a povinnosti fyzických a právnických osob při přípravě a přijetí hospodářských opatření pro krizové stavy [3].

Zákon č. 237/2000 Sb., kterým se mění zákon č. 133/1985 Sb., o požární ochraně ve znění pozdějších předpisů

Tento zákon stanoví podmínky pro účinnou ochranu života a zdraví občanů, majetku před požáry, pro poskytování pomoci při živelních pohromách a jiných mimořádných

událostech stanovením povinností ministerstev a jiných správních úřadů, právnických a fyzických osob [4].

2008/114/ES

Směrnice rady EPCIP o identifikaci a označení evropských prvků KI a zhodnocení potřeby zlepšit jejich ochranu. Tento dokument definuje prvek kritické infrastruktury a evropskou kritickou infrastrukturu. Význam je především v souvislosti se stanovením kritérií pro sektory energetika a doprava, které jsou použitelné i v souvislosti s národní KI. Směrnicí EPCIP se věnuje samostatná kapitola 2.2 Vývoj v Evropě a Evropské unii.

2 VÝVOJ OBORU KRITICKÁ INFRASTRUKTURA

Kritická infrastruktura se vyvíjí již mnoho let. Jde o všeobecný pojem, proto je v různých státech, nebo společenstvech, vnímán rozdílně. To vše je zapříčiněno rozdílným vývojem, odlišným stavem legislativy a různým uvažováním nad možnými riziky.

2.1 Vývoj v České republice

Základní povinností a tedy funkcí státu je ochrana životů obyvatel, zdraví a majetkových hodnot spolu se zajištěním svrchovanosti, územní celistvosti a ochranou demokratických základů ČR. Důležitý je proto komplexní přístup ke zdokonalování opatření v oblasti ochrany životů a zdraví obyvatelstva, základních funkcí státu a ochrany kritické infrastruktury při krizových situacích, respektující vytyčené směry výzkumu EU a NATO. ČR prošla v uplynulých letech výraznými změnami v oblasti bezpečnostních hrozeb a rizik. Zapojením do struktur Evropské unie a Atlantické aliance bylo nezbytné vytvořit zcela novou bezpečnostní politiku státu, a to jak v oblasti vnější, tak i vnitřní bezpečnosti. Uvedené skutečnosti byly zohledněny v *Bezpečnostní strategii a Prioritách bezpečnostní politiky v oblasti veřejného pořádku a vnitřní bezpečnosti*. V současné době je ČR zapojena do všech bezpečnostních struktur Evropské unie a Atlantické aliance a to na všech úrovních.

2.1.1 Vývoj před rokem 1989

Během existence Československé socialistické republiky nebyla kritická infrastruktura neznámý pojem. Již od 80. let 20. století byla hlavním cílem ochrany především potřeba zvýšení odolnosti objektů národního hospodářství. Prioritou byla ochrana proti účinkům zbraní hromadného ničení. Avšak v této době se již nepohlíželo na hodnocení zranitelnosti kritické infrastruktury jenom z důvodu účinků zbraní hromadného ničení. V příslušných platných pokynech z této doby bylo uvedeno, že při hodnocení zranitelnosti kritické infrastruktury je třeba brát mimo jiné v úvahu i rizika živelných pohrom a provozních havárií [5].

2.1.2 Vývoj po roce 1989

1998 – 10. června je ustanoven *Výbor pro civilní nouzové plánování (VCNP)*. Ten se později stane jedním z klíčových výborů *Bezpečnostní rady státu (BRS)* v oblasti ochrany KI.

2000 – Probíhá první činnost týkající se ochrany KI. Jedná se usnesení BRS č. 123 z roku 2000, týkající se ochrany počítačových sítí. V souvislosti s tímto usnesením je zpracován projekt *Strategie výstavby informačních systémů na podporu krizového plánování a řízení ve státní správě*.

Vláda v témže roce také vydává **Zákon č. 240/2000 Sb., o krizovém řízení (krizový zákon)**. Ten stanoví působnost a pravomoc státních orgánů a orgánů územních samosprávných celků a práva a povinnosti právnických a fyzických osob při přípravě na krizové situace, které nesouvisejí se zajišťováním obrany České republiky před vnějším napadením, a při jejich řešení a při ochraně KI a odpovědnost za porušení těchto povinností. [6].

2001 – BRS projednává projekt *Informace ke zpracování definice a stanovení rozsahu základních funkcí státu za krizových situací*. Tento dokument definuje základní funkce státu, které je třeba zachovat během krizové události. Dále je prováděn výzkum a analýza týkající se povodní v letech 1997 a 1998 a také čerpá ze zahraniční literatury. Tato analýza vede ke zpracování materiálu, jenž se týká ochrany KI [7].

2002 – Otázkami KI se začíná zabývat VCNP. 17. září 2002 projednává tento výbor usnesení *Rozsah základních funkcí státu za krizových situací* a materiál *Zpráva o národní kritické infrastruktuře a návrh zásad na její zabezpečení*.

Podle těchto dokumentů se pod pojmem KI rozumí „povinnost vlády zabezpečit chování kontinuity hospodářského a sociálního života a zasáhnout, jestliže by měly být ohroženy elementární potřeby“. Oblasti pak tvoří systém dodávek energií (především elektřina), systém dodávek vody, systém odpadového hospodářství, přepravní síť, komunikační a informační systémy, bankovní a finanční sektor, nouzové služby (policie, hasičské záchranné sbory a zdravotnictví), veřejné služby (zásobování potravinami, sociální služby a pohřební služby), státní správa a samospráva [8].

2003 – V červnu je vydán dokument s názvem *Analýza zabezpečení základních funkcí státu a prvků kritické infrastruktury v ČR za krizových situací*. Tento dokument představuje ucelený a souhrnný soupis situace ve všech odvětvích KI. Obsahuje 3 fáze:

- Informace o jednotlivých oblastech včetně právních dokumentů.
- Přehled subjektů KI (rozčleněn na tři části – subjekty KI s celostátním, regionálním a s lokálním významem).

- Zajištění vzájemných vazeb a závislostí.

2004 – Usnesením č. 191 ze dne 22. června je na 24. schůzi VCNP bylo schváleno 10 oblastí KI ČR. Ty tvoří základní stavební kámen pro odborné posuzování v rámci působnosti příslušných ministerstev a dalších správních úřadů a pro řádné zpracování popisu zranitelnosti systému v každé z uvedených oblastí podle jednotlivého druhu ohrožení. Tyto oblasti jsou uvedeny v příloze č. 1 [9].

*Vzhledem ke vstupu České republiky do Evropské unie v roce 2004, souvisí další dokumenty, závazné pro Českou republiku s ustanoveními a nařízeními Evropské unie, která jsou závazná pro všechny členské státy Evropské unie. Nejdůležitějším dokumentem v oblasti kritické infrastruktury v rámci Evropské unie je **Zelená kniha o Evropském programu na ochranu kritické infrastruktury** z roku 2005.*

2006 – V tomto roce je vydáno usnesení VCNP č. 222/2006 - *Zpráva o stavu řešení problematiky kritické infrastruktury*. Jedná se o první český dokument, který srovnává Českou republiku a zahraničí v oblasti ochrany KI.

2007 - BRS vydává usnesení č. 30/2007 ke *Zprávě o řešení problematiky kritické infrastruktury v České republice*. V tomto dokumentu je také poprvé stanovena definice kritické infrastruktury.

„Kritickou infrastrukturou se rozumí výrobní a nevýrobní systémy a služby, jejichž nefunkčnost by měla závažný dopad na bezpečnost státu, ekonomiku, veřejnou správu a zabezpečení základních životních potřeb obyvatelstva.“ [10]

2.2 Vývoj v Evropě a Evropské Unii



Obrázek 1. Vlajka EU

Prvními státy, které začaly řešit otázku kritické infrastruktury, byly Velká Británie a Německo. V roce 1999 je ve Velké Británii ustanoveno *Koordinační centrum pro bezpečnost národní infrastruktury (CPNI - Centre for the Protection of National Infrastructure)*. Ve Spolkové Republice Německo je v témže roce schválen dokument s názvem *Informačně technické ohrožení klíčových infrastruktur v Německu*. Ten se stává základním kamenem pro další rozvoj ochrany kritické infrastruktury v Německu.

V rámci Evropské unie se téma ochrany evropské kritické infrastruktury (EKI) poprvé objevuje mnohem později. Stejně jako v USA, tak i v EU existují milníky moderního vnímání ochrany kritické infrastruktury. Jsou jimi:

- Série narušení dodávek elektrické energie (tzv. blackouty) v některých státech Evropy způsobené přírodními katastrofami v letech 2003 (Dánsko, Švédsko, Itálie) a 2004 (Řecko).
- Teroristické útoky v Londýně dne 7. července 2005, kdy došlo k útoku na dopravní prostředky během ranní dopravní špičky.
- Teroristický útok v Madridu 11. března 2004, kdy došlo k útoku na vlakovou soupravu.

Evropská rada na svém zasedání v červnu 2004 požádala Komisi evropských společenství o přípravu celkové strategie na ochranu kritické infrastruktury. Komise na základě toho přijala 20. října 2004 sdělení *„Ochrana kritické infrastruktury v boji proti terorismu“*, v kterém předložila jasné návrhy, jak by se v EU měla zlepšit prevence, připravenost a schopnost reakce na teroristické útoky zasahující kritickou infrastrukturu. Rada ve svých závěrech nazvaných *„Předcházení, připravenost a reakce na teroristické útoky“* a

„Program solidarity EU o následcích teroristických hrozeb a útoků“ přijatých na zasedání Rady v prosinci 2004, podpořila záměr Komise předložit *Evropský program na ochranu kritické infrastruktury (EPCIP)* a souhlasila, aby Komise zřídila *Výstražnou informační síť kritické infrastruktury (CIWIN)* [11].

2.2.1 Základní principy EPCIP

Subsidiarita – základem EPCIP by měl být princip subsidiarity, kdy ochrana kritické infrastruktury je v odpovědnosti subjektů především na národní úrovni. Hlavní odpovědnost za ochranu kritické infrastruktury by spadala pod členské státy a vlastníky/provozovatele jednající ve společném rámci. Komise by se naopak zaměřila na aspekty spojené s ochranou KI s přeshraničním dosahem v rámci EU. Odpovědnost za rozhodnutí a plány na ochranu vlastního majetku by měla zůstat na vlastnících a provozovatelích.

Doplňkovost – společný rámec EPCIP by doplňoval již existující opatření. Zavedené komunitární mechanismy by měly být nadále využívány, aby přispívaly k zajištění celkové implementace EPCIP.

Důvěrnost – sdílení informací o ochraně kritické infrastruktury by zůstalo zachováno v důvěrném prostředí. To je nezbytné zejména proto, že konkrétní údaje o kritické infrastruktuře by mohly být zneužity a způsobit tak její selhání nebo jiné nepříjemné důsledky. Informace o ochraně kritické infrastruktury by byly jak na úrovni EU, tak na úrovni členských států utajovány a přístup k nim by byl povolen jen v potřebných případech.

Spolupráce zainteresovaných subjektů – svou roli při ochraně KI mají všechny zainteresované subjekty včetně členských států, Komise, průmyslových/obchodních sdružení, normalizačních orgánů, vlastníků, provozovatelů a uživatelů („uživatel“ je definován jako organizace užívající danou infrastrukturu pro obchodní účely a pro poskytování služeb). Všichni by měli v rámci své odpovědnosti a specifické úlohy spolupracovat a přispívat tak k rozvoji a implementaci EPCIP. Vůdčí a koordinační úlohu při rozvoji a implementaci přístupu při ochraně KI v rámci daného území, by měly orgány členských států. Takový přístup by měl být vždy konzistentní v celostátním měřítku. Vlastníci, provozovatelé a uživatelé by byli aktivně zapojeni jak na národní úrovni, tak na úrovni EU. Tam, kde neexistují odvětvové normy nebo ještě nebyly zavedeny normy mezinárodní, mohou normalizační orgány přijmout vhodné společné normy.

Proporcionalita – vzhledem k tomu, že by nebylo opodstatněné chránit veškerou infrastrukturu před všemi hrozbami (např. rozvodné sítě elektrické energie jsou příliš rozsáhlé na to, aby je bylo možné oplotit nebo hlídat), měly by být ochranné strategie a opatření úměrné úrovni daného nebezpečí. S pomocí vhodných technik řízení rizik lze soustředit pozornost na nejrizikovější oblasti, přičemž je nutno brát v úvahu danou hrozbu, její relativní význam pro infrastrukturu, poměr nákladů a výnosů, stávající úroveň bezpečnostní ochrany a účinnost dostupných zmírňujících strategií [11].

2.2.2 Cíle EPCIP

Cílem EPCIP je zajistit, aby v rámci celé Evropské unie existovala přiměřená a rovnoměrná úroveň bezpečnostní ochrany kritické infrastruktury, co nejméně možnosti selhání a rychlá, vyzkoušená nápravná opatření. Úroveň ochrany by neměla být stejná pro všechny, ale měla by být odvozená od dopadu, jenž by mohl způsobit jejich možné selhání. EPCIP by měl co nejvíce minimalizovat veškeré negativní dopady, které zvýšené investice na ochranu mohou mít na konkurenceschopnost příslušného odvětví. Při výpočtu přiměřenosti nákladů nesmíme opomíjet potřebu udržovat stabilitu trhů, která je rozhodující zejména u dlouhodobého investování, ani vliv, jenž taková ochrana má na vývoj akciových trhů a na makroekonomické prostředí [11].

2.2.3 Definice a oblasti evropské kritické infrastruktury

EKI by měla zahrnovat takové materiální zdroje, služby, zařízení informačních technologií, sítě a majetek, které mají v případě narušení nebo zničení vážný dopad na zdraví, bezpečnost, zabezpečení, hospodářský nebo sociální blahobyt ve:

- (a) dvou a více členských státech – včetně některé kritické infrastruktury bilaterální povahy (podle potřeby);
- (b) třech a více členských státech – kromě veškeré kritické infrastruktury bilaterální povahy [11].

Oblasti evropské kritické infrastruktury jsou uvedeny v příloze č. 2.

2.3 Vývoj v rámci Severoatlantické aliance



Obrázek 2. Vlajka NATO

V České republice má kromě EU na vývoj a řešení ochrany kritické infrastruktury vliv také společenství států v rámci Severoatlantické aliance. Zájem NATO o ochranu kritické infrastruktury se datuje od roku 2001. Od tohoto roku jsou postupně sloučeny některé z politických dokumentů a programů. Některé z orgánů NATO se začíná zabývat problematikou ochrany kritické infrastruktury koordinovaným způsobem.

V roce 2003 byl pro řešení této problematiky zřízen *Hlavní výbor pro civilní nouzové plánování (Senior Civil Emergency Planning Committee SCEPC)*. Ten se stal seniorním poradním výborem Severoatlantické rady, řídicího orgánu NATO, v oblasti civilního nouzového plánování. Existuje zde osm podřízených plánovacích výborů, na které Hlavní výbor dohlíží a koordinuje je.

V roce 2004 se hlavy států a předsedové vlád dohodli na programu *Plánu na obranu proti terorismu (Programme of Work on defence Against Terrorism)*, jehož cílem je podporovat rozvoj špičkových technologií pro ochranu vojenských prostředků a vojáků. KI je jedním z deseti priorit programu, a je veden v Belgii.

Při civilním pohledu na nouzové plánování, role NATO nespočívá na regulačním přístupu. Alianční programy jsou spíše zaměřeny na budování dovedností a schopností, podporou správy a odolnost v oblasti civilního nouzového plánování, se zaměřením na zvládání následků. Hlavním cílem je podpořit vnitrostátní plány podporou vyšších standardů připravenosti a lepší interoperability v zvládání následků. Prostřednictvím *Akčního plánu civilního nouzového plánování (Civil Emergency Planning Action Plan)* NATO rozšiřuje tuto podporu do svých 49 partnerských zemí.

NATO nedávno vyvinula zvláštní důraz na energetickou bezpečnost, která zahrnuje jak bezpečnost dodávek, tak i infrastrukturu zabezpečení. Na summitu v Rize, se vedení států a vlád vyslovila pro "koordinované, mezinárodní úsilí pro posouzení rizika energetické infrastruktury a podporu zabezpečení energetické infrastruktury „ Severoatlantická rada byla pověřena "definovat oblasti, kde NATO může zvýšit hodnotu ochrany bezpečnostních zájmů spojenců a na požádání pomoci vnitrostátním a mezinárodním úsilím" [12].

2.4 Vývoj ve Spojených státech amerických



Obrázek 3. Vlajka USA

Spojené státy americké byly jedny z prvních států, které si hrozbu zranitelnosti KI začaly uvědomovat. Proto byla již v roce 1996 prezidentem Billem Clintonem zřízena Komise pro ochranu kritické infrastruktury (*President's Commission on Critical Infrastructure Protection – PCCIP*). Tato nově zřízená komise měla za úkol právě výzkum závislosti americké populace na KI. Později, v říjnu 1997, vydala Komise zprávu, z které vyplývá nutnost zajištění ochrany kritické infrastruktury USA v důležitých oblastech, jakými jsou např. bankovníctví a finance, telekomunikace a doprava. Na základě této zprávy vznikají v květnu 1998 první dva ucelené dokumenty týkající se ochrany KI.

První z dvou směrnic je *PDD-62 (Prezidentské rozhodnutí - Presidential Decision Directive)*, týkající se boje proti terorismu. Tato směrnice vytváří nový a systematický přístup k boji proti teroristické hrozbě. Posiluje práva mnoha amerických agentur zaměřených naproti teroristickou činností. Dále také objasňuje jejich činnost v široké škále programů amerických protiteroristických programů, z dopadení a stíhání teroristů, zvýšení dopravní bezpečnosti, posílení schopnosti reakce a ochrany počítačových systémů, které leží v srdci amerického hospodářství. Směrnice pomáhá dosáhnout prezidentův cíl a zajistit, že bude jednáno s hrozbou terorismu v 21. století se stejnou silou a razancí [13].

Druhou důležitou směrnicí je *PDD-63*, tzv. „*Bílá kniha*.“ Směrnice 63 je vyvrcholením intenzivního, mezirezortního úsilí k hodnocení KI a vytvoření funkčního a inovativního

rámce pro ochranu kritické infrastruktury. Cílem této směrnice bylo tedy ochránit národní kritickou infrastrukturu před všemi hrozbami, včetně počítačových útoků. Zařazuje také ochranu KI na úroveň národního zájmu [14].



Obrázek 4. Útok na WTC

Po teroristickém útoku na WTC 11. září 2001 se však vše mění. Po tomto útoku začínají USA věnovat značnou část svých prostředků do oblasti ochrany KI. Útok totiž ukázal na důležitost bezpečného prostoru v rámci státu.

Bezprostředně po událostech 11. září využívá George. W. Bush svých prezidentských pravomocí a vytváří nové úřady, zabývající se vnitřní bezpečností státu. Tím nejdůležitějším je *Úřad pro vnitřní bezpečnost (Office of Homeland Security)* založený 8. října 2001. Dále také dne 16. října 2001 podepisuje *Vládní nařízení na ochranu kritické infrastruktury (Executive Order on Critical Infrastructure Protection)* „na ochranu proti narušení provozu informačních systémů pro kritické infrastruktury, a aby zajistily, že jakákoli narušení, která se objevují, jsou minimální doby trvání a zvládnutelné, a aby vzniklo co nejméně možné škody.“ Tato vyhláška také zakládá Prezidentskou radu pro ochranu kritické infrastruktury. Rada, skládající se z federálních úředníků, je oprávněna doporučit politiku ochrany KI a koordinaci programů ochrany KI. Rada byla také zaměřena na návrh Národního plánu ochrany KI ve spolupráci s Úřadem pro vnitřní bezpečnost [15].

2.4.1 Department of Homeland Security



Obrázek 5. Znak Úřadu pro vnitřní bezpečnost

Dne 14. listopadu 2002 Sněmovna reprezentantů a 20. listopadu 2002 Senát Kongresu USA schválili zákon o vytvoření *Ministerstva vnitřní bezpečnosti (Department of Homeland Security - DHS)*. Prezident George W. Bush zákon podepsal 25. Listopadu 2002. Jeho hlavním úkolem je chránit území USA před jakoukoliv hrozbou terorismu a reagovat na přírodní katastrofy [15].

Oficiálně jsou předkládány tyto strategické cíle rezortu:

- předcházení teroristickým útokům na území USA;
- snížení zranitelnosti země před terorismem;
- minimalizace dopadu útoků, které již nastanou.

Další úkoly

- posílení bezpečnosti civilní letecké dopravy;
- *ochrana kritické infrastruktury;*
- snaha snížit riziko chemického, biologického či jaderného útoku na teritoriu USA;
- boj proti pašování drog na území USA;
- naturalizační a imigrační agenda;
- výcvik specializovaných složek i nejšířší veřejnosti v zájmu zvládnutí základů civilní ochrany;
- výzkumná činnost;

- zajišťování týlového materiálního zabezpečení pro jiné agentury, zabývající se ochranou vnitřní bezpečnosti USA;
- další úkoly, které rezortu udělí prezident [15].

2.4.2 rozdělení odpovědnosti za kritickou infrastrukturu v rámci USA

- vláda (všechny rezorty),
- zemědělství (Ministerstvo zemědělství),
- potraviny (Ministerstvo zemědělství a Ministerstvo zdravotnictví),
- pitná voda (Agentura na ochranu životního prostředí / EPA – Environment Protection Agency)
- veřejný zdravotnický sektor (Ministerstvo zdravotnictví),
- základny obranného průmyslu (Ministerstvo obrany),
- informační a telekomunikační oblast (HLS),
- energetika, rozvodná síť (Ministerstvo energetiky),
- doprava (HLS a Ministerstvo dopravy),
- chemická výroba (EPA),
- poštovní a doručovací služby (HLS),
- národní památníky (Ministerstvo vnitra) [15].

3 VÝZNAM KRITICKÉ INFRASTRUKTURY

Moderní společnost je závislá na dobře fungující KI. Především však na technologické infrastruktuře, která zajišťuje veškeré dodávky vody a potravin, elektřiny a tepla apod. Jakékoli selhání této infrastruktury by mělo neblahý důsledek na obyvatelstvo, na naplnění základních lidských potřeb a kvalitu lidského života. Technologická infrastruktura spolu s infrastrukturou řízení státu tvoří infrastrukturu společnosti, kterou můžeme charakterizovat následovně: [16]

- V současnosti je lidská společnost naprosto závislá na normálním a neměnném průběhu operací technologické infrastruktury (produkty a služby) a infrastruktury státu (veřejné služby). Tato závislost však přináší sníženou odolnost vůči jakýmkoliv nepříznivým vlivům.
- Jednotlivé infrastruktury společnosti jsou vzájemně provázané, což zvyšuje jejich složitost a vnímavost vůči poruchám. Tato vlastnost se nazývá *konektivita*.
- Ke snižování zranitelnosti KI je potřeba vynaložit značné finanční prostředky, kterých je nedostatek.
- Deregulace infrastrukturu rozdělila mezi různé vlastníky (státní i soukromé).
- Civilizované prostředí, jako forma technologické infrastruktury, se snaží přebírat některé funkce za přírodu. Proto se stále více musíme chránit proti vlivům prostředí, v němž žijeme.
- Každá infrastruktura poskytující produkty či služby využívá prostředky informačních technologií, což vede k centralizaci řízení a poklesu odolnosti digitálních systémů vůči poruchám [16].

Ze společenského hlediska se KI rozumí vzájemně propojené sítě či systémy, které obsahují identifikovatelná odvětví a instituce a poskytují spolehlivý tok produktů a služeb důležitých pro obranu a ekonomickou bezpečnost. Tato bezpečnost je chápána jako schopnost státu konkurovat na globálních trzích, zatímco se udržují na přijatelné úrovni reálné příjmy obyvatel a fungování veřejné správy na všech úrovních společnosti.

Kromě ekonomické bezpečnosti rozlišujeme:

- bezpečnost fyzickou, která se týká ochrany fyzických zařízení před škodami v důsledku působení fyzických sil.

- Bezpečnost kybernetickou, která se zabývá především ochranou před poruchami nebo neautorizovanými přístupy do počítačových sítí.

Kromě zachování životů a státu je tedy také důležité zachování běžného provozu společnosti [16].

Obecně se infrastruktura společnosti skládá z ekonomické, sociální a „nehmotné“ infrastruktury:

- Ekonomická infrastruktura obsahuje fyzická zařízení komunikační, dopravní, energetické a vodní sítě a dále obsahuje všechny typy budov, přehrady, továrny.
- Sociální infrastruktura zahrnuje fyzická zařízení jako školy, nemocnice, vězení, historické budovy, kostely, obchodní centra, stadiony, parky, muzea atd.
- Nehmotná infrastruktura se skládá z nehmotných aktiv vyjadřujících schopnosti a zdravotní stav komunity a její produktivní vlastnosti.

Prostřednictvím vybraných prvků společenské infrastruktury se uskutečňuje proces řízení společnosti [16].

4 PRVKY KRITICKÉ INFRASTRUKTURY



Obrázek 6. Prvky kritické infrastruktury

Prvky kritické infrastruktury jsou základním stavebním kamenem kritické infrastruktury. Jsou rozděleny do deseti oblastí a čtyřiceti čtyř produktů a služeb, viz příloha č. 1.

„Prvkem kritické infrastruktury je zejména stavba, zařízení, prostředek nebo veřejná infrastruktura, určené podle průřezových a odvětvových kritérií (je-li prvek kritické infrastruktury součástí evropské kritické infrastruktury, považuje se za prvek evropské kritické infrastruktury). Tato kritéria jsou obsažena v nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury [17].“

4.1 Proces určování prvků kritické infrastruktury

Prvky KI, jejichž provozovatelem je organizační složka státu (dále jen „OSS“):

- ministerstva a ústřední správní úřady a ČNB zasílají Ministerstvu vnitra návrhy prvků KI a EKI, jejichž provozovatelem je OSS (§ 9 odst. 3 písm. d) a §13 odst. 4 písm. c) krizového zákona),
- Ministerstvo vnitra zpracuje seznam, který je podkladem pro určení prvků KI a EKI, jejichž provozovatelem je OSS (§ 10 odst. 1 písm. f) krizového zákona),

- vláda usnesením určí prvky KI a EKI, jejichž provozovatelem je OSS (§ 4 odst. 1 písm. e) krizového zákona).

Prvky KI, které nejsou určovány podle § 4 odst. 1 písm. e) krizového zákona (jejichž provozovatelem není OSS):

- ministerstva a ústřední správní úřady a ČNB určí opatřením obecné povahy prvky KI a EKI,
- o tomto určení informují bez zbytečného odkladu Ministerstvo vnitra [17].

4.2 Zdravotní péče



Obrázek 7. Zdravotní péče [18]

Zdravotnickou KI tvoří zejména zdravotnická zařízení neodkladné péče, resortní organizace zdravotnické logistiky a další účelová zařízení nutná k zajištění nezbytné zdravotní péče.

Zajištění správného fungování KI zdravotnictví pro poskytnutí zdravotní péče je při mimořádných událostech a krizových situacích jedna z priorit. Při většině situací, které ohrožují správné fungování společnosti, mohou vzniknout zranění. Jako možná nebezpečí, která mohou narušit plynulý chod nemocnice, lze uvést například výpadek proudu, povodně (poškození budovy, zvýšený počet pacientů), epidemie nebo požár.

Navzdory tomu, že zdravotnictví nemá v ČR prvek KI, má mezi sektory KI velký význam, protože při neštěstích a katastrofách přebírá důležité úkoly: Musí zajistit lékařskou péči o značně vyšší počet pacientů než v běžné situaci. Výpadek tohoto sektoru by měl významný dopad na celou společnost.

4.2.1 Přednemocniční neodkladná péče



Obrázek 8. Přednemocniční neodkladná péče [18]

Přednemocniční neodkladná péče se provádí na místě úrazu nebo během transportu postižené osoby. Je poskytována v případech, kdy je bezprostředně ohrožen život pacienta. Zahrnuje zdravotní záchrannou službu (včetně letecké) a nezbytné transportní kapacity pro dopravu zraněných z místa nehody

4.2.2 Nemocniční péče



Obrázek 9. Nemocniční péče [18]

V ČR je nemocniční péče poskytována sítí nemocnic a lékařských zařízení. Každá nemocnice poskytuje komplex služeb lůžkové, ambulantní a komplementární péče. Součástí nemocnice jsou lůžková oddělení, specializovaný ambulantní provoz, technické zázemí, management (vedení), lékárny a výdejny pomůcek.

4.2.3 Ochrana veřejného zdraví



Obrázek 10. Ochrana veřejného zdraví [18]

Ochrana a podpora veřejného zdraví je souhrn činností opatření k vytváření a ochraně zdravých životních a pracovních podmínek a zabránění šíření infekčních a hromadně se vyskytujících onemocnění, ohrožení zdraví v souvislosti s vykonávanou prací, vzniku nemocí souvisejících s prací a jiných významných poruch zdraví a dozoru nad jejich zachováním. Opírá se o zákon č.258/2000, o ochraně veřejného zdraví a o změně některých souvisejících zákonů.

4.2.4 Výroba, skladování a distribuce léčiv a zdravotnických prostředků



Obrázek 11. Výroba, skladování a distribuce léčiv a zdravotnických prostředků [18]

Výroba, skladování a distribuce léčiv a zdravotnických prostředků v České republice mají na starosti především podnikající právnické a fyzické osoby. Podle zákona č. 240/2000 Sb., o krizovém řízení jsou stanoveny dodávky potřebné v případě krizových stavů.

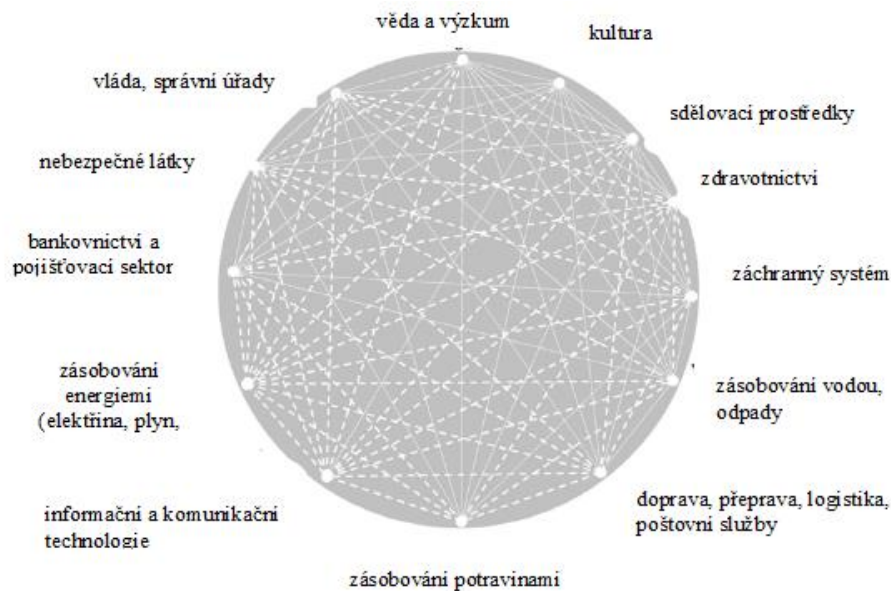
5 OHROŽENÍ KRITICKÉ INFRASTRUKTURY

Narušení, poškození nebo zničení jakéhokoliv prvku kritické infrastruktury je možno způsobit přírodními katastrofami, selháním techniky anebo selháním technologických postupů, jakož i příznivým či nepříznivým vlivem člověka, včetně terorismu a organizovaného zločinu.

5.1 Kritická infrastruktura jako komplexní systém

Na problematiku v oblasti kritické infrastruktury musíme nahlížet jako a komplexní systém. KI se skládá ze samostatných prvků a sítě spojnic, které mají síťové uspořádání. Tyto jednotlivé prvky jsou vzájemně provázány. Podobně jako v klasické síti, tak i zde lze najít místa, kde se nachází více prvků spojnic. Ty tvoří uzly. Z tohoto důvodu jakékoliv narušení, poškození nebo zničení některého z těchto uzlů může mít závažný dopad na funkčnost dalších uzlů. Takovýto výpadek by mohl dominovým efektem způsobit následné zhroucení celé sítě. Z tohoto důvodu je v zájmu ochrany KI takovéto uzly chránit.

5.2 Propojitelnost kritické infrastruktury



Obrázek 12. Propojitelnost prvků kritické infrastruktury [18]

Propojitelnost (konektivita) je charakteristická závislost mezi dvěma a více infrastrukturami. Prostřednictvím tohoto spojení událost vzniklá v rámci jednoho prvku může ovlivnit stav jiné infrastruktury, např. závislost na elektrické energii. Závislost se

také týká infrastrukturu jako celku. To znamená, že na sobě mohou být závislé i celé infrastruktury. Tato vzájemná závislost může být *územní, kybernetická, logická anebo fyzická* [19]. Přitom platí

- Mezi infrastrukturou existuje *fyzická závislost*, jestliže výstup jedné infrastruktury je přímo závislý na stavu druhé. Např. závislost nemocniční péče na dodávce energie.
- Pokud stav jedné infrastruktury závisí na informacích z druhé, jedná se o *kybernetickou závislost*. Např. závislost vodního hospodářství na předpovědi počasí.
- Jestliže událost vzniklá na daném území může měnit stav více prvku infrastruktury, jedná se *územní závislost*. Např. povodně.
- Jestliže stav jedné infrastruktury přímo závisí na stavu jiné a přitom se nejedná ani o jednu z výše uvedených typů závislosti, pak se jedná o *logickou závislost*. Např. závislosti přenášené pomocí finančních toků [19].

Právě díky těmto vzájemným propojením může stav jednoho prvku infrastruktury ovlivnit jiný prvek.

5.3 Kritičnost kritické infrastruktury

Kritičnost lze v souvislosti s KI definovat jako „relativní míru dopadů četnosti výskytu poruch a selhání.“ Určení kritičnosti infrastruktury tedy vyplývá z velikosti dopadů narušení funkčního stavu KI na společnost.

Kritičností se tedy myslí relativní význam jednoho prvku KI ve vztahu k následkům, které by mělo narušení nebo přerušení činnosti tohoto prvku pro plynulou činnost celého systému, a tím i dopad na obyvatelstvo. Riziko může vzniknout jak v samotném prvku nebo může být ohroženo vlivem jiného prvku.

Stanovení kritičnosti může být popsána následovně:

- Charakteristika zařízení (fyzická, kybernetická a lidská).
- Stanovení kritičnosti (analýza ohrožení od pohrom a zvážení zranitelností).
- Hodnocení dopadů na zařízení (koncentrace lidí a zařízení, ekonomické dopady,
- vzájemné závislosti, spolehlivost).

- Hodnocení důsledků ztrát, obětí, škod a poškození zařízení.
- Priorizace zařízení podle zadaných pravidel.

Jedním z možných způsobů hodnocení kritičnosti je například matice kritičnosti, kdy je však potřeba znát pravděpodobnost výskytu události a její dopad.

5.4 Hrozby ohrožující kritickou infrastrukturu

Jedná se především o hrozby mající negativní vliv na bezpečnost a ochranu KI, stanovení její zranitelnosti a stanovení odolnosti KI. Použití pojmu hrozba je často spojené s konkrétním jevem, procesem či událostí, která svou přítomností vytváří nebezpečí.

Vliv na bezpečnost a funkčnost KI mohou mít například dlouhodobá inverzní oblačnost, povodně, rozsáhlé lesní požáry, sněhová kalamita, sesuv půdy, zemětřesení, dlouhotrvající sucho a teplo, extrémní teploty, vichřice, vánice, epidemie, epifytie, epizootie, radiační havárie, havárie způsobené chemickými látkami, technické havárie, narušení hrází, terorismus, narušení finančního a devizového hospodářství, narušení dodávek elektrické energie (tzv. blackout), narušení dodávky ropy a ropných produktů a jiné.

5.4.1 Blackout

Po výpadku elektřiny (blackoutu) nastupuje velice rychle chaos. Už po pár hodinách nejde prakticky nic. Okamžitě přestane fungovat průmysl, kolejová doprava, internet, pevné a mobilní sítě. Brzy následují dodávky vody, čerpací stanice pohonných hmot a posléze se zastaví vozy policie a hasičů a vyčerpají se záložní zdroje pro provoz úředních komunikačních sítí.

Jedno z nejzávažnějších a tedy nejkritičtějších ohrožení správného fungování kritické infrastruktury je tedy výpadek zásobování elektřinou velkého rozsahu. Příčinou je právě vzájemná závislost (propojitelnost) prvků KI, která může vyvolat dominový efekt šíření krizových situací. Případy důsledků déletrvajících výpadků jsou známy ze zahraničí. Například 14. 8. 2003 došlo na severovýchodě USA a v Kanadě k dvoudennímu výpadku elektřiny způsobeným zkratem při kontaktu vodiče venkovního vedení el. proudu se stromem. Toto krátkodobé přetížení vyvolalo kaskádové šíření poruchy a ta posléze vyřadila 256 elektráren. Tento výpadek zasáhl sedm amerických států a v Kanadě provincii Ontario a města Toronto a Ottawu, tedy zhruba 15.000 kilometrů čtverečních, a 50 až 60 milionů osob. Kolaps provázelo také rabování a vyžádal si tři lidské oběti.

6 ODOLNOST KRITICKÉ INFRASTRUKTURY

Odolnost je definována ve slovníku jako *"schopnost a vlastnost hmoty odolávat vnějším vlivům a účinkům prostředí."* Definice se v případě může KI mírně lišit, ale všechny definice mají podobný, ne-li stejný význam. Schopnost odolávat vůči fyzické zátěži. Obecně lze odolnost KI považovat za schopnost zajistit funkci systému, působí-li na systém vnější nebo vnitřní nepříznivé vlivy. Odolný systém tedy i přes vliv těchto sil plní nadále svou předepsanou funkci.

Odolnost je tedy vnímána jako vlastnost systému absorbovat narušení, snášet negativní změny systému a přitom zabezpečit základní funkce, strukturu, identitu a zpětnou vazbu systému.

V dnešní době však nemůžeme odolnost vnímat pouze jako odolnost fyzickou, ale také sociální. Vzhledem k tomu, že důležité prvky KI jsou úzce spjaty s hospodářstvím, bezpečností a strukturou společnosti, tak schopnost odolávat nepříznivým vlivům souvisí s jistou „komunitní odolností“ [20].

Odolnost jak pro fyzické, tak pro sociální systémy má čtyři důležité vlastnosti:

- Robustnost – vlastní síla nebo odolnost systému umožňující odolávat vnějším vlivům bez zhoršení nebo ztráty funkcionality. Do této kategorie spadá jak využití prvků ochrany KI (fyzická ostraha, technické a technologické zabezpečení, organizační aspekty), tak využití krizového a nouzového plánování.
- Redundanci – možnosti systému využívat alternativní možnosti a zdroje v případě narušení. Nejčastěji se jedná o technické (nouzové generátory) nebo organizační nástroje.
- Reakce schopnost – schopnost mobilizovat potřebné zdroje a služby v případě potřeby. Schopnost využívat inovativních postupů a reagovat na základě dostupných zdrojů na vzniklou situaci.
- Schopnost rychlé reakce – rychlost, s jakou lze reagovat na vzniklou situaci a obnovit funkci systému, nebo alespoň zabezpečit základní funkce [20].

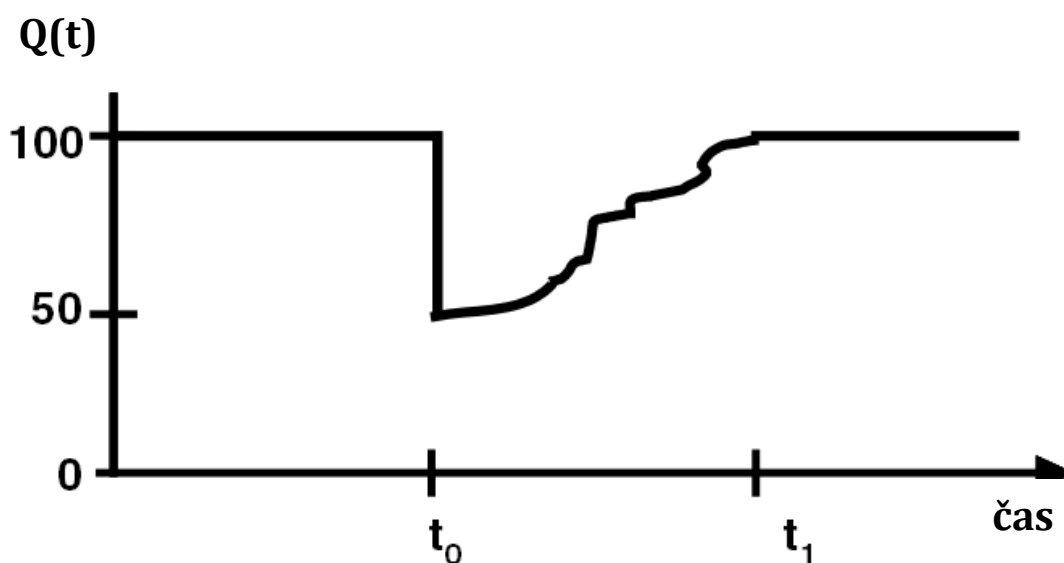
6.1 Hodnocení odolnosti kritické infrastruktury

Hodnocení odolnosti KI je vhodné provádět podle kategorií činitelů, které ovlivňují její funkci. Obecně tyto činitele dělíme na vnější a vnitřní, proto i odolnost KI hodnotíme dvěma rozdílnými ukazateli. Ukazatel, který vyjadřuje odolnost vlivu vnitřních činitelů, představuje spolehlivost systému plnit požadovanou funkci. Spolehlivost odráží především odolnost vůči vlivu technických poruch zařízení a nesprávné činnosti obsluh při zajištění funkce systému. Čím lepší je návrh a konstrukce systému, použitý materiál k výrobě prvků, přesnější výroba a implementace, tím je menší pravděpodobnost, že dojde k vyřazení jeho funkce. Totéž platí i pro kvalitu obslužného personálu.

Ukazatel, který vyjadřuje schopnost plnit funkci v podmínkách působení vnějších činitelů, označujeme jako použitelnost (životnost). Základními vnějšími činiteli, které ovlivňují činnost KI, jsou především živelní pohromy, fyzické útoky, počítačové (informační) útoky, poruchy v dodávce vstupních surovin atd. Aktivita těchto činitelů je na správci systému kritické infrastruktury značně nezávislá [20].

6.1.1 Modelování změn v čase – diferenciální rovnice

Tento způsob hodnocení odolnosti KI patří mezi základní způsoby zobrazení a slouží především k ukázce funkce hodnocení odolnosti KI. V dalších kapitolách se práce věnuje specifitějším způsobům hodnocení.



Graf 1. Kvalita infrastruktury v čase

Jak je znázorněno v grafu 1, kvalita infrastruktury $Q(t)$ se může měnit s časem. Například u budov se může měnit strukturální integrita, která se vyjadřuje v procentech. Při zajištění dodávek elektřiny, plynu a vody může být procentuálně vyjádřen počet zákazníku s funkční dodávkou služeb. Pokud je systém odolný, pak zůstává na 100 procentech. Celková ztrátě služeb je vyjádřena jako 0 procent. Pokud dojde k narušení systému v čase t_0 , například v reakci na živelnou pohromu (povodně, orkán), může dojít k poškození infrastruktury a tedy k snížení kvality poskytovaných služeb. Úroveň služeb, což se odráží v robustnosti systému, je funkcí pravděpodobnosti a důsledku poškození. V čase t_1 se systém opět vrací do své původní kapacity [20].

Ztráta odolnosti R může být měřena jako očekávaná ztráta kvality (pravděpodobnost poruchy) v průběhu času k zotavení, $t_1 - t_0$. Matematicky je R definováno jako:

$$R = \int_{t_0}^{t_1} [100 - Q(t)] dt \quad (1)$$

7 OCHRANA KRITICKÉ INFRASTRUKTURY V ČR

V souvislosti s potřebou řešení problematiky ochrany kritické infrastruktury na národní úrovni a implementací příslušné evropské legislativy do českého právního prostředí byl v roce 2010 zákonem č. 430/2010 Sb. novelizován zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů.

Tato novela mimo jiné upravuje postup při určování prvků kritické národní a evropské infrastruktury a vymezuje povinnosti jejich provozovatelů, tedy subjektů kritické infrastruktury. Mezi tyto povinnosti patří i zpracování plánů krizové připravenosti subjektů kritické infrastruktury.

Subjekt kritické infrastruktury je povinen vypracovat plán krizové připravenosti do jednoho roku od rozhodnutí vlády nebo ode dne nabytí právní moci opatření obecné povahy, kterým byl prvek kritické infrastruktury určen. V plánu krizové připravenosti subjektu KI jsou identifikována možná ohrožení funkce prvku kritické infrastruktury a stanovena opatření na jeho ochranu [21].

Účelem plánu krizové připravenosti subjektu kritické infrastruktury je zejména:

- identifikovat možné zdroje rizik,
- analyzovat možná ohrožení a jejich dopad na funkci prvků kritické infrastruktury,
- popsat a zhodnotit stávající bezpečnostní opatření na ochranu kritické infrastruktury, včetně návrhu na jejich doplnění, optimalizaci a stanovení priorit v této oblasti,
- stanovit scénáře a postupy pro řešení mimořádných událostí a krizových situací k ochraně funkce prvku kritické infrastruktury.

S výše uvedenou problematikou souvisí následující činnosti a služby

- zpracování příslušných analýz, nezbytných pro zpracování plánu krizové připravenosti,
- komplexní zpracování plánu krizové připravenosti subjektů kritické infrastruktury podle NV č. 462/2000 Sb., ve znění pozdějších předpisů,
- součinnost při zajištění implementace opatření na ochranu kritické infrastruktury do systému řízení rizik v organizaci,
- součinnost při ověřování funkčnosti plánu a při jeho aktualizaci,

- součinnost při jednání s příslušnými orgány krizového řízení ohledně zaměření a rozsahu zpracování plánu a dalších souvisejících záležitostí [21].

Způsob zpracování plánu krizové připravenosti lze modifikovat a přizpůsobit konkrétním potřebám subjektu kritické infrastruktury, specifikům daného odvětví nebo oblasti kritické infrastruktury. Vlastní plán je zpracován na základě analýzy a hodnocení rizik a expertního posouzení stávající úrovně bezpečnostních opatření. V případě potřeby je zpracován návrh na jejich případné doplnění a optimalizaci, včetně stanovení priorit [21].

8 PRINCIPY HODNOCENÍ ODOLNOSTI KRITICKÉ INFRASTRUKTURY

Při multikriteriálním hodnocení odolnosti KI, je třeba si připomenout, že odolnost KI je závislá na několika faktorech. Ty jsou na sobě navzájem závislé a ovlivňují tedy celkovou odolnost. Pokud tedy například dojde k dlouhodobému výpadku proudu, může se nám stát, že náš bezpečnostní systém ztratí svou schopnost odhalit pachatele. Stejně tak špatná úroveň fyzické bezpečnosti může zapříčinit nevyužití potenciálu technického zabezpečení. Je třeba uplatnit zde principy kritičnosti a propojitelnosti (viz kapitola 5.2 a 5.3).

Oblasti, které ovlivňují odolnost KI, jsou následující:

- Fyzická a objektová bezpečnost
- Informační bezpečnost
- Řízení kontinuity činnosti organizace
- Administrativní bezpečnost
- Zajištění dostupnosti personálu

Fyzická a objektová bezpečnost

Využití fyzické ostrahy je v kombinaci s organizační a technickou bezpečností nejdůležitějším prvkem ochrany objektu. Zajišťuje ochranu objektu před fyzickou hrozbou nebo narušením plynulého provozu. Jde o velmi významný prvek, který slouží jako podpůrný mechanismus pro ostatní oblasti. Na této oblasti lze předvést právě provázanost jednotlivých systémů. Například informační systém lze zabezpečit kvalitními prostředky, jako jsou firewally a přístupová práva. Avšak pokud stačí útočníkovi přijít k PC, HDD s citlivými daty vyjmout z počítače a odejít, pak jakákoliv informační bezpečnost ztrácí svůj význam [22].

Výsledkem hodnocení této oblasti je **index fyzické a objektové odolnosti Fi**.

Informační bezpečnost

Informační technologie patří ke klíčovým strukturám většiny zařízení. Zajištění bezpečnosti těchto systémů se však stále více prodražuje. Současně by mělo být stanoveno, jaká je skutečná závislost na těchto systémech a zda při jejich výpadku nebo ztrátě dat může práce vůbec pokračovat [22].

Výsledkem hodnocení této oblasti je **index informační bezpečnosti Ii**.

Řízení kontinuity činnosti organizace

Jedná se o řídicí proces podporovaný vedením společnosti, který identifikuje potenciální dopady ztrát a jehož cílem je vytvořit takové postupy a prostředí, které umožní zajistit kontinuitu a obnovu klíčových procesů a činností organizace, na předem stanovené minimální úrovni, v případě jejich narušení nebo ztráty. Ochrání zájmy klíčových podílníků, akcionářů a dalších zájmových skupin, dobrou pověst a značku společnosti [22].

Výsledkem hodnocení této oblasti je **index řízení kontinuity činnosti organizace Ki**.

Administrativní bezpečnost

Administrativní bezpečnost tvoří systém opatření při tvorbě, příjmu, evidenci, zpracování, odesílání, přepravě, přenášení, ukládání, skartačním řízení, archivaci, případně jiném nakládání s utajovanými nebo citlivými případně důvěrnými informacemi [22].

Výsledkem hodnocení této oblasti je **index administrativní bezpečnosti Ai**.

Zajištění dostupnosti personálu

Kvalifikovaný personál je ve většině zařízení nejdůležitější komponentou, bez které je provoz nemožný. Proto je velmi důležité, aby při kterémkoliv ohrožení bylo možné zajistit nutný počet zaměstnanců na pracovišti. Tato problematika je řešena v plánech vyrozumění jako součást krizového plánu nebo nouzového plánu [22].

Výsledkem hodnocení této oblasti je **index zajištění dostupnosti personálu Pi**.

Pro hodnocení jednotlivých částí lze použít mnoho metod, nejjednodušší metodou však je **Check-List** (kontrolní seznam). Tato metoda je založena na systematické kontrole plnění předem stanovených podmínek a opatření. Seznam kontrolních otázek je vytvářen na základě seznamu charakteristik sledovaného systému.

Každá z těchto částí je hodnocena jednotlivě, na základě výsledku hodnocení se stanoví **index bezpečnosti jednotlivé oblasti**. Tyto indexy poté násobíme a výsledná hodnota představuje **hodnotu odolnosti KI**.

$$KIR = Fi * Ii * Ki * Ai * Pi \quad (2)$$

Předpokládáme, že v případě pravděpodobnostního přístupu, násobením kumulují pravděpodobnosti, což snižuje celkovou pravděpodobnost a narušuje vnímání celkové kritické úrovně infrastruktury ochrany. Druhý možný přístup, který je založen na současném stavu znalostí, je vyjádřením průměrné hodnoty definovaných indexů. Toho docílíme sečtením jednotlivých indexů prvků a následným vydělením počtem prvků (x) [22].

$$KIR = \frac{Fi + Ii + Ki + Ai + Pi}{x} \quad (3)$$

8.1 Systémy a metody pro hodnocení a analýzu

Za účelem hodnocení a analýzy prvků KI byly vytvořeny mnohé nástroje a metody. Jak již zmiňovaná metoda KARS, tak jiné, ať už jednodušší nebo složitější. Nastíním alespoň v krátkosti některé z metod analýzy.

Metoda PHA

Metoda PHA (Preliminary Hazard Analysis = Předběžná analýza ohrožení) je technika odvozená z požadavků amerického bezpečnostního vojenského programu. Obecným způsobem se soustřeďuje na hlavní procesy a na nebezpečné látky b podniku. Metoda je založena na vyhledávání nebezpečných stavů, jejich příčin a dopadů a na jejich zařazení do kategorií dle stanovených kritérií. Koncept PHA představuje souhrn několika různých technik vhodných k posouzení rizikovosti. Těmito technikami jsou What – If analýza, HAZOP (Hazard Operation Process = analýza ohrožení a provozuschopnosti), FMEA (Failure Mode and Effect Analysis = analýza poruch a jejich dopadů), FTA (Failure Tree Analysis = analýza stromu poruch) a jejich kombinace.

Aplikační kroky metody PHA mohou být následující:

1. hledání souvislostí mezi událostmi,
2. kladení dotazů (Co by kdyby ...),
3. klasifikace činitelů vedoucích k ohrožení,
4. klasifikace nehod, nouzových stavů,
5. klasifikace chyb v systému,
6. výrok o riziku a protiopatření.

PHA se nejčastěji provádí v raných etapách vývoje projektů, kdy není k dispozici dostatek informací a může tedy předcházet dalším studiím [23].

Systém RAMCAP

RAMCAP (Risk Analysis and Management for Critical Asset Protection = Analýza rizik a řízení pro ochranu kritických aktiv) je rámec pro analýzu a řízení rizik spojených s teroristickými útoky proti prvkům KI. Výrobce, firma ASME Innovative Technologies Institute, uvádí, že RAMCAP poskytuje konzistentní a technicky spolehlivé metody pro identifikaci, analýzu, kvantifikaci a informace o charakteristikách a možnostech dopadů, které mohou vést teroristy ke zvolení konkrétního cíle a dále také možné dopady určitých forem útoku. Dále dokumentuje proces identifikace chyby zabezpečení a poskytuje metody pro hodnocení a možnosti k odstranění těchto nedostatků. Samotný proces hodnocení je rozdělen do sedmi analytických oblastí:

1. Charakterizace aktiv - vymezuje, které zařízení a aktiva jsou nezbytné pro plnění poslání nebo funkci organizace.
2. Charakterizace hrozby - definuje jaké konkrétní hrozby pro každé aktivum hrozí.
3. Analýza dopadů - je odhadem nejhoršího možného výsledku dopadu konkrétní hrozby na konkrétní aktivum.
4. Analýza zranitelnosti - je odhadem pravděpodobnosti, že konkrétní útok na konkrétní aktivum vzniká do odhadovaného dopadu a to i ve vztahu k účinnosti stávajících bezpečnostních opatření.
5. Hodnocení hrozeb - je odhadem nebo pravděpodobností, že nastane očekávaná událost.
6. Hodnocení rizik a odolnosti - odhad rizika a odolnosti je určen posuzováním pro každou událost a každé aktivum.
7. Řízení rizik a odolnosti - posouzení rizik i odolnosti a způsoby snižování rizik spolu s možností zvýšení odolnosti.

Tato metoda je v USA využívána především jako společný mechanismus pro porovnání rizik a jejich řízení v oblastech jaderná energie a odpad, chemický průmysl, ropný průmysl, zemní plyn, přehrady, nádrže a odpadní systémy [24].

Pro hodnocení odolnosti KI existuje mnoho matematických a technologických přístupů. Vždy však vychází z potřeb pozorovatele, respektive hodnotitele. Příslušný model by měl být založen na typu prvku KI a způsobu jeho hodnocení. Je třeba si uvědomit, že ať se jedná o určení nebo hodnocení rizika, vždy je potřeba použít analytickou metodu vhodnou k dané problematice. Existuje celá řada metod a postupů. Mnoho nástrojů označovaných jako analytické se však přímo netýká, avšak slouží jako podpůrný mechanismus k stanovení rizika. Obecně lze říci, že jsou nástroje k analýze rizika velmi široké, pro každý prvek by se dal tedy upravit stávající nebo vytvořit nový postup nebo metoda. Výběr metody pro analýzu a hodnocení je třeba vybírat cíleně. Cíle těchto procesů jsou však jasně dány, je třeba zajistit nástroj pro rozhodování a možnost matematicky vyjádřit hodnocení prvků KI. Někdy nám stačí pouze orientační výsledky a jindy je třeba zjistit přesné konkrétní hodnoty.

Pro účel multikriteriálního hodnocení a zpracování do formy nástroje pro hodnocení odolnosti kritické infrastruktury jsem si vybral metodiku, která vychází z analýzy **KARS (Kvalitativní analýza rizik s využití jejich souvztažností)** a kombinuje v sobě další metody analýzy, především jednoduché a uživatelsky snadno editovatelné Check-Listy.

Tvorba nástroje vychází z dokumentu „*Metodika hodnocení odolnosti vybraných prvků a systému prvků kritické infrastruktury*“, která vznikla jako výstup projektu bezpečnostního výzkumu „*VG20112014067 - Systém hodnocení odolnosti prvků a sítí vybraných oblastí kritické infrastruktury*.“

II. PRAKTICKÁ ČÁST

9 MULTIKRITERIÁLNÍ HODNOCENÍ ODOLNOSTI KRITICKÉ INFRASTRUKTURY

Nyní se dostáváme do stěžejní části mé práce. Tedy vytvoření nástroje pro multikriteriální hodnocení odolnosti kritické infrastruktury a aplikace na prvek KI.

Při tvorbě nástroje pro hodnocení odolnosti prvku KI jsem zvolil zmiňovanou jsem zvolil metodu KARS aplikovanou na prvek Zdravotní péče, Nemocniční péči. Ta vychází z dokumentu „*Metodika hodnocení odolnosti vybraných prvků a systému prvků kritické infrastruktury*“, která vznikla jako výstup projektu bezpečnostního výzkumu „*VG20112014067 - Systém hodnocení odolnosti prvků a sítí vybraných oblastí kritické infrastruktury*.“

9.1 KARS

Základním principem, který metoda KARS využívá, je možná eskalace událostí, kdy událost vzniklá v jednom objektu může zapříčinit vznik události v jiném objektu. Může tedy dojít ke zvýšení pravděpodobnosti vzniku nepříznivé události a ke zvýšení následků. Jelikož je velmi těžké nalézt systém, kde by existovalo pouze jedno riziko, tak lze tuto metodu využít ve většině případů. Pokud budeme vycházet z principu kritičnosti a propojitelnosti, tak můžeme prohlásit, že neexistuje zcela bezpečný systém a že mezi všemi systémy existuje souvztažnost.

9.2 Aplikace metody KARS při hodnocení odolnosti kritické infrastruktury

9.2.1 Soupis rizik

Prvním krokem při zpracování daného problému pomocí analýzy KARS je sestavení soupisu možných rizik. Rizika jsem rozdělil do tří kategorií: energetika, přírodní vlivy a rizika vzniklé s přičiněním lidského faktoru. Počet rizik jsem stanovil na 24, z důvodu větší přehlednosti. Níže uvedený seznam jsem sestavil dle českého překladu příručky *Schutz Kritischer Infrastruktur: Risikomanagement im Krankenhaus (Ochrana kritické infrastruktury: Management rizik v nemocnici)* a s ohledem na univerzálnost nástroje.

Energetika

1. Krátkodobý výpadek elektřiny

2. Dlouhodobý výpadek elektřiny
3. Výpadek dodávky vody
4. Výpadek dodávky plynu

Přírodní vlivy

5. Povodeň, záplava, zátopa
6. Dlouhotrvající sucho
7. Extrémní vedro a sucho
8. Silný mráz
9. Pandemie, epidemie

Rizika spojené s přičiněním lidského faktoru

10. Požár
11. Výbuch
12. Krádež
13. Únik škodlivin v okolí
14. Výpadek v oblasti transport-logistika
15. Virtuální napadení informační techniky
16. Teroristický útok
17. Narušení veřejného pořádku
18. Nedostupnost personálu
19. Náhlý nápor pacientů
20. Technické poruchy
21. Sabotáž
22. Násilná kriminální činnost
23. Vandalismus
24. Rabování

9.2.2 Sestavení tabulky rizik

Druhým krokem je sestavení tabulky rizik. Tato metoda je založena na použití jednoduchých matematických vztahů. Z tohoto důvodu jsem použil k programování nástroje prostředí MS Excel 2010, který umožňuje snadnou editaci a práci s grafem. Tabulka se vytváří tak, že do prvního sloupce vypíšeme veškerá rizika a přiřadíme jim pořadové číslo (index) pro větší přehlednost. Indexy následně přepíšeme do prvního řádku

tabulky. Jelikož událost nemůže způsobit sama sebe, tak je daná buňka označena křížkem. Výsledná tabulka vypadá následovně:

Tabulka 1. Tabulka souvztažnosti rizik

i	Tabulka souvztažnosti	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	
Energetika																												
1	Krátkodobý výpadek elektřiny	+																										
2	Dlouhodobý výpadek elektřiny		+																									
3	Výpadek dodávky vody			+																								
4	Výpadek dodávky plynu				+																							
Přírodní vlivy																												
5	Povodeň, záplava, zátopa					+																						
6	Dlouhotrvající sucho						+																					
7	Extrémní vedro a sucho							+																				
8	Silný mráz								+																			
9	Pandemie, epidemie									+																		
Rizika spojená s přičiněním lidského faktoru																												
10	Požár										+																	
11	Výbuch											+																
12	Krádež												+															
13	Únik škodlivin v okolí													+														
14	Výpadek v oblasti logistika														+													
15	Virtuální napadení															+												
16	Teroristický útok																+											
17	Narušení veřejného pořádku																	+										
18	Nedostupnost personálu																		+									
19	Náhlý nápor pacientů																			+								
20	Technické poruchy																				+							
21	Sabotáž																					+						
22	Násilná kriminální činnost																						+					
23	Vandalismus																							+				
24	Rabování																								+			
25	Rezerva 1																									+		
26	Rezerva 2																										+	

9.2.3 Vyplnění tabulky souvztažnosti rizik

Jelikož metoda KARS je založena na vzájemné souvztažnosti možných rizik. Vztahy mezi jednotlivými riziky je nutno popsat. Pokud máme v systému x rizik \mathbf{R} , tak označíme rizika aktiva \mathbf{R}_i a rizika pasiva \mathbf{R}_j , kde i udává číslo řádku a j číslo sloupce.

Tabulku vyplníme následujícím způsobem:

- 1) Riziko \mathbf{R} nemůže vyvolat samo sebe
- 2) Pro vyplnění dalších pozic postupujeme po řádcích zleva doprava. Do pozic \mathbf{R}_{ij} vyplňujeme následující hodnoty:

1 – je-li reálná možnost, že riziko \mathbf{R}_i může vyvolat riziko \mathbf{R}_j

0 – v případě, že riziko \mathbf{R}_i nevyvolá riziko \mathbf{R}_j

Takto vyplníme všechny buňky \mathbf{R}_{ij} . Pro snadnější manipulaci jsem nahradil ruční vyplňování zaškrťovacími poli.

9.2.4 Výpočet koeficientů aktivity a pasivity

V další fázi musíme převést vyplněné hodnoty v tabulce do matematicky a graficky vyjádřitelné podoby. Toho docílíme výpočtem koeficientů pasivity a aktivity.

Koeficient aktivity $K_A R_i$

je vyjádření počtu návazných rizik pro riziko R_i , která mohou být vyvolána, v případě, že nastane riziko R_i .

$$K_A R_i = \frac{\sum R_i}{x - 1} \quad (4)$$

Koeficient pasivity $K_P R_i$

je vyjádření počtu rizik pro riziko R_i , která mohou vyvolat následně riziko R_i .

$$K_P R_i = \frac{\sum R_i}{x - 1} \quad (5)$$

Kde:

$\sum R_i$ je součet rizik :

- pro koeficient aktivity je to horizontální osa
- pro koeficient pasivity je to vertikální osa

x je celkový počet rizik. Pro x rizik platí, že počet kombinací je roven $x - 1$.

9.2.5 Grafické vyhodnocení

Pro účely prioritizace rizik je nutné vytvořený graf rozdělit na jednotlivé segmenty, které diverzifikují rizika podle jejich významnosti. K rozdělení grafu na tři segmenty je nutné definovat přímkou P_1 a P_2 , které rozdělí samotný graf tak i rizika do segmentů, kde se předpokládá, že v prvním segmentu bude 80% nejvýznamnějších rizik.

Pro vyjádření parametrů pro přímkou P_1 a P_2 použijeme vztah:

$$P_1 = K_{Amax} - \frac{(K_{Amax} - K_{Amin})}{100} * 80 \quad (6)$$

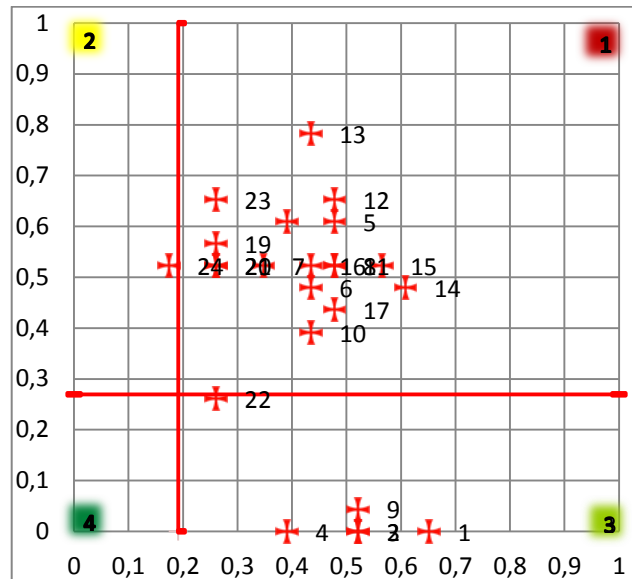
$$P_2 = K_{Pmax} - \frac{(K_{Pmax} - K_{Pmin})}{100} * 80 \quad (7)$$

Kde:

K_{Amax} a K_{Amin} jsou minimální a maximální hodnoty z tabulky s koeficienty aktivity

K_{Pmax} a K_{Pmin} jsou minimální a maximální hodnoty z tabulky s koeficienty pasivity

Výsledný graf může vypadat takto:



Graf 2. Graf souvztažnosti rizik

Pomocí přímek P_1 a P_2 je následně rozdělen graf do 4 segmentů. Vlastnosti segmentů vyjadřuje následující tabulka:

Tabulka 2. Vlastnosti segmentů

S	Vlastnosti segmentu
1	Oblast primárně i sekundárně nebezpečných rizik
2	Oblast sekundárně nebezpečných rizik
3	Oblast primárně nebezpečných rizik
4	Oblast relativně bezpečná

9.2.6 Stanovení hodnoty rizikovosti

Hodnota rizikovosti H_{RZi} vyjadřuje faktor, který zásadním způsobem snižuje odolnost systému KI. Vyjadřuje tedy potenciální dopad rizika na funkčnost KI.

Z grafického výstupu je zřejmé, že za kritická rizika a to i ve vztahu k stanovení bezpečnostních opatření či hodnocení odolnosti prvku kritické infrastruktury lze považovat rizika náležící do 1. segmentu KARS analýzy. Následně se těmto rizikům přidělí hodnota

rizikivosti, která zohledňuje i míru a význam dopadu vybraného rizika na daný systém. Pro výpočet hodnoty rizikivosti jsem použil následující vztah:

$$H_{Rzi} = \frac{H_{Ri}}{H_{Rimax}} \quad (8)$$

Kde:

H_{Ri} je původní hodnota rizika vyplývající z prvního stupně analýzy rizik

H_{Rimax} je maximálně dosažitelná hodnota rizika v rámci hodnotové škály.

Pro výpočet hodnoty rizika H_{Ri} jednotlivých rizik použijeme vztah:

$$H_{Ri} = P \times N \quad (9)$$

Kde:

P je bodová hodnota pro vyjádření pravděpodobnosti výskytu hrozby doplněná dle tabulky 3.

N je bodová hodnota pro vyjádření účinku hrozby vybraná z tabulky 4.

Tabulka 3. Bodová hodnota pro vyjádření pravděpodobnosti výskytu hrozby

Bodová hodnota pro vyjádření pravděpodobnosti výskytu hrozby	
0	Nepravděpodobná nebo nehodnocená
1	Velmi málo pravděpodobná
2	Málo pravděpodobná
3	Středně pravděpodobná
4	Značně pravděpodobná
5	Vysoce pravděpodobná až jistá

Tabulka 4. Bodová hodnota pro vyjádření účinku hrozby

Bodová hodnota pro vyjádření účinku hrozby	
0	Žádný
1	Nízký
2	Nevýznamný
3	Střední
4	Vysoký
5	Velmi vysoký

Výsledný list pro určení hodnoty rizikivosti prvků kritické infrastruktury poté vypadá následovně:

i	Rizika	S	P	N	Haz
Energetika					
1	Krátkodobý výpadek elektřiny	2	0	0	X
2	Dlouhodobý výpadek elektřiny	1	0	0	0,00
3	Výpadek do dávký vody	1	0	0	0,00
4	Výpadek do dávký plynu	1	0	0	0,00
Přírodní vlivy					
5	Povoďeň, záplava, zátopa	2	0	0	X
6	Dlouho trvající sucho	1	0	0	0,00
7	Extrémní vedro a sucho	1	0	0	0,00
8	Silný mraz	3	0	0	X
9	Pandemie, epidemie	1	0	0	0,00
Rizika spojená s přičiněním lidského faktoru					
10	Požár	2	0	0	X
11	Výbuch	2	0	0	X
12	Krádež	2	0	0	X
13	Únik škodlivin v okolí	2	0	0	X
14	Výpadek v oblasti logistika	1	0	0	0,00
15	Virtuální napadení	3	0	0	X
16	Teroristický útok	2	0	0	X
17	Narušení veřejného pořádku	1	0	0	0,00
18	Nedostupnost personálu	1	0	0	0,00
19	Náhly nápor pacientů	3	0	0	X
20	Technické poruchy	2	0	0	X
21	Sabotáž	4	0	0	X
22	Násilná kriminální činnost	3	0	0	X
23	vandalismus	2	0	0	X
24	Rabování	1	0	0	0,00

Bodová hodnota pro vyjádření pravděpodobnosti výskytu hrozby	
0	Nepravděpodobná nebo nehodnocená
1	Velmi málo pravděpodobná
2	Málo pravděpodobná
3	Středně pravděpodobná
4	Značně pravděpodobná
5	Vysoce pravděpodobná až jistá

Bodová hodnota pro vyjádření účinku hrozby	
0	Žádný
1	Nízký
2	Nevýznamný
3	Střední
4	Vysoký
5	Velmi vysoký

Obrázek 13. List Stanovení rizikivosti

9.2.7 Stanovení koeficientu závislosti

Stanovení koeficientu závislosti K_S je důležitým aspektem, který představuje vzájemné vazby a závislosti oblastí KI v rámci systému kritické infrastruktury. Mezi základní typy vazeb patří:

- fyzické vazby,
- logické vazby,
- územní vazby.

Pro potřebu stanovení koeficientu závislosti jsem vytvořil tabulku závislosti prvku KI Nemocniční péče na jiných službách či produktech (prvcích) KI. Pro vyjádření hodnoty závislosti na jednotlivých prvcích jsem danému prvku (službě) přiřadil hodnotu 1-10, která vyjadřuje význam (stupeň) dané vazby. Stejně jako v případě vyjádření hodnoty rizikivosti je koeficient závislosti považován za faktor zvyšující potenciální míru degradace funkce a snížení hodnoty odolnosti posuzovaného systému.

Pro stanovení koeficientu závislosti se použije vztah:

$$K_S = \frac{\sum S_i}{S_{max}} \quad (10)$$

Kde:

K_S je koeficient závislosti,

Suma S_i je součet míry závislosti prvku KI na i-tém produktu (službě),

S_{ma} je maximální hodnota, které lze v rámci vymezeného systému dosáhnout.

Výsledný list pro určení hodnoty rizikovosti prvků kritické infrastruktury poté vypadá následovně:

Tabulka 5. Určení hodnoty rizikovosti

Produkt nebo služba	Je prvek Nemocniční péče závislý na jiném produktu (službě)?		Míra závislosti
Zásobování elektřinou	<input type="radio"/> ano	<input type="radio"/> ne	0
Zásobování plynem	<input type="radio"/> ano	<input type="radio"/> ne	0
Zásobování vodou	<input type="radio"/> ano	<input type="radio"/> ne	0
Zásobování potravinami	<input type="radio"/> ano	<input type="radio"/> ne	0
Funkčnost komunikačních sítí	<input type="radio"/> ano	<input type="radio"/> ne	0
Přístup k datovým službám	<input type="radio"/> ano	<input type="radio"/> ne	0
Dostupnost personálu	<input type="radio"/> ano	<input type="radio"/> ne	0
Zásobování zdravotnickým materiálem	<input type="radio"/> ano	<input type="radio"/> ne	0
Předpovědní, varovná a hlásná služba	<input type="radio"/> ano	<input type="radio"/> ne	0
Veřejná správa	<input type="radio"/> ano	<input type="radio"/> ne	0
Doprava	<input type="radio"/> ano	<input type="radio"/> ne	0
	K_S		0,00

9.2.8 Stanovení koeficientu robustnosti

Koeficient robustnosti K_{RO} , představuje pevnost, stálost, odolnost vůči deformaci. Je to schopnost vydržet a přestát účinky negativního působení bez významné degradace funkce (funkčnosti). V této metodice je robustnost prvku členěna na **strukturální robustnost** a **robustnost zabezpečení**. Tyto dvě oblasti, respektive jejich vyjádření, nám formulují vztah pro hodnocení robustnosti systému:

$$K_{RO} = K_{RZ} \times K_{SR} \quad (11)$$

Kde:

K_{RO} je koeficient robustnosti

K_{RZ} je koeficient robustnosti zabezpečení

K_{SR} je koeficient strukturální robustnosti

Koeficient robustnosti zabezpečení K_{RZ}

Ukazatel robustnosti zabezpečení vyjadřuje rozsah a kvalitu opatření v oblasti zabezpečení prvku KI vůči identifikovaným rizikům. Jednotlivá opatření jsou podle charakteru a účinku uskupena do specifických oblastí bezpečnosti. Jedná se o oblast fyzické a objektové bezpečnosti, informační bezpečnosti, administrativní bezpečnosti a řízení kontinuity činnosti organizace.

Jako první se při výpočtu robustnosti musí určit **význam (váha) jednotlivých oblastí V_i** bezpečnosti resp. složek parametru/koeficientu robustnosti zabezpečení je stejně individuální jako postavení a význam robustnosti a připravenosti ve vztahu k odolnosti vybraného prvku nebo systému prvků KI. Stanovení významu resp. váhy jednotlivých složek robustnosti zabezpečení je realizováno pomocí párového srovnání (Fullerův trojúhelník). V praxi to znamená, že si položíme otázku, zda je jedna oblast důležitější než druhá. Například v případě nemocnice bude schopnost zajištění kontinuity činnosti organizace důležitější než informační bezpečnost. Pro jednoduché porovnání jsem vytvořil tabulku, ve které se rozhodujeme, která oblast je pro správné fungování důležitější. Každá oblast je porovnána s ostatními.

Tabulka 6. Určení vah jednotlivých oblastí

Fyzická a objektová bezpečnost	☺	☺	Informační bezpečnost
Fyzická a objektová bezpečnost	☺	☺	Řízení kontinuity činnosti organizace
Fyzická a objektová bezpečnost	☺	☺	Administrativní bezpečnost
Informační bezpečnost	☺	☺	Řízení kontinuity činnosti organizace
Informační bezpečnost	☺	☺	Administrativní bezpečnost
Řízení kontinuity činnosti organizace	☺	☺	Administrativní bezpečnost

Pro výpočet vah jednotlivých oblastí použijeme vztah:

$$V_i = \frac{\sum v_i}{K_V} \quad (12)$$

Kde:

V_i je váha jednotlivých oblastí:

- V_{FB} – váha fyzické bezpečnosti,
- V_{IB} – váha informační bezpečnosti,
- V_{AB} – váha administrativní bezpečnosti,
- V_{KO} – váha řízení kontinuity činnosti organizace,

$\sum v_i$ je suma odpovědí, kdy má jedna oblast vyšší postavení než druhá,

K_V je maximální počet kombinací jednotlivých oblastí bezpečnosti (v tomto případě 3).

Další složkou pro výpočet robustnosti je vyjádření **míry kvality přijatých opatření M_i** . Ta se vyjádří pomocí Check-Listu pro každou ze zkoumaných oblastí (fyzická a objektová bezpečnost, informační bezpečnost, administrativní bezpečnost a řízení kontinuity činnosti organizace). Vyjadřuje míru přijatých opatření, která byla zavedena pro minimalizaci rizika a zvýšení robustnosti jak jednotlivých oblastí, tak i celku. Pro každou z oblastí jsem vyrobil samostatný Check-List. Tabulka Check-Listu může vypadat následovně:

Tabulka 7. Určení míry kvality přijatých opatření

Fyzická a objektová bezpečnost	Ano	Ne
Je v objektu přítomna ostraha 24/7	<input type="radio"/>	<input type="radio"/>
Je v objektu nainstalován CCTV	<input type="radio"/>	<input type="radio"/>
Je v objektu nainstalován IH&S	<input type="radio"/>	<input type="radio"/>
Je v objektu nainstalován EPS	<input type="radio"/>	<input type="radio"/>
Je v objektu nainstalován ACCESS	<input type="radio"/>	<input type="radio"/>
Je objekt napojen na PPC PČR	<input type="radio"/>	<input type="radio"/>
Byl proveden bezp. audit?	<input type="radio"/>	<input type="radio"/>
Perimetrická ochrana vyšší než 2 m	<input type="radio"/>	<input type="radio"/>
Školení zaměstnanců	<input type="radio"/>	<input type="radio"/>
Prevence	<input type="radio"/>	<input type="radio"/>

Pro výpočet vah jednotlivých oblastí použijeme vztah:

$$M_i = \frac{\sum m_i}{K_M} \quad (13)$$

Kde:

M_i je míra kvality jednotlivých oblastí:

- M_{FB} – vyjádření míry kvality přijatých opatření fyzické bezpečnosti,
- M_{IB} – vyjádření míry kvality přijatých opatření informační bezpečnosti,
- M_{AB} – vyjádření míry kvality přijatých opatření administrativní bezpečnosti,
- M_{KO} – vyjádření míry kvality přijatých opatření kontinuity činnosti organizace,

$\sum m_i$ je suma kladných odpovědí,

K_M je maximální počet odpovědí jednotlivých oblastí bezpečnosti (v tomto případě 10).

Posledním krokem pro výpočet robustnosti je dosazení do vzorce definujícího **robustnost zabezpečení K_{RZ}** :

$$K_{RZ} = M_{FB} \times V_{FB} + M_{IB} \times V_{IB} + M_{AB} \times V_{AB} + M_{KO} \times V_{KO} \quad (14)$$

Koeficient strukturální robustnosti K_{SR}

Koeficient strukturální robustnosti prvku KI vyjadřuje schopnost přestát působení negativních činitelů díky jeho struktuře, systémovým vlastnostem a vlastnostem technologií. Zahrnuje také schopnost vydržet účinky negativních činitelů bez degradace funkce, nasadit redundantní subsystémy, izolovat poruchy (zabránit jejich šíření) a flexibilně přesměrovat provoz. Vzhledem k tomu, že prvky KI mají charakter objektu, technologického celku, personálně technického systému, soustavy procesů či služeb, je hodnocení strukturální robustnosti prováděno metodou multikriteriálního hodnocení.

Pro určení hodnoty strukturální robustnosti jsem vytvořil následující tabulku:

Tabulka 8. Hodnocení strukturální robustnosti

Typ topologie	bod		plocha			linie		uzel
	do 1000 m ²	nad 1000 m ²	do 1 km ²	1 – 10 km ²	nad 10 km ²	do 10 km	nad 10 km	metodika
Složitost	jednoduchý (do 10 zaměstnanců)		střední (10 – 100 zaměstnanců)			složitý (nad 100 zaměstnanců)		
Počet klíčových technologií	do 2 technologií		3 – 4 technologií			5 a více technologií		
Flexibilita	ne					ano		
Redundance	ne					ano		
Perimetrická ochrana	bez ochrany		lokální			úplná		

V případě, že se jedná o typ topologie uzel, je třeba doplnit doplňující informace, k čemuž slouží následující tabulka:

Tabulka 9. Doplňující tabulka hodnocení strukturální robustnosti

Typ topologie	sběrnice/bus	hvězda/kruh	strom	polygon
Počet klíčových uzlů	1 uzel	2 uzly	3 uzly	4 uzly a více nebo žádný
Celkový počet uzlů	do 5 uzlů	6 – 15 uzlů	16 – 40 uzlů	nad 40 uzlů
Průměrný počet hran na uzel	do 1,5 hrany	1,6 – 2,2 hrany	2,3 – 3 hrany	více jak 3 hrany

Výsledná hodnota koeficientu strukturální robustnosti K_{SR} je vypočtena podle vzorce:

$$K_{SR} = 0,9 + \frac{I_t + I_s + I_{kt} + I_f + I_r + I_{po}}{120} \quad (15)$$

Kde:

- I_t je index topologie,
- I_s je index složitosti,
- I_{kt} je index klíčových technologií,
- I_f je index flexibility,
- I_{po} je index perimetrické ochrany.

Jednotlivé hodnoty pro určení indexů jsou uvedeny v příloze č. 3.

9.2.9 Výpočet hodnoty koeficientu připravenosti K_{PR}

Výpočet koeficientu připravenosti je posledním z kritérií pro hodnocení odolnosti KI. Připravenost prvku na mimořádnou událost je hodnocena **koeficientem připravenosti** K_{PR} . Ten lze chápat jako vyjádření schopnosti prvku KI k dostatečné reakci, respektive

odezvě, na vznik mimořádné události nebo bezpečnostního incidentu. Také ji lze chápat i jako schopnost obnovy prvku a návrat k požadované funkčnosti systému.

Matematické vyjádření připravenosti vybraného prvku nebo systému prvků KI je dáno vztahem:

$$K_{PR} = \frac{K_r + K_p + K_i}{3} \quad (16)$$

Kde:

K_r je koeficient správnosti identifikovaných rizik,

K_p je koeficient kvality zpracování plánu krizové připravenosti subjektu KI,

K_i je koeficient kvality implementace plánu krizové připravenosti subjektu KI.

Podobně tedy jako u koeficientu robustnosti, pro vyjádření koeficientu připravenosti musíme provést dílčí výpočty ostatních koeficientů.

Koeficient správnosti identifikovaných rizik K_r

Koeficient správnosti identifikace rizik vyjadřuje správnost námi provedené identifikace rizik. Před námi provedeným hodnocením prvku KI je provedena kontrola nezávislým kontrolním orgánem pomocí více metod hodnocení a analýz. Počet takto zjištěných rizik označíme jako R_i . Pro účel výpočtu R_p použijeme pouze rizika, která spadají do prvního segmentu, tedy do oblasti primárně i sekundárně nebezpečných rizik získanými za pomoci KARS analýzy. Každé opomenuté riziko může znamenat snížení stupně připravenosti. Pro vyjádření koeficientu použijeme následující vzorec:

$$K_r = \frac{R_p}{R_i} \quad (17)$$

Kde:

R_p vyjadřuje, kolik rizik ze seznamu rizik jsme identifikovali jako významnou hrozbu,

R_i vyjadřuje, kolik rizik bylo kontrolním orgánem nezávisle identifikováno.

Hodnota K_r se musí pohybovat v intervalu $\langle 0;1 \rangle$, pokud je hodnota větší než 1, k účelu výpočtů použijeme maximální hodnotu.

Koeficient kvality zpracování plánu krizové připravenosti K_p

Koeficient kvality zpracování plánu krizové připravenosti subjektu kritické infrastruktury vyjadřuje počet naplněných kritérií respektive kladných odpovědí v rámci kontrolního seznamu (Check-Listu) pro posuzování kvality zpracování plánu krizové připravenosti subjektu KI. Pro účel zjištění tohoto koeficientu jsem vytvořil jednoduchou tabulku:

Tabulka 10. Krizová připravenost

Krizová připravenost	Ano	Ne
Identifikace možných událostí	<input type="radio"/>	<input type="radio"/>
Pravděpodobnost výskytu událostí	<input type="radio"/>	<input type="radio"/>
Soupis potřeb a zdrojů	<input type="radio"/>	<input type="radio"/>
Organizační struktura	<input type="radio"/>	<input type="radio"/>
Určení zodpovědných osob	<input type="radio"/>	<input type="radio"/>
Kontaktní údaje	<input type="radio"/>	<input type="radio"/>
Pojistné smlouvy	<input type="radio"/>	<input type="radio"/>
Popis hlavních činností	<input type="radio"/>	<input type="radio"/>
Soupis postupů	<input type="radio"/>	<input type="radio"/>
Bezpečnostní audit	<input type="radio"/>	<input type="radio"/>

Hodnota koeficientu je dána vztahem:

$$K_p = \frac{\sum K_{ip}}{x_p} \quad (18)$$

Kde:

$\sum K_{ip}$ je počet naplněných kritérií,

x_i je celkový počet stanovených kritérií v této oblasti připravenosti.

Koeficient kvality implementace plánu krizové připravenosti K_i

Koeficient kvality implementace plánu krizové připravenosti subjektu kritické infrastruktury vyjadřuje počet naplněných kritérií respektive kladných odpovědí v rámci kontrolního seznamu (Check-Listu) pro posuzování kvality implementace plánu krizové připravenosti subjektu KI. Pro účel zjištění tohoto indexu jsem vytvořil jednoduchou tabulku:

$$K_i = \frac{\sum K_{ii}}{x_i} \quad (19)$$

Kde:

$\sum K_{ii}$ je počet naplněných kritérií,

x_i je celkový počet stanovených kritérií v této oblasti připravenosti.

9.2.10 Výpočet hodnoty odolnosti prvku kritické infrastruktury

O obecném principu hodnocení odolnosti KI pojednává kapitola 6. Proto se v této kapitole budu věnovat převážně využití tohoto matematického modelu v kombinaci s metodou KARS. Každá oblast bezpečnosti, mající pozitivní vliv na odolnost prvku, byla posuzována ve vztahu k vytvořeným kritériím pro danou oblast a to prostřednictvím Check-Listů. Celková hodnota odolnosti v rámci posuzovaného systému je průměrnou hodnotou odolností systému ve vztahu i-tému riziku. Prvním krokem k výpočtu odolnosti prvku je tedy matematické vyjádření hodnocení **odolnosti prvku kritické infrastruktury ve vztahu k i-tému riziku OD_i** :

$$OD_i = \frac{(1 - H_{Rzi}) + (1 - K_s) + (K_{RO} * V_{RO} + K_{PR} * V_{PR})}{3} \quad (20)$$

Kde:

H_{Rzi} je hodnota rizikovosti i-tého rizika (viz kapitola 9.2.6),

K_s je koeficient závislosti (viz kapitola 9.2.7),

K_{RO} je koeficient robustnosti (viz kapitola 9.2.8),

V_{RO} váha robustnosti (zde jsem zvolil hodnotu 0,5),

K_{PR} je koeficient připravenosti (viz kapitola 9.2.9),

V_{PR} váha připravenosti (zde jsem zvolil hodnotu 0,5).

Vztah $(1 - H_{Rzi})$ vyjadřuje skutečnost, že hodnota rizikovosti nám negativním způsobem ovlivňuje hodnotu odolnosti vybraného prvku nebo systému prvků kritické infrastruktury. Pro proces hodnocení používáme pouze rizika nacházející se v prvním segmentu.

Vztah $(1 - K_s)$ vyjadřuje fakt, že i koeficient souvztažnosti lze považovat za negativní faktor, snižující konečnou hodnotu odolnosti.

Důležité je ještě připomenout, že za účelem výpočtu odolnosti vybíráme pouze prvky, které náleží do prvního segmentu.

Dalším krokem při výpočtu je stanovení průměrné hodnoty odolnosti systému, která pro nás představuje **hodnotu odolnosti vybraného prvku kritické infrastruktury ODP**.

K tomu nám slouží následující matematické vyjádření:

$$ODP = \frac{\sum OD_i}{x_i} \quad (21)$$

Kde:

OD_i je hodnota odolnosti prvku ve vztahu k vybranému (i-tému) riziku,

x_i je počet vybraných rizik.

10 KŘIŽÁK

Na základě poznatků získaných v kapitole 9 jsem byl schopen vytvořit **Nástroj pro multikriteriální hodnocení odolnosti kritické infrastruktury Křížák**. Nástroj jsem se po zvážení několika možností vývojových prostředí a programovacích jazyků rozhodl vytvořit v programu MS Excel 2010 s využitím VisualBasic maker a skriptů. Toto prostředí se výborně hodí k práci s tabulkami a grafy, stejně jako pro aplikaci matematických vzorců. Taktéž snadná editace a uživatelsky snadná manipulace s daty byl jeden z klíčových faktorů pro volbu tohoto prostředí. Při vytváření ovládacích prvků jsem se zaměřil na jednoduchost a snadnou pochopitelnost. Ovládání je velmi intuitivní a pomocí funkce uzamčení sešitu nástroj neumožňuje zásah do editace vzorců a jiných klíčových částí. K editaci jsou tedy odemčeny pouze buňky k tomu určené. Veškeré prvky se ovládají myší, k zadávání hodnot není v celém nástroji potřeba klávesnice. Tuto možnost asi nejvíce ocení majitelé notebooku bez samostatné numerické klávesnice. Samozřejmostí je také možnost změny jazyku mezi češtinou a angličtinou.

V následujících kapitolách se seznámíme s prostředím, v kterém budeme pracovat a s používáním nástroje. Názvy kapitol jsou totožné s názvy záložek (listů).

10.1 Menu

Úvodní obrazovka (viz příloha č. 4) má převážně informační charakter. Obsahuje souhrnné informace o programu, autorovi a vizualizační tabulku, kde se zobrazují dílčí výsledky (koeficienty závislosti, robustnosti a připravenosti) a výsledek odolnosti prvku KI, včetně slovního hodnocení. Dále v levém horním rohu obsahuje menu pro volbu jazyka a tlačítko Export, které slouží k publikaci celého dokumentu ve formátu pdf.

10.2 R

Tato záložka (viz příloha č. 4) obsahuje tabulku rizikovosti. Tabulka je vytvořena za pomoci zaškrtačací polí CheckBox, která mají dvě polohy – zaškrtnuto/nezaškrtnuto (1/0). K vyplnění tabulky rizikovosti nám stačí držet se pravidel vypsanych v kapitole 9.2.3. Ve zkratce si stačí položit otázku: „Může riziko udané v řádku způsobit riziko udávané ve sloupci?“ Záložka obsahuje také ovládací prvek tlačítko Reset, které nastaví v celé tabulce hodnoty na nulu.

10.3 R2

Záložka (viz příloha č. 4) sloužící pouze k přehlednější vizualizaci předešlé záložky R. Zaškrtnutá a nezaškrtnutá pole jsou zde nahrazena přehlednějšími znaky, které neumožňují editaci. Tato záložka je určena převážně pro tisk a export dokumentu.

10.4 A, P

V této záložce (viz příloha č. 4) je provedena grafická vizualizace výpočtů koeficientů aktivity a pasivity (viz kapitola 9.2.4) a následná vizualizace výsledků (viz kapitola 9.2.5). Obsahuje tedy graf souvztažnosti rizik, hodnoty aktiv a pasiv, rozdělení do segmentů a tabulku s legendou.

10.5 Hrzi

Záložka (viz příloha č. 4) určená k stanovení hodnoty rizikovosti (viz kapitola 9.2.6). Do sloupců označených jako P (Pravděpodobnost výskytu hrozby) a N (Dopad hrozby) vyplňujeme z rozbalovacího seznamu hodnoty 0 až 5 dle přiložené legendy. Tyto hodnoty vyplňujeme pouze pro rizika v segmentu 1.

10.6 Ks

Tato záložka (viz příloha č. 4) obsahuje tabulku, která slouží ke stanovení koeficientu závislosti (viz kapitola 9.2.7). Při vyplňování si člověk klade za otázku: „Je prvek Nemocniční péče závislý na jiném produktu (službě)?“ Podle odpovědi poté zaškrtneme buďto odpověď kladnou nebo zápornou. Hodnoty závislosti jsou předem definovány, ale je možnost je změnit v rozsahu 0 až 10 za pomoci rolovacího seznamu. Samozřejmě je také resetovací tlačítko.

10.7 Krz

Záložka (viz příloha č. 4) sloužící k sestavení koeficientu robustnosti (viz kapitola 9.2.8). Tento list slouží k výpočtu koeficientu robustnosti zabezpečení. Obsahuje pět tabulek, tabulku pro určení váhy jednotlivých oblastí zabezpečení a čtyři tabulky pro hodnocení míry kvality přijatých opatření. Při vyplňování tabulky vah si pokládáme otázku: „Která z těchto oblastí je pro správné fungování prvku kritické infrastruktury důležitější?“ Následně vyplníme jednotlivé tabulky pro určení míry kvality Fyzické a objektové

bezpečnosti, Informační bezpečnosti, Administrativní bezpečnosti a Řízení kontinuity činnosti organizace. Záložka opět obsahuje resetovací tlačítko.

10.8 Ksr

Druhá ze záložek (viz příloha č. 4) sloužících k sestavení koeficientu robustnosti (viz kapitola 9.2.8). V tomto listu jsou dvě tabulky, které určují koeficient strukturální robustnosti. V první tabulce se vyplňují možnosti dle nastavených parametrů, zatímco druhá tabulka je rozšiřující a aktivuje se pouze, pokud je vybrána topologie uzlů. Záložka, stejně jako předešlé, obsahuje tlačítko Reset.

10.9 Kpr

Záložka Kpr (viz příloha č. 4) obsahuje dvě tabulky a buňku s rolovacím seznamem. Ty slouží k výpočtu dílčích koeficientů. S těmito koeficienty následně získáme hodnotu koeficientu připravenosti (viz kapitola 9.2.9). Jednotlivé tabulky opět obsahují rozhodovací možnosti ano/ne, díky nimž dokážeme stanovit hodnoty koeficientů kvality zpracování plánu krizové připravenosti a kvality implementace plánu krizové připravenosti. Rolovací seznam *Počet rizik identifikovaných kontrolním orgánem v segmentu 1* slouží k posouzení správnosti posuzovaných rizik. Součástí listu je i resetovací tlačítko pro vynulování hodnot.

10.10 ODP

Tato záložka (viz příloha č. 4) slouží jako výsledková listina. Jsou zde zobrazeny jednotlivé odolnosti vůči i-tému riziku ODi a výsledná hodnota ODP (viz kapitola 9.2.10). Dále obsahuje tabulku se slovním hodnocením včetně minimálních hodnot jednotlivých koeficientů.

10.11 Help

V této záložce (viz kapitola č. 4) jsou obsaženy veškeré zkratky používané v nástroji. Slouží především jako pomůcka při práci s exportovanou nebo vytisknutou verzí nástroje.

Pro účinnou ochranu prvků KI je důležité znát jeho odolnost vůči předpokládaným rizikům. Právě proces hodnocení odolnosti KI vede k zavádění potřebných opatření nutných k nápravě. Jedná se tedy o důležitý krok, který umožňuje cíleně zlepšovat stav ochrany prvku KI. Jak z práce vyplývá, proces hodnocení odolnosti prvků a systému prvků představuje složitý proces. Jeho zjednodušení i použití metodického postupu umožňuje metodika hodnocení odolnosti prvků a systému prvků KI. Právě ucelená metodika vytváří jistý ucelený postup hodnocení odolnosti. Vlastní hodnocení je provedeno multikriteriálně se semi-kvantitativním vyjádřením stupně odolnosti.

Použitá metodika, ze které jsem vycházel při tvorbě nástroje, byla vytvořena v rámci řešení projektu bezpečnostního výzkumu „*VG 20112014067 Systém hodnocení odolnosti vybraných prvků a sítí kritické infrastruktury.*“

ZÁVĚR

Hodnocení odolnosti prvku kritické infrastruktury patří k velmi významným oblastem pro zajištění plynulého provozu kritické infrastruktury. V dnešní době, kdy v rámci propojitelnosti a kritičnosti, jsou na sebe prvky navzájem závislé, se důležitost odolnosti jednotlivých prvků zvyšuje. Jakákoliv negativní změna může mít nedozírné následky na ostatní prvky. Z tohoto důvodu se hodnocení odolnosti stává klíčovým prvkem v ochraně kritické infrastruktury.

Ochrana kritické infrastruktury prošla během historie vývojem a změnami. Právě vývoj kritické infrastruktury v jednotlivých státech a organizacích jsem zmapoval v teoretické části mé práce. Dále se v ní zabývám principy hodnocení odolnosti a způsoby ochrany, včetně legislativní rešerše.

Poznatků z teoretické části jsem využil v praktické části při vytváření nástroje pro multikriteriální hodnocení odolnosti kritické infrastruktury. Právě multikriteriálního hodnocení jsem využil k zvýšení přesnosti výsledku, jelikož existuje mnoho faktorů, které ovlivňují odolnost prvku kritické infrastruktury. Tyto faktory jsem zhodnotil, přiřadil jim hodnoty a zpracoval do podoby nástroje pro jejich hodnocení. Při zpracování nástroje jsem vycházel především z prací týkajících se odolnosti kritické infrastruktury pana Ing. Martina Hromady Ph.D., mého vedoucího diplomové práce, a pana doc. Ing. Lud'ka Lukáše, CSc.

Při zpracování této metody a matematických vztahů do formy jednoduchého nástroje pro hodnocení odolnosti jsem uvažoval nad různými způsoby zpracování. Nakonec jsem se rozhodl dle hesla „V jednoduchosti je síla“ pro zpracování do podoby jednoduchých rozhodovacích tabulek v prostředí MS Excel 2010. Právě tento nástroj pro multikriteriální hodnocení odolnosti prvku kritické infrastruktury Nemocniční péče, který jsem pojmenoval Křížák, je výsledkem mé práce.

ZÁVĚR V ANGLIČTINĚ

Evaluation of the resistance elements of critical infrastructure is one of the most important areas to ensure smooth operation of critical infrastructure. Nowadays, when the connectivity and criticality, are themselves interdependent elements, the importance of resistance of elements increases. Any negative change can have dire consequences on other elements. Therefore, evaluation of resistance becomes a key element in the critical infrastructure protection.

Critical infrastructure protection has undergone throughout history, evolution and change. In the theoretical part of my work, I mapped the development of critical infrastructure in individual countries and organizations. I am dealing with the principles of evaluating resistance and protection methods, including legislative research.

Knowledge from the theoretical part was used in the creation of multi-criteria evaluation resilience tool. I used multi-criteria evaluation to increase the accuracy of the results, since there are many factors that affect the resistance elements of critical infrastructure. These factors've reviewed, assign them values and processed into the tool for their evaluation. During processing tools designing I was inspired primarily by the works about the resilience of critical infrastructure written by Mr. Ing. Martin Hromada Ph.D., Head of my thesis, and Mr. doc. Ing. Luděk Lukáš, CSc.

In developing this method and mathematical relationships to form a simple tool for evaluating the resistance I was thinking of different ways of processing. I decided according to the motto "Keep it simple" for processing into a simple decision tables in MS Excel 2010. Tool for multi-criteria evaluation of critical infrastructure resistance element Hospital care, which I named Crusader, is the result of my work.

SEZNAM POUŽITÉ LITERATURY

- [1] Zákon č. 240/2000 Sb., o krizovém řízení a změně některých zákonů (krizový zákon), ve znění zákona č. 320/2002 Sb., 127/2005 Sb., 112/2006 Sb., 267/2006 Sb. a 110/2007 Sb.
- [2] Zákon č. 239/2000 Sb., o integrovaném záchranném systému a o změně některých zákonů, ve znění zákona č. 320/2002 Sb., 20/2004 Sb., 186/2006 Sb. a 267/2006 Sb.
- [3] Zákon č. 241/2000 Sb., o hospodářských opatřeních pro krizové stavy a o změně některých souvisejících zákonů, ve znění zákona č. 320/2002 Sb., 354/2003 Sb., 237/2004 Sb., 413/2005 Sb. a 444/2005 Sb.
- [4] Zákon č. 133/1985 Sb., o požární ochraně, ve znění zákona č. 425/1990 Sb., 40/1994 Sb., 203/1994 Sb., 163/1998 Sb., 71/2000 Sb., 237/2000 Sb., 320/2002 Sb., 413/2005 Sb., 186/2006 Sb. a 267/2006 Sb.
- [5] VEVERKA, I., *Vybrané kapitoly krizového řízení pro záchranářství*, 1. vydání Praha, 2003, 175 s., ISBN: 80-7251-126-2
- [6] Hasičský záchranný sbor České republiky. Integrovaný záchranný systém. HZS ČR. [Online] červen 26, 2010. [cit. 2013-02-20] <http://www.hzscr.cz/clanek/prehled-zakladnich-pravnich-predpisu-v-oblasti-krizoveho-rizeni.aspx>.
- [7] Usnesení BRS č. 204/2001 k Informacím ke zpracování definice a stanovení rozsahu základních funkcí státu za krizových situací
- [8] LINHART, Petr; RICHTER, Rostislav. Ochrana kritické infrastruktury [online]. *112 – odborný časopis požární ochrany integrovaného záchranného systému a ochrany obyvatelstva*. 2003. Dostupný z http://www.hzscr.cz/soubory/casopis_112_rok_2003.pdf
- [9] KOVAŘÍK, J., *Kritická infrastruktura a ochrana obyvatelstva*, Ochrana obyvatel, 2007, Ochrana kritické infrastruktury, s. 145-153, ISBN: 80-86634-51-5
- [10] Usnesení BRS č. 30/2007 ke Zprávě o řešení problematiky kritické infrastruktury v České republice
- [11] Komise evropských společenství. *Zelená kniha o evropském programu na ochranu kritické infrastruktury*. *EUR-Lex*. [Online] listopad 17, 2005. [cit. 2013-02-25] http://eur-lex.europa.eu/LexUriServ/site/cs/com/2005/com2005_0576cs01.pdf.
- [12] NATO's role in Critical Infrastructure Protection. In: *European Parliament online* [online]. 2008 [cit. 2013-04-23]. Dostupné z: http://www.europarl.europa.eu/hearings/20070131/libe/nato_role_cip_en.pdf
- [13] USA. Presidential Decision Directive 62. In: *Presidential Decision Directive* [online]. 1998. Dostupné z: <http://www.fas.org/irp/offdocs/pdd-62.htm>
- [14] USA. Presidential Decision Directive 63. In: *Presidential Decision Directive* [online]. 1998. Dostupné z: <http://www.fas.org/irp/offdocs/pdd-63.htm>
- [15] KRULÍK, Oldřich. Místo a úkoly ministerstva vnitřní bezpečnosti USA. *Obrana a strategie* [online]. 2003, č. 2 [cit. 2013-05-02]. Dostupné z: www.defenceandstrategy.eu/filemanager/files/file.php?file=6363
- [16] MOZGA, J., VÍTEK M., KOVAŘÍK F., *Kritická infrastruktura společnosti*, Hradec Králové: Gaudeamus, 2008, 1. vydání, 156 s. ISBN : 978-80-7041-299-2
- [17] *Kritická infrastruktura. Hasičský záchranný sbor České republiky* [online]. 2010 [cit. 2013-02-28]. Dostupné z: <http://www.hzscr.cz/clanek/web-krizove-rizeni-a-cnp-kriticka-infrastruktura-kriticka-infrastruktura.aspx>

- [28] Schutz Kritischer Infrastruktur: Risikomanagement im Krankenhaus. In: *Leitfaden zur Identifikation und Reduzierung von Ausfallrisiken in Kritischen Infrastrukturen des Gesundheitswesens* [online]. Bonn: BBK, 2008. Dostupné z: http://www.bbk.bund.de/cln_007/nn_398010/SharedDocs/Publikationen/Praxis__Bevoelkerungsschutz/Langfassung__Leitfaden__Krankenh__Risiko-Kritis.html__nnn=true
- [19] PROCHÁZKOVÁ D. Kritická infrastruktura a její problémy. Ostrava: VŠB a SPBI, 2008, 77 s. ISBN 978-80-7385-034-0.
- [20] Critical Infrastructure, Interdependencies, and Resilience. *Engineering for the Threat of Natural Disasters* [online]. 2007, roč. 37, č. 1. Dostupné z: <http://www.nae.edu/Publications/Bridge/EngineeringfortheThreatofNaturalDisasters/CriticalInfrastructureInterdependenciesandResilience.aspx>
- [21] Plán krizové připravenosti subjektu kritické infrastruktury. *TPL spol. s.r.o.* [online]. 2010 [cit. 2013-03-11]. Dostupné z: <http://www.tlp-emergency.com/pkpski.html>
- [22] LUKÁŠ, L.; HROMADA, M.; Možnosti hodnocení odolnosti kritické infrastruktury/ Evaluating the Resistance of Critical Infrastructure, Bezpečnost v informační společnosti, Brno, 2009.
- [23] ERICSON, Clifton A. *Hazard analysis techniques for system safety* [online]. Hoboken, NJ: Wiley-Interscience, c2005, 499 s. ISBN 978-0-471-72019-5.
- [24] 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.
- [25] LUKÁŠ, L.; HROMADA, M. *Multicriterial Evaluation of Critical Infrastructure Element Protection in Czech Republic*. 2012.
- [26] 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.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

BRS	Bezpečnostní rada státu
CPNI	The Centre for the Protection of National Infrastructure
ČNB	Česká národní banka
ČR	Česká Republika
DHS	The Department of Homeland Security
EKI	Evropská kritická infrastruktura
EPA	The United States Environmental Protection Agency
EPCIP	The European Programme for Critical Infrastructure Protection
EU	The European Union
FMEA	Failure Mode and Effect Analysis
HAZOP	Hazard Operation Process
HDD	Hard Disk Drive
HLS	Homeland Security Department
KARS	Kvalitativní analýza rizik s využitím jejich souvstažností
KI	Kritická infrastruktura
MS	Microsoft
NATO	The North Atlantic Treaty Organisation
PC	Personal Computer
PCCIP	The President's Commission on Critical Infrastructure Protection
PDD	Presidential Decision Directives
PHA	Preliminary Hazard Analysis
Q(t)	kvalita v čase t
RAMCAP	Risk Analysis and Management of Critical Asset Protection
SCEPC	Senior Civil Emergency Planning Committee

t	čas
USA	The United States of America
VCNP	Výbor pro civilní nouzové plánování

SEZNAM OBRÁZKŮ

Obrázek 1. Vlajka EU	17
Obrázek 2. Vlajka NATO	20
Obrázek 3. Vlajka USA	21
Obrázek 4. Útok na WTC	22
Obrázek 5. Znak Úřadu pro vnitřní bezpečnost	23
Obrázek 6. Prvky kritické infrastruktury	27
Obrázek 7. Zdravotní péče [18]	28
Obrázek 8. Přednemocniční neodkladná péče [18]	29
Obrázek 9. Nemocniční péče [18]	29
Obrázek 10. Ochrana veřejného zdraví [18]	30
Obrázek 11. Výroba, skladování a distribuce léčiv a zdravotnických prostředků [18]	30
Obrázek 12. Propojitelnost prvků kritické infrastruktury [18]	31
Obrázek 13. List Stanovení rizikovosti	51

SEZNAM TABULEK

Tabulka 1. Tabulka souvztažnosti rizik	47
Tabulka 2. Vlastnosti segmentů	49
Tabulka 3. Bodová hodnota pro vyjádření pravděpodobnosti výskytu hrozby	50
Tabulka 4. Bodová hodnota pro vyjádření účinku hrozby	50
Tabulka 5. Určení hodnoty rizikovosti	52
Tabulka 6. Určení vah jednotlivých oblastí	53
Tabulka 7. Určení míry kvality přijatých opatření	54
Tabulka 8. Hodnocení strukturální robustnosti	56
Tabulka 9. Doplňující tabulka hodnocení strukturální robustnosti	56
Tabulka 10. Krizová připravenost	58
Tabulka 11: Bodové hodnocení indexů strukturální robustnosti	79
Tabulka 12: Bodové ohodnocení struktury uzal	80
Tabulka 13: Převodní tabulka I_p na I_t	80

SEZNAM GRAFŮ

Graf 1. Kvalita infrastruktury v čase	35
Graf 2. Graf souvztažnosti rizik.....	49

SEZNAM PŘÍLOH

- P I Seznam oblastí národní kritické infrastruktury navrhovaných v roce 2004
- P II Indicative list of critical infrastructure sectors
- P III Bodové hodnocení indexů strukturální robustnosti
- P IV Křižák/Crussader

**PŘÍLOHA P I: SEZNAM OBLASTÍ NÁRODNÍ KRITICKÉ
INFRASTRUKTURY NAVRHOVANÝCH V ROCE 2004**

	Oblasti kritické infrastruktury	Produkt nebo služba
1.	Energetika	1.1 Elektřina
		1.2 Plyn
		1.3 Tepelná energie
		1.4 Ropa a ropné produkty
2.	Vodní hospodářství	2.1 Zásobování pitnou a užitkovou vodou
		2.2 Zabezpečení a správa povrchových vod a podzemních zdrojů vody
		2.3 Systém odpadních vod
3.	Potravinařství a zemědělství	3.1 Produkce potravin
		3.2 Péče o potraviny
		3.3 Zemědělská výroba
4.	Zdravotní péče	4.1 Přednemocniční neodkladná péče
		4.2 Nemocniční péče
		4.3 Ochrana veřejného zdraví
		4.4 Distribuce léčiv
5.	Doprava	5.1 Silniční
		5.2 Železniční
		5.3 Letecká
		5.4 Vnitrozemská vodní
6.	Komunikační a informační systémy	6.1 Služby pevných komunikačních sítí
		6.2 Služby mobilních komunikačních sítí
		6.3 Radiová komunikace a navigace
		6.4 Satelitní komunikace
		6.5 Televizní a rádiové vysílání
		6.6 Přístup k internetu a k datovým službám
		6.7 Poštovní a kurýrní služby
7.	Bankovní a finanční sektor	7.1 Správa veřejných financí
		7.2 Bankovníctví
		7.3 Pojišťovnictví
		7.4 Kapitálový trh
8.	Nouzové služby	8.1 Policie ČR

		jednotky požární ochrany
		8.2 Hasičský záchranný sbor ČR
		8.3 Zdravotnické záchranné služby
		8.4 Letecká zdravotnická záchranná služba
		8.5 Armáda ČR
		8.6 Radiační monitorování
		8.7 Předpovědní, varovná a hlásná služba
9.	Veřejná správa	9.1 Sociální ochrana a zaměstnanost
		9.2 Diplomacie
		9.3 Výkon justice a vězeňství
		9.4 Státní správa a samospráva
10.	Odpadové hospodářství	10.1 Nakládání s odpady
		10.2 Radioaktivní odpady

**PŘÍLOHA P II: INDICATIVE LIST OF CRITICAL
INFRASTRUCTURE SECTORS**

	Sector	Product or service
1.	Energy	1 Oil and gas production, refining, treatment and storage, including pipelines
		2 Electricity generation
		3 Transmission of electricity, gas and oil
		5 Information system and network protection
2.	Information, Communication Technologies, ICT	6 Instrumentation automation and control systéme (SCADA etc.)
		7 Internet
		8 Provision of fixed telecommunications
		9 Provision of mobile telecommunications
		10 Radio communication and navigation
		11 Satellite communication
		12 Broadcasting
3.	Water	III Water 13 Provision of drinking water
		14 Control of water duality
		15 Stemming and control of water quantity
4.	Food	16 Provision of food and safeguarding food safety and security
5.	Health	17 Medical and hospital care
		18 Medicines, serums, vaccines and pharmaceuticals
		19 Bio-laboratories and bio-agents
6.	Financial	20 Payment services/payment structures (private)
		21 Government financial assignment
7.	Public & Legal Order and Safety	22 Maintaining public & legal order, safety and security
		23 Administration of justice and detention
8.	Civil administration	24 Government functions
		25 Armed forces

		26 Civil administration services
		27 Emergency services
		28 Postal and courier services
9.	Transport	29 Road transport
		30 Rail transport
		31 Air traffic
		32 Inland waterways transport
		33 Ocean and short-sea shipping
10.	Chemical and nuclear industry	34 Production and storage/processing of chemical and nuclear substance
		35 Pipelines of dangerous goods (chemical substances)
11	Space and Research	36 Space
		37 Research

PŘÍLOHA P III: BODOVÉ HODNOCENÍ INDEXŮ STRUKTURÁLNÍ ROBUSTNOSTI

Tabulka 11: Bodové hodnocení indexů strukturální robustnosti

typ topologie <i>index topologie - I_t</i>	Bod		plocha			linie		síť
	do 1000 m ²	nad 1000 m ²	do 1 km ²	1 – 10 km ²	nad 10 km ²	do 10 km	nad 10 km	metodika
	3	2	2	1	0	1	0	0 - 3
složitost <i>index složitosti - I_s</i>	jednoduchý (do 10 zaměstnanců)		střední (10 – 100 zaměstnanců)			složitý (nad 100 zaměstnanců)		
	2		1			0		
počet klíčových technologií <i>index klíčových technologií - I_{kt}</i>	do 2 technologií		3 – 4 technologií			5 a více technologií		
	2		1			0		
flexibilita <i>index flexibility - I_f</i>	ne					Ano		
	0					2		
redundance <i>index redundance - I_r</i>	ne					Ano		
	0					1		
perimetrická ochrana <i>index perimetrické ochrany - I_{po}</i>	bez ochrany		lokální			Úplná		
	0		1			2		

Tabulka 12: Bodové ohodnocení struktury uzlu

typ topologie I_s	sběrnice/bus	hvězda/kruh	strom	polygon
	0	4	8	12
počet klíčových uzlů I_{ku}	1 uzel	2 uzly	3 uzly	4 uzly a více nebo žádný
	0	3	6	9
celkový počet uzlů I_c	do 5 uzlů	6 – 15 uzlů	16 – 40 uzlů	nad 40 uzlů
	0	2	2	6
průměrný počet hran na uzel I_h	do 1,5 hrany	1,6 – 2,2 hrany	2,3 – 3 hrany	více jak 3 hrany
	0	1	2	3

$$I_b = I_s + I_{ku} + I_c + I_h$$

Tabulka 13: Převodní tabulka I_b na I_t

I_b - počet bodů	index topologie I_t
0 – 7	0
8 – 15	1
16 – 22	2
23 – 30	3

PŘÍLOHA P IV: KŘÍŽAK/CRUSSADER

Menu

Zvolte jazyk / Choose your language

čeština



english

	Nástroj pro multikriteriální hodnocení odolnosti kritické infrastruktury Křížak pro prvek Nemocniční péče									
	Popis nástroje Nástroj je situován do sešitu MS Excelu, obsahuje uživateli dostupné listy pro dílčí výpočty. Jeho součástí jsou makra ve VisualBasic, které zabezpečují funkci některých ovládacích prvků. Hodnoty rizikovosti lze zadávat pouze do buněk k tomu určených, ostatní buňky jsou chráněné proti případnému přepsání.									
	<table border="1"><tr><td>Koeficient závislosti</td><td></td></tr><tr><td>Koeficient robustnosti</td><td></td></tr><tr><td>Koeficient připravenosti</td><td></td></tr><tr><td>Odolnost prvku kritické infrastruktury</td><td></td></tr><tr><td>Slovní hodnocení</td><td></td></tr></table> <p>Export</p>		Koeficient závislosti		Koeficient robustnosti		Koeficient připravenosti		Odolnost prvku kritické infrastruktury	
Koeficient závislosti										
Koeficient robustnosti										
Koeficient připravenosti										
Odolnost prvku kritické infrastruktury										
Slovní hodnocení										
	autor: A. Venclík datum: 22.5.2013									

Zvolte jazyk / Choose your language

čeština

english

	Multi-criteria Evaluation of Critical Infrastructure Resilience Tool Crussader for facility Health Care									
	Tool description The tool is located in MS Excel, contains user accessible pages for partial calculations. It includes macros in VisualBasic, which provide some of function controls. Values of risk can only be entered in the designated cells, other cells are protected against eventual overwriting.									
	<table border="1"><tr><td>The coefficient of dependence</td><td></td></tr><tr><td>The coefficient of robustness</td><td></td></tr><tr><td>The coefficient of preparedness</td><td></td></tr><tr><td>Critical infrastructure resistance</td><td></td></tr><tr><td>Verbal rating</td><td></td></tr></table> <p>Export</p>		The coefficient of dependence		The coefficient of robustness		The coefficient of preparedness		Critical infrastructure resistance	
The coefficient of dependence										
The coefficient of robustness										
The coefficient of preparedness										
Critical infrastructure resistance										
Verbal rating										
	author: A. Venclík date: 22.5.2013									

R

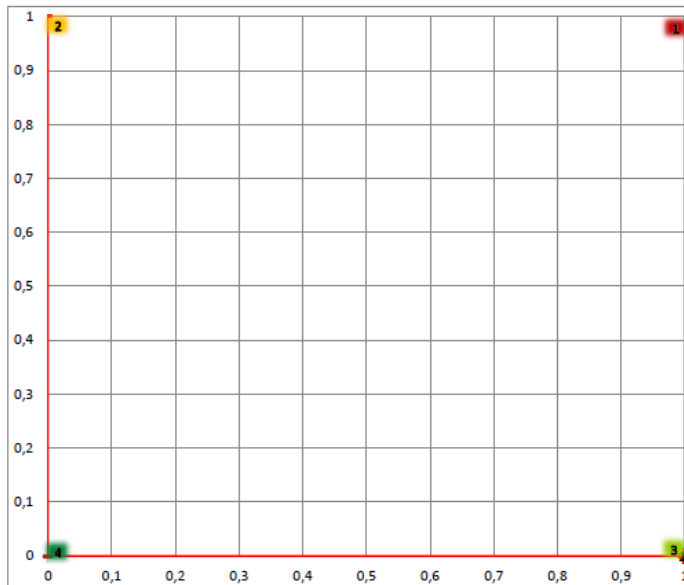
i	Tabulka souvstažnosti	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Energetika																											
1	Krátkodobý výpadek elektřiny	+																									
2	Dlouhodobý výpadek elektřiny		+																								
3	Výpadek dodávky vody			+																							
4	Výpadek dodávky plynu				+																						
Přírodní vlivy																											
5	Povodeň, záplava, zátopa					+																					
6	Dlouhotrvající sucho						+																				
7	Extrémní vedro a sucho							+																			
8	Silný mráz								+																		
9	Pandemie, epidemie									+																	
Rizika spojená s příčiněním lidského faktoru																											
10	Požár											+															
11	Výbuch												+														
12	Krádež													+													
13	Unik škodlivin v okolí														+												
14	Výpadek v oblasti logistika															+											
15	Virtuální napadení																+										
16	Teroristický útok																	+									
17	Narušení veřejného pořádku																		+								
18	Nedostupnost personálu																			+							
19	Náhly nápor pacientů																				+						
20	Technické poruchy																					+					
21	Sabotáž																						+				
22	Násilná kriminální činnost																							+			
23	Vandalismus																								+		
24	Rabování																									+	
25	Rezerva 1																										+
26	Rezerva 2																										+

Reset

i	Table of correlations	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Energetics																											
1	Short-term electricity outage	+																									
2	Long-term electricity outage		+																								
3	Outage of water supply			+																							
4	Outage of gas supply				+																						
Natural impacts																											
5	Flood					+																					
6	Prolonged drought						+																				
7	Extreme heat and drought							+																			
8	Thick frost								+																		
9	Pandemic, epidemic									+																	
Risks associated with the human factor																											
10	Conflagration											+															
11	Explosion												+														
12	Robbery													+													
13	Leaks of pollutants in the area														+												
14	Outage in logistics															+											
15	The virtual attack																+										
16	The terrorist attack																	+									
17	Disruption of public order																		+								
18	Unavailability of staff																			+							
19	Sudden rush of patients																				+						
20	Technical failures																					+					
21	Sabotage																						+				
22	Violent criminal activity																							+			
23	Acts of vandalism																								+		
24	Plundering																									+	
25	Reserve 1																										+
26	Reserve 2																										+

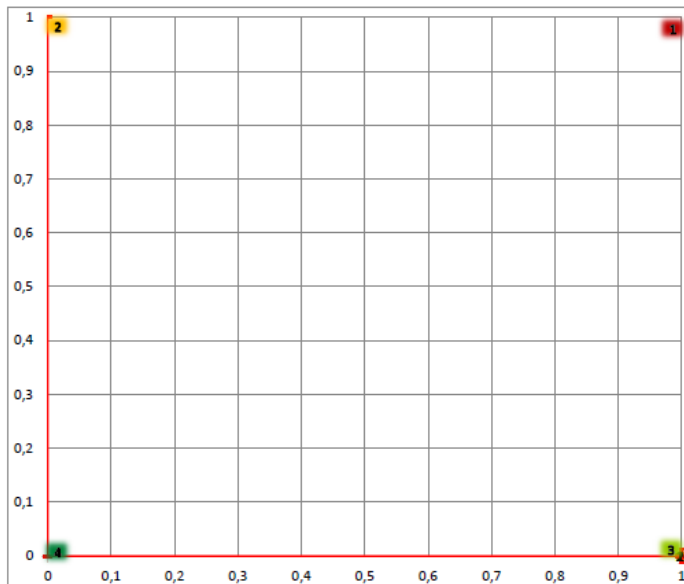
Reset

A, P



S	Vlastnosti segmentu
1	Oblast primárně i sekundárně nebezpečných rizik
2	Oblast sekundárně nebezpečných rizik
3	Oblast primárně nebezpečných rizik
4	Oblast relativně bezpečná

i	Rizika	Aktiva	Pasiva	S
Energetika				
1	Krátkodobý výpadek elektřiny	0,00	0,00	1
2	Dlouhodobý výpadek elektřiny	0,00	0,00	1
3	Výpadek dodávky vody	0,00	0,00	1
4	Výpadek dodávky plynu	0,00	0,00	1
Přírodní vlivy				
5	Povodeň, záplava, zátopa	0,00	0,00	1
6	Dlouhotrvající sucho	0,00	0,00	1
7	Extrémní vedro a sucho	0,00	0,00	1
8	Silný mráz	0,00	0,00	1
9	Pandemie, epidemie	0,00	0,00	1
Rizika spojená s přičiněním lidského faktoru				
10	Požár	0,00	0,00	1
11	Výbuch	0,00	0,00	1
12	Krádež	0,00	0,00	1
13	Únik škodlivin v okolí	0,00	0,00	1
14	Výpadek v oblasti logistika	0,00	0,00	1
15	Virtuální napadení	0,00	0,00	1
16	Teroristický útok	0,00	0,00	1
17	Narušení veřejného pořádku	0,00	0,00	1
18	Nedostupnost personálu	0,00	0,00	1
19	Náhly nápor pacientů	0,00	0,00	1
20	Technické poruchy	0,00	0,00	1
21	Sabotáž	0,00	0,00	1
22	Násilná kriminální činnost	0,00	0,00	1
23	Vandalismus	0,00	0,00	1
24	Rabování	0,00	0,00	1



S	Segment properties
1	Areas of primary and secondary dangerous risks
2	Areas of secondary dangerous risks
3	Areas of primary dangerous risks
4	Relatively safe area

i	Risks	Active	Passive	S
Energetics				
1	Short-term electricity outage	0,00	0,00	1
2	Long-term electricity outage	0,00	0,00	1
3	Outage of water supply	0,00	0,00	1
4	Outage of gas supply	0,00	0,00	1
Natural impacts				
5	Flood	0,00	0,00	1
6	Prolonged drought	0,00	0,00	1
7	Extreme heat and drought	0,00	0,00	1
8	Thick frost	0,00	0,00	1
9	Pandemic, epidemic	0,00	0,00	1
Risks associated with the human factor				
10	Conflagration	0,00	0,00	1
11	Explosion	0,00	0,00	1
12	Robbery	0,00	0,00	1
13	Leaks of pollutants in the area	0,00	0,00	1
14	Outage in logistics	0,00	0,00	1
15	The virtual attack	0,00	0,00	1
16	The terrorist attack	0,00	0,00	1
17	Disruption of public order	0,00	0,00	1
18	Unavailability of staff	0,00	0,00	1
19	Sudden rush of patients	0,00	0,00	1
20	Technical failures	0,00	0,00	1
21	Sabotage	0,00	0,00	1
22	Violent criminal activity	0,00	0,00	1
23	Acts of vandalism	0,00	0,00	1
24	Plundering	0,00	0,00	1

Hrzi

i	Rizika	S	P	N	Hrzi
Energetika					
1	Krátkodobý výpadek elektřiny	1	0	0	0,00
2	Dlouhodobý výpadek elektřiny	1	0	0	0,00
3	Výpadek dodávky vody	1	0	0	0,00
4	Výpadek dodávky plynu	1	0	0	0,00
Přírodní vlivy					
5	Povodeň, záplava, zátopa	1	0	0	0,00
6	Dlouhotrvající sucho	1	0	0	0,00
7	Extrémní vedro a sucho	1	0	0	0,00
8	Silný mráz	1	0	0	0,00
9	Pandemie, epidemie	1	0	0	0,00
Rizika spojená s přičiněním lidského faktoru					
10	Požár	1	0	0	0,00
11	Výbuch	1	0	0	0,00
12	Krádež	1	0	0	0,00
13	Únik škodlivin v okolí	1	0	0	0,00
14	Výpadek v oblasti logistika	1	0	0	0,00
15	Virtuální napadení	1	0	0	0,00
16	Teroristický útok	1	0	0	0,00
17	Narušení veřejného pořádku	1	0	0	0,00
18	Nedostupnost personálu	1	0	0	0,00
19	Náhly nápor pacientů	1	0	0	0,00
20	Technické poruchy	1	0	0	0,00
21	Sabotáž	1	0	0	0,00
22	Násilná kriminální činnost	1	0	0	0,00
23	Vandalismus	1	0	0	0,00
24	Rabování	1	0	0	0,00

Reset

P	Bodová hodnota pro vyjádření pravděpodobnosti výskytu hrozby
0	Nepravděpodobná nebo nehodnocená
1	Velmi málo pravděpodobná
2	Málo pravděpodobná
3	Středně pravděpodobná
4	Značně pravděpodobná
5	Vysoce pravděpodobná až jistá

N	Bodová hodnota pro vyjádření účinku hrozby
0	Žádný
1	Nízký
2	Nevýznamný
3	Střední
4	Vysoký
5	Velmi vysoký

i	Risks	S	P	N	Hrzi
Energetics					
1	Short-term electricity outage	1	0	0	0,00
2	Long-term electricity outage	1	0	0	0,00
3	Outage of water supply	1	0	0	0,00
4	Outage of gas supply	1	0	0	0,00
Natural impacts					
5	Flood	1	0	0	0,00
6	Prolonged drought	1	0	0	0,00
7	Extreme heat and drought	1	0	0	0,00
8	Thick frost	1	0	0	0,00
9	Pandemic, epidemic	1	0	0	0,00
Risks associated with the human factor					
10	Conflagration	1	0	0	0,00
11	Explosion	1	0	0	0,00
12	Robbery	1	0	0	0,00
13	Leaks of pollutants in the area	1	0	0	0,00
14	Outage in logistics	1	0	0	0,00
15	The virtual attack	1	0	0	0,00
16	The terrorist attack	1	0	0	0,00
17	Disruption of public order	1	0	0	0,00
18	Unavailability of staff	1	0	0	0,00
19	Sudden rush of patients	1	0	0	0,00
20	Technical failures	1	0	0	0,00
21	Sabotage	1	0	0	0,00
22	Violent criminal activity	1	0	0	0,00
23	Acts of vandalism	1	0	0	0,00
24	Plundering	1	0	0	0,00

Reset

P	The point value for the expression of probability of occurrence threats
0	Improbable or unrated
1	Very improbable
2	Not very probable
3	Moderately probable
4	Very propable
5	Highly probable or certain

N	The point value for expressing the effect of threats
0	None
1	Low
2	Insignificant
3	Medium
4	High
5	Very high

Ks

Produkt nebo služba	Je prvek Nemocniční péče závislý na jiném produktu (službě)?		Míra závislost
Zásobování elektřinou	<input type="radio"/> ano	<input type="radio"/> ne	0
Zásobování plynem	<input type="radio"/> ano	<input type="radio"/> ne	0
Zásobování vodou	<input type="radio"/> ano	<input type="radio"/> ne	0
Zásobování potravinami	<input type="radio"/> ano	<input type="radio"/> ne	0
Funkčnost komunikačních sítí	<input type="radio"/> ano	<input type="radio"/> ne	0
Přístup k datovým službám	<input type="radio"/> ano	<input type="radio"/> ne	0
Dostupnost personálu	<input type="radio"/> ano	<input type="radio"/> ne	0
Zásobování zdravotnickým materiálem	<input type="radio"/> ano	<input type="radio"/> ne	0
Předpovědní, varovná a hlásná služba	<input type="radio"/> ano	<input type="radio"/> ne	0
Veřejná správa	<input type="radio"/> ano	<input type="radio"/> ne	0
Doprava	<input type="radio"/> ano	<input type="radio"/> ne	0
	Reset	Ks	0,00

Product or Service	Is the element Hospital care dependent on another product		Depend ency
Electricity supply	<input type="radio"/> yes	<input type="radio"/> no	0
Gas supply	<input type="radio"/> yes	<input type="radio"/> no	0
Water supply	<input type="radio"/> yes	<input type="radio"/> no	0
Food supply	<input type="radio"/> yes	<input type="radio"/> no	0
Functionality of communication networks	<input type="radio"/> yes	<input type="radio"/> no	0
Access to data services	<input type="radio"/> yes	<input type="radio"/> no	0
Availability of staff	<input type="radio"/> yes	<input type="radio"/> no	0
Supply of medical materials	<input type="radio"/> yes	<input type="radio"/> no	0
Forecasting and warning service	<input type="radio"/> yes	<input type="radio"/> no	0
Public Administration	<input type="radio"/> yes	<input type="radio"/> no	0
Transportation	<input type="radio"/> yes	<input type="radio"/> no	0
	Reset	Ks	0,00

Krz

Porovnej důležitost jednotlivých oblastí			
Fyzická a objektová bezpečnost	<input type="radio"/>	<input type="radio"/>	Informační bezpečnost
Fyzická a objektová bezpečnost	<input type="radio"/>	<input type="radio"/>	Řízení kontinuity činnosti organizace
Fyzická a objektová bezpečnost	<input type="radio"/>	<input type="radio"/>	Administrativní bezpečnost
Informační bezpečnost	<input type="radio"/>	<input type="radio"/>	Řízení kontinuity činnosti organizace
Informační bezpečnost	<input type="radio"/>	<input type="radio"/>	Administrativní bezpečnost
Řízení kontinuity činnosti organizace	<input type="radio"/>	<input type="radio"/>	Administrativní bezpečnost

Krz	0,00
------------	------

Reset

Fyzická a objektová bezpečnost	Ano	Ne
Byl proveden bezp. audit?	<input type="radio"/>	<input type="radio"/>
Je objekt napojen na PPC PČR?	<input type="radio"/>	<input type="radio"/>
Je v objektu nainstalován ACCESS?	<input type="radio"/>	<input type="radio"/>
Je v objektu nainstalován CCTV	<input type="radio"/>	<input type="radio"/>
Je v objektu nainstalován EPS?	<input type="radio"/>	<input type="radio"/>
Je v objektu nainstalován IH&S?	<input type="radio"/>	<input type="radio"/>
Je v objektu přítomna ostraha 24/7?	<input type="radio"/>	<input type="radio"/>
Perimetrická ochrana vyšší než 2 m?	<input type="radio"/>	<input type="radio"/>
Školení zaměstnanců	<input type="radio"/>	<input type="radio"/>
Prevence	<input type="radio"/>	<input type="radio"/>

Informační bezpečnost	Ano	Ne
Antivir	<input type="radio"/>	<input type="radio"/>
Firewall	<input type="radio"/>	<input type="radio"/>
Identifikace a autentizace	<input type="radio"/>	<input type="radio"/>
RAID pole	<input type="radio"/>	<input type="radio"/>
Řízení přístupu	<input type="radio"/>	<input type="radio"/>
Řízení síťového provozu	<input type="radio"/>	<input type="radio"/>
Šifrování 256 bit	<input type="radio"/>	<input type="radio"/>
Zajištění sterility prostředí	<input type="radio"/>	<input type="radio"/>
Školení zaměstnanců	<input type="radio"/>	<input type="radio"/>
Prevence	<input type="radio"/>	<input type="radio"/>

Řízení kontinuity činnosti organizace	Ano	Ne
Audit řízení kontinuity	<input type="radio"/>	<input type="radio"/>
Kontroly kriz. kontaktů	<input type="radio"/>	<input type="radio"/>
Návrh postupu detekce rušivé události	<input type="radio"/>	<input type="radio"/>
Zajištění lidských rezerv	<input type="radio"/>	<input type="radio"/>
Udržování schopnosti řízení rizik	<input type="radio"/>	<input type="radio"/>
Vytvoření plánu kriz. připravenosti	<input type="radio"/>	<input type="radio"/>
Zajištění dodávek léčiv	<input type="radio"/>	<input type="radio"/>
Zajištění náhradních dodávek energií	<input type="radio"/>	<input type="radio"/>
Školení zaměstnanců	<input type="radio"/>	<input type="radio"/>
Prevence	<input type="radio"/>	<input type="radio"/>

Administrativní bezpečnost	Ano	Ne
Archivace dat	<input type="radio"/>	<input type="radio"/>
Identifikace zdrojů osobních dat	<input type="radio"/>	<input type="radio"/>
Kontrola přístupů	<input type="radio"/>	<input type="radio"/>
Organizační opatření k ochraně	<input type="radio"/>	<input type="radio"/>
Skartace materiálů	<input type="radio"/>	<input type="radio"/>
Šifrování	<input type="radio"/>	<input type="radio"/>
Technická opatření k ochraně	<input type="radio"/>	<input type="radio"/>
Zabezpečení automat. zpracování	<input type="radio"/>	<input type="radio"/>
Školení zaměstnanců	<input type="radio"/>	<input type="radio"/>
Prevence úniku dat	<input type="radio"/>	<input type="radio"/>

Compare the importance of individual areas			
Physical and object security	<input type="radio"/>	<input type="radio"/>	IT security
Physical and object security	<input type="radio"/>	<input type="radio"/>	Business continuity management
Physical and object security	<input type="radio"/>	<input type="radio"/>	Administrative security
IT security	<input type="radio"/>	<input type="radio"/>	Business continuity management
IT security	<input type="radio"/>	<input type="radio"/>	Administrative security
Business continuity management	<input type="radio"/>	<input type="radio"/>	Administrative security

Krz	0,00
------------	------

Reset

Physical and object security	Yes	No
Was made sec. audit?	<input type="radio"/>	<input type="radio"/>
Is alarm connected to the Police?	<input type="radio"/>	<input type="radio"/>
Is ACCESS system installed in object?	<input type="radio"/>	<input type="radio"/>
Is CCTV system installed in object?	<input type="radio"/>	<input type="radio"/>
Is Fire alarm syst. installed in object?	<input type="radio"/>	<input type="radio"/>
Is security system installed in object?	<input type="radio"/>	<input type="radio"/>
Is sec. guard present in object (24/7)?	<input type="radio"/>	<input type="radio"/>
Perimeter protection higher than 2 m?	<input type="radio"/>	<input type="radio"/>
Staff training	<input type="radio"/>	<input type="radio"/>
Prevention	<input type="radio"/>	<input type="radio"/>

IT security	Yes	No
Antivir	<input type="radio"/>	<input type="radio"/>
Firewall	<input type="radio"/>	<input type="radio"/>
Identification and authentication	<input type="radio"/>	<input type="radio"/>
RAID	<input type="radio"/>	<input type="radio"/>
Access control	<input type="radio"/>	<input type="radio"/>
Traffic Control	<input type="radio"/>	<input type="radio"/>
256-bit encryption	<input type="radio"/>	<input type="radio"/>
Ensuring sterility of environment	<input type="radio"/>	<input type="radio"/>
Staff training	<input type="radio"/>	<input type="radio"/>
Prevention	<input type="radio"/>	<input type="radio"/>

Business continuity management	Yes	No
Audit of Business Continuity Manag.	<input type="radio"/>	<input type="radio"/>
Crisis contacts checks	<input type="radio"/>	<input type="radio"/>
Disruptive events detection proposal	<input type="radio"/>	<input type="radio"/>
Human reserves ensuring	<input type="radio"/>	<input type="radio"/>
Maintaining the ability to risk control	<input type="radio"/>	<input type="radio"/>
Plan for the crisis readiness creating	<input type="radio"/>	<input type="radio"/>
Ensuring the supply of drugs	<input type="radio"/>	<input type="radio"/>
Ensuring alternative energy supply	<input type="radio"/>	<input type="radio"/>
Staff training	<input type="radio"/>	<input type="radio"/>
Prevention	<input type="radio"/>	<input type="radio"/>

Administrative security	Yes	No
Data archiving	<input type="radio"/>	<input type="radio"/>
Identifying sources of personal data	<input type="radio"/>	<input type="radio"/>
Control of access	<input type="radio"/>	<input type="radio"/>
Organisation protection measures	<input type="radio"/>	<input type="radio"/>
Shredding	<input type="radio"/>	<input type="radio"/>
Encryption	<input type="radio"/>	<input type="radio"/>
Technical protection measures	<input type="radio"/>	<input type="radio"/>
Security of automatic processing	<input type="radio"/>	<input type="radio"/>
Staff training	<input type="radio"/>	<input type="radio"/>
Data leakage prevention	<input type="radio"/>	<input type="radio"/>

Ksr

Typ topologie	bod		plocha			linie		uzel
	> 1000 m2 <input type="radio"/>	< 1000 m2 <input type="radio"/>	> 1 km2 <input type="radio"/>	1–10 km2 <input type="radio"/>	< 10 km2 <input type="radio"/>	> 10 km <input type="radio"/>	< 10 km <input type="radio"/>	metodika <input checked="" type="radio"/>
Složitost	jednoduchý (do 10 zaměstnanců) <input type="radio"/>		střední (10–100 zaměstnanců) <input type="radio"/>			složitý (nad 100 zaměstnanců) <input type="radio"/>		
Počet klíčových technologií	do 2 technologií <input type="radio"/>		3–4 technologií <input type="radio"/>			5 a více technologií <input type="radio"/>		
Flexibilita	ne <input type="radio"/>					ano <input type="radio"/>		
Redundance	ne <input type="radio"/>					ano <input type="radio"/>		
Perimetrická ochrana	bez ochrany <input type="radio"/>		lokální <input type="radio"/>			úplná <input type="radio"/>		

K_{sr}	0,90	Reset
-----------------------	-------------	-------

Typ topologie	sběrnice/bus <input type="radio"/>	hvězda/kruh <input type="radio"/>	strom <input type="radio"/>	polygon <input type="radio"/>
Počet klíčových uzlů	1 uzel <input type="radio"/>	2 uzly <input type="radio"/>	3 uzly <input type="radio"/>	4 uzly a více nebo žádný <input type="radio"/>
Celkový počet uzlů	do 5 uzlů <input type="radio"/>	6 - 15 uzlů <input type="radio"/>	16 - 40 uzlů <input type="radio"/>	nad 40 uzlů <input type="radio"/>
Průměrný počet hran na uzel	do 1,5 hrany <input type="radio"/>	1,6 -2,2 hran <input type="radio"/>	2,3 - 3 hrany <input type="radio"/>	více jak 3 hrany <input type="radio"/>

Type of topology	point		area			line		node
	> 1000 m2 <input type="radio"/>	< 1000 m2 <input type="radio"/>	> 1 km2 <input type="radio"/>	1–10 km2 <input type="radio"/>	< 10 km2 <input type="radio"/>	> 10 km <input type="radio"/>	< 10 km <input type="radio"/>	method <input checked="" type="radio"/>
Complexity	simple (under 10 employees) <input type="radio"/>		medium (10-100 employees) <input type="radio"/>			complex (over 100 employees) <input type="radio"/>		
Number of core technologies	0-2 of technology <input type="radio"/>		3-4 of technology <input type="radio"/>			5 or more technologies <input type="radio"/>		
Flexibility	no <input type="radio"/>					yes <input type="radio"/>		
Redundancy	no <input type="radio"/>					yes <input type="radio"/>		
Perimetric protection	unprotected <input type="radio"/>		local <input type="radio"/>			complete <input type="radio"/>		

K_{sr}	0,90	Reset
-----------------------	-------------	-------

Type of topology	bus <input type="radio"/>	star / circle <input type="radio"/>	tree <input type="radio"/>	polygon <input type="radio"/>
Number of core nodes	1 node <input type="radio"/>	2 nodes <input type="radio"/>	3 nodes <input type="radio"/>	4 nodes and more or none <input type="radio"/>
The number of nodes	to 5 nodes <input type="radio"/>	6 - 15 nodes <input type="radio"/>	16 - 40 nodes <input type="radio"/>	over 40 nodes <input type="radio"/>
The average number of edges per node	to 1,5 edge <input type="radio"/>	1,6 - 2,2 edges <input type="radio"/>	2,3 - 3edges <input type="radio"/>	more than 3 edges <input type="radio"/>

Kpr

Krizová připravenost	Ano	Ne
Bezpečnostní audit	<input type="radio"/>	<input type="radio"/>
Identifikace možných událostí	<input type="radio"/>	<input type="radio"/>
Kontaktní údaje	<input type="radio"/>	<input type="radio"/>
Organizační struktura	<input type="radio"/>	<input type="radio"/>
Pojistné smlouvy	<input type="radio"/>	<input type="radio"/>
Popis hlavních činností	<input type="radio"/>	<input type="radio"/>
Pravděpodobnost výskytu událostí	<input type="radio"/>	<input type="radio"/>
Soupis postupů	<input type="radio"/>	<input type="radio"/>
Soupis potřeb a zdrojů	<input type="radio"/>	<input type="radio"/>
Určení zodpovědných osob	<input type="radio"/>	<input type="radio"/>

Implementace plánu kriz. připravenosti	Ano	Ne
Cvičení	<input type="radio"/>	<input type="radio"/>
Informační tabule	<input type="radio"/>	<input type="radio"/>
Označení nouzových východů	<input type="radio"/>	<input type="radio"/>
Poučení personálu	<input type="radio"/>	<input type="radio"/>
Poučení vedoucích osob	<input type="radio"/>	<input type="radio"/>
Poučení pro třetí strany	<input type="radio"/>	<input type="radio"/>
Pravidelná kontrola	<input type="radio"/>	<input type="radio"/>
Průběžná údržba	<input type="radio"/>	<input type="radio"/>
Testování krizových plánů	<input type="radio"/>	<input type="radio"/>
Výstražné tabule	<input type="radio"/>	<input type="radio"/>

Počet rizik identifikovaných kontrolním orgánem v segmentu 1	0
--	---

K_R	0,00
-------	------

K_P	0
-------	---

K_I	0
-------	---

K_{PR}	0,00
----------	------

Reset

Crisis preparedness	Yes	No
Security audit	<input type="radio"/>	<input type="radio"/>
Identification of possible events	<input type="radio"/>	<input type="radio"/>
Contact Information	<input type="radio"/>	<input type="radio"/>
Organization structure	<input type="radio"/>	<input type="radio"/>
Insurance contracts	<input type="radio"/>	<input type="radio"/>
Description of the main activities	<input type="radio"/>	<input type="radio"/>
Probability of events occurrence	<input type="radio"/>	<input type="radio"/>
List of procedures	<input type="radio"/>	<input type="radio"/>
List of needs and resources	<input type="radio"/>	<input type="radio"/>
Determination of responsible persons	<input type="radio"/>	<input type="radio"/>

Implementation of the crisis plan	Yes	No
Practice	<input type="radio"/>	<input type="radio"/>
Information boards	<input type="radio"/>	<input type="radio"/>
Marking of emergency exits	<input type="radio"/>	<input type="radio"/>
Instructions for staff	<input type="radio"/>	<input type="radio"/>
Instructions for directors	<input type="radio"/>	<input type="radio"/>
Instruction for others	<input type="radio"/>	<input type="radio"/>
Regular inspection	<input type="radio"/>	<input type="radio"/>
Ongoing maintenance	<input type="radio"/>	<input type="radio"/>
Testing of emergency plans	<input type="radio"/>	<input type="radio"/>
Warning signs	<input type="radio"/>	<input type="radio"/>

Number of risks identified by control authority in first segment	0
--	---

K_R	0,00
-------	------

K_P	0
-------	---

K_I	0
-------	---

K_{PR}	0,00
----------	------

Reset

ODP

i	Rizika	S	P	N	Hrzi	Odi
Energetika						
1	Krátkodobý výpadek elektřiny	1	0	0	0	0,00
2	Dlouhodobý výpadek elektřiny	1	0	0	0	0,00
3	Výpadek dodávky vody	1	0	0	0	0,00
4	Výpadek dodávky plynu	1	0	0	0	0,00
Přírodní vlivy						
5	Povodeň, záplava, zátopa	1	0	0	0	0,00
6	Dlouhotrvající sucho	1	0	0	0	0,00
7	Extrémní vedro a sucho	1	0	0	0	0,00
8	Silný mráz	1	0	0	0	0,00
9	Pandemie, epidemie	1	0	0	0	0,00
Rizika spojená s přičiněním lidského faktoru						
10	Požár	1	0	0	0	0,00
11	Výbuch	1	0	0	0	0,00
12	Krádež	1	0	0	0	0,00
13	Únik škodlivin v okolí	1	0	0	0	0,00
14	Výpadek v oblasti logistika	1	0	0	0	0,00
15	Virtuální napadení	1	0	0	0	0,00
16	Teroristický útok	1	0	0	0	0,00
17	Narušení veřejného pořádku	1	0	0	0	0,00
18	Nedostupnost personálu	1	0	0	0	0,00
19	Náhlý nápor pacientů	1	0	0	0	0,00
20	Technické poruchy	1	0	0	0	0,00
21	Sabotáž	1	0	0	0	0,00
22	Násilná kriminální činnost	1	0	0	0	0,00
23	Vandalismus	1	0	0	0	0,00
24	Rabování	1	0	0	0	0,00

ODP	0,00
-----	------

i	Risks	S	P	N	Hrzi	Odi
Energetics						
1	Short-term electricity outage	1	0	0	0	0,00
2	Long-term electricity outage	1	0	0	0	0,00
3	Outage of water supply	1	0	0	0	0,00
4	Outage of gas supply	1	0	0	0	0,00
Natural impacts						
5	Flood	1	0	0	0	0,00
6	Prolonged drought	1	0	0	0	0,00
7	Extreme heat and drought	1	0	0	0	0,00
8	Thick frost	1	0	0	0	0,00
9	Pandemic, epidemic	1	0	0	0	0,00
Risks associated with the human factor						
10	Conflagration	1	0	0	0	0,00
11	Explosion	1	0	0	0	0,00
12	Robbery	1	0	0	0	0,00
13	Leaks of pollutants in the area	1	0	0	0	0,00
14	Outage in logistics	1	0	0	0	0,00
15	The virtual attack	1	0	0	0	0,00
16	The terrorist attack	1	0	0	0	0,00
17	Disruption of public order	1	0	0	0	0,00
18	Unavailability of staff	1	0	0	0	0,00
19	Sudden rush of patients	1	0	0	0	0,00
20	Technical failures	1	0	0	0	0,00
21	Sabotage	1	0	0	0	0,00
22	Violent criminal activity	1	0	0	0	0,00
23	Acts of vandalism	1	0	0	0	0,00
24	Plundering	1	0	0	0	0,00

ODP	0,00
-----	------

Hodnocení odolnosti	Hodnota ODP	Slovní hodnocení	Minimální hodnota robustnosti	Minimální hodnota robustnosti zabezpečení	Minimální hodnota připravenosti
Výborně (A)	0,8– 1	na všechna identifikovaná rizika je systém připraven, žádné z rizik není zanedbáno	0,5 jako výsledek vztahu $K_{RO} * V_{RO}$	Je dána váhami jednotlivých parametrů $V_{FB}, V_{IB}, V_{AB}, V_{KO}$	0,5 jako výsledek vztahu $K_{PR} * V_{PR}$
Velmi dobře (B)	0,6 – 0,8	na všechna důležitá identifikovaná rizika je systém připraven	0,4 jako výsledek vztahu $K_{RO} * V_{RO}$	Je dána váhami jednotlivých parametrů $V_{FB}, V_{IB}, V_{AB}, V_{KO}$	0,4 jako výsledek vztahu $K_{PR} * V_{PR}$
Dobře (C)	0,4 – 0,6	na většinu důležitých identifikovaných rizik je systém připraven	0,3 jako výsledek vztahu $K_{RO} * V_{RO}$	Je dána váhami jednotlivých parametrů $V_{FB}, V_{IB}, V_{AB}, V_{KO}$	0,3 jako výsledek vztahu $K_{PR} * V_{PR}$
Dostatečně (D)	0,2 – 0,4	na většinu identifikovaných rizik je systém připraven	0,3 jako výsledek vztahu $K_{RO} * V_{RO}$	Je dána váhami jednotlivých parametrů $V_{FB}, V_{IB}, V_{AB}, V_{KO}$	0,3 jako výsledek vztahu $K_{PR} * V_{PR}$
Není schopen odolat (E)	0 – 0,2	na většinu (více jak 1/2) identifikovaných rizik systém není připraven	0,2 jako výsledek vztahu $K_{RO} * V_{RO}$	Je dána váhami jednotlivých parametrů $V_{FB}, V_{IB}, V_{AB}, V_{KO}$	0,2 jako výsledek vztahu $K_{PR} * V_{PR}$

Resistance evaluation	Value of ODP	Verbal rating	The minimum value of the robustness	The minimum value of the robustness of security	The minimum value of preparedness
Great (A)	0,8– 1	system is ready for all identified risks, none risks was neglected	0,5 as a result of the relationship $K_{RO} * V_{RO}$	Is given by the weights of individual parameters $V_{FB}, V_{IB}, V_{AB}, V_{KO}$	0,5 as a result of the relationship $K_{PR} * V_{PR}$
Very good (B)	0,6 – 0,8	system is ready for all of the important identified risks	0,4 as a result of the relationship $K_{RO} * V_{RO}$	Is given by the weights of individual parameters $V_{FB}, V_{IB}, V_{AB}, V_{KO}$	0,4 as a result of the relationship $K_{PR} * V_{PR}$
Good (C)	0,4 – 0,6	system is ready for the most of important identified risks	0,3 as a result of the relationship $K_{RO} * V_{RO}$	Is given by the weights of individual parameters $V_{FB}, V_{IB}, V_{AB}, V_{KO}$	0,3 as a result of the relationship $K_{PR} * V_{PR}$
Enough (D)	0,2 – 0,4	system is ready for the most of the identified risks	0,3 as a result of the relationship $K_{RO} * V_{RO}$	Is given by the weights of individual parameters $V_{FB}, V_{IB}, V_{AB}, V_{KO}$	0,3 as a result of the relationship $K_{PR} * V_{PR}$
Unable to resist (E)	0 – 0,2	system is not ready for the majority (more than half) of the identified risks	0,2 as a result of the relationship $K_{RO} * V_{RO}$	Is given by the weights of individual parameters $V_{FB}, V_{IB}, V_{AB}, V_{KO}$	0,2 as a result of the relationship $K_{PR} * V_{PR}$

Help

Seznam zkratk	
A	Aktiva
Hrzi	Hodnota rizikovosti
i	index
Ki	Koeficient implementace plánu kriz. připravenosti
Kp	Koeficient krizové připravenosti
Kpr	Koeficient připravenosti
Kr	Koeficient správnosti identifikace
Krz	Koeficient robustnosti zabezpečení
Ks	Koeficient závislosti
Ksr	Koeficient strukturální robustnosti
N	Dopad hrozby
ODi	Critical infrastructure resistance of i-risk
ODP	Odolnost prvku kritické infrastruktury
P	Pasiva
R	Rizika
R2	Rizika - vizualizace
S	Segment

List of Abbreviations	
A	Active
Hrzi	Risk level
i	index
Ki	The coefficient of crisis plan implementation
Kp	The coefficient of the crisis preparedness
Kpr	The coefficient of preparedness
Kr	The coefficient of accuracy identification
Krz	The coefficient of security robustness
Ks	The coefficient of dependence
Ksr	The coefficient of structural robustness
N	Threats impact
ODi	Critical infrastructure resistance of i-risk
ODP	Critical infrastructure resistance
P	Passive
R	Risks
R2	Risks - visualization
S	Segment