VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA CHEMICKÁ
ÚSTAV CHEMIE A TECHNOLOGIE OCHRANY ŽIVOTNÍHO PROSTŘEDÍ

FACULTY OF CHEMISTRY
INSTITUTE OF CHEMISTRY AND TECHNOLOGY OF ENVIRONMENTAL PROTECTION

BEZPEČNOST A OCHRANY KRITICKÉ INFRASTRUKTURY SPOLEČNOSTI V ČESKÉ REPUBLICE

PROTECTION OF THE CRITICAL INFRASTRUCTURE OF SOCIETY IN THE CZECH REPUBLIC

BAKALÁŘSKÁ PRÁCE
BACHELOR´S THESIS

AUTOR PRÁCE
AUTHOR
LENKA KUBICOVÁ

VEDOUCÍ PRÁCE
SUPERVISOR
Ing. OTAKAR JIŘÍ MIKA, CSc.

BRNO 2010

Vysoké učení technické v Brně
Fakulta chemická
Purkyňova 464/118, 61200 Brno 12

Zadání bakalářské práce

Číslo bakalářské práce:	**FCH-BAK0437/2009**	Akademický rok:	**2009/2010**
Ústav:	Ústav chemie a technologie ochrany životního prostředí		
Student(ka):	**Lenka Kubicová**		
Studijní program:	Ochrana obyvatelstva (B2825)		
Studijní obor:	Krizové řízení a ochrana obyvatelstva (2804R002)		
Vedoucí práce	**Ing. Otakar Jiří Mika, CSc.**		
Konzultanti:			

Název bakalářské práce:

Bezpečnost a ochrana kritické infrasktruktury společnosti v České republice

Zadání bakalářské práce:

Zpracovat odborné pojednání o ochraně kritické infrasktruktury společnosti v České republice se zaměřením na platné legislativní normy České republiky a Evropské unie.

Termín odevzdání bakalářské práce: 28.5.2010

Bakalářská práce se odevzdává ve třech exemplářích na sekretariát ústavu a v elektronické formě vedoucímu bakalářské práce. Toto zadání je přílohou bakalářské práce.

Lenka Kubicová Student(ka)	Ing. Otakar Jiří Mika, CSc. Vedoucí práce	doc. Ing. Josef Čáslavský, CSc. Ředitel ústavu

V Brně, dne 1.12.2009

prof. Ing. Jaromír Havlica, DrSc.
Děkan fakulty

ABSTRAKT

Práce je věnována bezpečnosti a ochraně kritické infrastruktury. Popisuje historii kritické infrastruktury ve Spojených státech, Evropské unii a České republice. Charakterizuje jednotlivé prvky kritické infrastruktury a možné hrozby, které tyto prvky ohrožují. Vysvětluje základní pojmy z oblasti kritické infrastruktury a její bezpečnost a ochranu, zabývá se legislativou. Obsahuje hodnocení bezpečnosti a ochrany kritické infrastruktury a navrhuje možnosti pro zlepšení situace v této oblasti.

ABSTRACT

Main content of this thesis is safety and protection of the critical infrastructure. It describes the history of the critical infrastructure in United States of America, European Union and in the Czech Republic. It describes the individual elements of critical infrastructure and the possible extraordinary events that threaten these elements. It explains basic terms from area safety and protection of the critical infrastructure and describes relevant laws. It evaluates safety and protection of critical infrastructure and proposes some possibilities for improvement the situation in the area.

KLÍČOVÁ SLOVA

kritická infrastruktura, bezpečnost kritické infrastruktury, ochrana kritické infrastruktury, hrozba, prvky kritické infrastruktury, mimořádná událost

KEYWORDS

critical infrastructure, security of critical infrastructure, critical infrastructure protection, threat, elements of critical infrastructure, extraordinary event

KUBICOVÁ, L. *Bezpečnost a ochrana kritické infrastruktury společnosti v České republice.* Brno: Vysoké učení technické v Brně, Fakulta chemická, 2010. 59 s. Vedoucí bakalářské práce Ing. Otakar Jiří Mika, CSc.

PROHLÁŠENÍ

Prohlašuji, že jsem bakalářskou práci vypracovala samostatně a že všechny použité literární zdroje jsem správně a úplně citovala. Bakalářská práce je z hlediska obsahu majetkem Fakulty chemické VUT v Brně a může být využita ke komerčním účelům jen se souhlasem vedoucího bakalářské práce a děkana FCH VUT.

.....

podpis studentky

PODĚKOVÁNÍ

Děkuju tímto panu Ing. Otakaru J. Mikovi, CSc. za cenné rady, připomínky, náměty a poskytnuté materiály při konzultacích k této bakalářské práci.

OBSAH

1 ÚVOD

Problematika kritické infrastruktury si právem zaslouží zvýšenou pozornost. Současná společnost je závislá na bezproblémovém chodu řady služeb a zařízení, které do této části infrastruktury patří. Při případném narušení či selhání může dojít k oslabení národní bezpečnosti a k ohrožení zdraví a životů obyvatelstva.

Kritická infrastruktura představuje fyzické, kybernetické a organizační systémy, které jsou nutné pro zajištění ochrany životů a zdraví lidí a majetku, minimální chodu ekonomiky a správy státu.

Ochrana kritické infrastruktury se vyvíjí již delší dobu a to nejen v zahraničí, ale také v České republice. V průběhu let se také měnil pohled na možné hrozby, které kritickou infrastrukturu ohrožují. Dříve byl kladen důraz především na ochranu před jaderným útokem. Postupně začala vznikat i ochrana před přírodními katastrofami, technickými haváriemi a v neposlední řadě také proti terorismu.

Ve své bakalářské práci se zabývám historickým vývojem kritické infrastruktury ve Spojených státech amerických, Evropské unii a zejména v České republice. Jsou zde uvedeny jednotlivé prvky kritické infrastruktury a mimořádné události, které mohou mít vliv na správnou funkčnost těchto prvků. V poslední kapitole je zhodnocena literatura v oblasti ochrany a bezpečnosti kritické infrastruktury, která poukazuje na potřebu legislativních úprav v této oblasti, neboť v České republice dosud není zákon, který by se touto problematikou zabýval.

2 VÝVOJ KRITICKÉ INFRASTRUKTURY A JEJÍ ZRANITELNOST

Poprvé byl pojem kritická infrastruktura použit v roce 1997 v amerických článcích, které se touto problematikou zabývaly. Ochranu „kritické infrastruktury“ lze ale datovat už do roku 1962, kdy došlo k tzv. Kubánské krizi. Po této události se začal řešit problém bezpečnosti telekomunikační sítě a poprvé se vyskytla otázka zranitelnosti tohoto systému.

V průběhu dalších let si společnost stále více začala uvědomovat svoji závislost na některých službách či zařízeních, které v současné době spadají do tzv. kritické infrastruktury. Mnoho těchto zařízení je zranitelných, což způsobuje i narůstající zranitelnost společnosti jako celku. Podle zkušeností jednotlivých státu s mimořádnými událostmi způsobující narušení kritické infrastruktury se odvíjí i pohled na její ochranu.

2.1 Vývoj v USA

Jednou z prvních zemí, která si začala uvědomovat zranitelnost životně důležité infrastruktury, byly Spojené státy americké. V roce 1996 byla prezidentem Billem Clintonem vytvořena Komise na ochranu kritické infrastruktury (*President's Commission on Critical Infrastructure Protection* PCCIP). Jejím cílem bylo prověřit rostoucí závislost americké ekonomiky a způsob života na kritické infrastruktuře (KI). V říjnu 1997 vydala Komise zprávu, která vyzývala k zajištění bezpečnosti Spojených státu a její stále zranitelnější a propojenější infrastruktury, jako jsou telekomunikace, bankovnictví a finance, doprava a základní vládní služby. Na základě této zprávy podepsal prezident Clinton v květnu 1998 dvě nové směrnice – PDD-62 (*Presidential Decision Directive)*, která se zaměřuje na boj proti terorismu a PDD-63, která se věnuje ochraně kritické infrastruktury. Cílem bylo chránit národní kritickou infrastrukturu před různými hrozbami, včetně počítačových útoků. **[*1*]**

Směrnice PDD-63 zahrnovala řešení zranitelnosti kritické infrastruktury ve veřejném i soukromém sektoru. Stanovila cíle, poskytla koncepci a zdroje a zařadila kritickou infrastrukturu mezi národní životní zájmy.

Po teroristickém útoku 11. září 2001 na světové obchodní centrum v New Yorku věnovaly Spojené státy americkému výzkumu bezpečnosti výraznou část celkových výdajů. Útoky totiž ukázaly, že hlavní prioritou pro stát a jeho subjekty je bezpečný prostor a další ekvivalenty založené na stejné filosofii. Řadí se sem i prostředky, které do výzkumu dává soukromý sektor.

16. října 2001 vydal prezident George W. Bush Vládní nařízení na ochranu kritické infrastruktury (*Executive Order on Critical Infrastructure Protection*). Jeho účelem bylo zabezpečit ochranu informačních systémů pro kritickou infrastrukturu, včetně nouzové komunikační připravenosti a ochrany hmotných zařízení, které informační systémy podporují. Jako prioritní bylo stanoveno zabezpečení tří vzájemně závislých funkcí: ekonomiky, činnost státu (vlády) a vedení národní obrany. **[*2*]**

V této době byl poprvé definován v tzv. *Patriot Act* pojem kritická infrastruktura jako „systémy a zařízení, jak hmotné tak virtuální, které jsou životně důležité pro Spojené státy a zneschopnění nebo zničení takových systému nebo zařízení by mělo vliv na snížení bezpečnosti, národní ekonomické bezpečnosti, národního veřejného zdraví nebo bezpečnosti nebo jakoukoliv jejich kombinaci.“ **[*3*]**

V roce 2002 byla vydána Národní strategie pro vnitřní bezpečnost (*The National Strategy for Homeland Security*). Má za cíl: „zajistit suverenitu a nezávislost Spojených států“ **[*4*]**, tzn. předcházet teroristickým útokům na Spojené státy, snížit zranitelnost Ameriky vůči terorismu a minimalizovat škody a zotavit se z útoků, které nastanou.

O rok později vydal Bílý dům Národní strategii fyzické ochrany kritické infrastruktury a klíčových zařízení (*The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets*) a Národní strategii zabezpečení kybernetického prostoru. (*The National Strategy to Secure Cyberspace*). Přijetím těchto strategií došlo k určité specifikaci kritické infrastruktury, a to z hlediska kybernetického a hmotného. V oblasti kybernetiky jde o ochranu kybernetického prostoru, který je vlastněn, řízen, kontrolován nebo se kterým je v interakci. Z hlediska hmotných prostředků se jedná o fyzickou ochranu kritické infrastruktury a klíčových zařízení. **[*2*]**

Národní strategie fyzické ochrany kritické infrastruktury a klíčových zařízení je v současné době nejkomplexnějším materiálem, který se zabývá problematikou ochrany kritické infrastruktury. Cílem strategie je dosáhnout jednotnějšího, koordinovaného a vzájemně se doplňujícího systému, který vyžaduje aktivní přístup jak státní administrativy, tak i soukromého sektoru a občanů USA. Formuluje a popisuje zabezpečení kritické infrastruktury v 11 sektorech a ochranu klíčových zařízení v pěti sektorech.

Výše uvedené strategie popisují obecný směr zabezpečení kritické infrastruktury v jednotlivých sektorech. Samotné plánování identifikace a prioritizace zabezpečení jednotlivých prvků má na starosti nařízení prezidenta tzv. *Homeland Security Presidential Directive 7*, které slouží jako podklad pro zpracování globálního plánu pro ochranu kritické infrastruktury a na něj navazujících jednotlivých sektorových plánů pro ochranu kritické infrastruktury. **[*5*]**

V roce 2006 se začal vypracovávat Národní plán pro ochranu kritické infrastruktury pod názvem *National Infrastructure Protection Plan (NIPP)*. Tento plán by měl obsahovat komplexní rámec pro řízení rizik, která jasně definuje ochranu kritické infrastruktury, role a odpovědnost za všechny úrovně státní správy, soukromého sektoru, nevládních agentur a kmenových partnerů. NIPP vychází ze zásad *National Strategy for Homeland Security* a dalších materiálů, které byly k této problematice vydány. Plán byl v loňském roce aktualizován a začal klást větší důraz na řízení rizik a odolnost. **[*6*]**

2.2 Vývoj v Evropě

Služby a rozsáhlé sítě jako jsou telekomunikace, elektrické a energetické sítě apod. jsou základním kamenem evropského hospodářství a hrají zásadní roli při plnění potřeb Evropanů. Narušení těchto služeb by mohlo mít zničující dopady, ztráty na životech a majetku a také možné zhroucení důvěry veřejnosti v tyto služby. Základní rolí vlád a Evropské unie je proto zajistit takové podmínky, aby nedocházelo k narušení kritické infrastruktury a případně minimalizovat možné dopady na životní podmínky členských států a jejich občanů a EU jako celku. Řadu opatření pro ochranu kritické infrastruktury začaly průběžně přijímat jednotlivé členské státy.

2.2.1 Velká Británie

V roce 1999 bylo ve Velké Británii vytvořeno Koordinační centrum pro bezpečnost národní infrastruktury (*National Infrastructure Security Coordination Centre* NISCC) jako součást Ministerstva vnitra. Cílem bylo koordinovat všechny vládní iniciativy pro ochranu kritické infrastruktury vůči kybernetickým útokům. Byly určeny systémy, jejichž ztráta nebo narušení by mohlo vést k ohrožení životů, vážným negativním hospodářským a sociálním dopadům na společnost. **[7]**

2.2.2 Německo

V Německu v reakci na PDD-63 vznikl v roce 1997 Spolkový úřad pro informační bezpečnost (*Bundesamt für Sicherheit in der Informationstechnik).* Fyzickými aspekty bezpečnosti se zabýval Spolkový úřad civilní ochrany a pomoci při pohromách *(Bundesamt für Bevölkerungsschutz und Katastrophenhilfe).* Důležitou roli zde hraje i Spolkové ministerstvo hospodářství a práce (*Bundesministerium für Wirtschaft und Arbeit),* protože je více než devadesát procent kritické infrastruktury ve vlastnictví soukromých subjektů. Nedávno zde vznikla i instituce Ochrana kritické infrastruktury v Německu *(Schutz Kritischer Infrastrukturen in Deutschland)*, která zkoumala zranitelnost německé infrastruktury a navrhla strategii ochrany a politiku spolupráce a kooperace veřejné správy se soukromými subjekty. **[7]**

2.2.3 Nizozemsko

V roce 2001 byl v Nizozemsku schválen *Akční plán bezpečnosti a boje proti terorismu*. Součástí byl projekt ochrany kritické infrastruktury skládající se ze tří částí: rychlé zajištění míry kritičnosti infrastruktury, stimulování spolupráce veřejného a soukromého sektoru a analýzy rozdílu mezi přijatými a potřebnými ochrannými opatřeními.

2.2.4 Evropská unie

Kritická infrastruktura v jednotlivých členských státech je mezi sebou propojená a vzájemně závislá. Poškození nebo ztráta jedné infrastruktury v jednom členském státě Evropské unie může negativně působit na ostatní státy a na evropské hospodářství jako celek. Nové technologie a liberalizace trhu způsobují, že mnoho infrastruktur je součástí rozsáhlejší sítě.

Je proto důležité zaměřit se na oblasti největšího rizika a snažit se snižovat zranitelnosti jednotlivých prvků kritické infrastruktury.

Evropská rada vyzvala v červnu 2004 Evropskou komisi, aby vypracovala celkovou strategii na ochranu kritické infrastruktury. V říjnu 2004 bylo přijato sdělení Ochrana kritické infrastruktury v boji proti terorismu (*Critical infrastructure protection in the fight against terrorism*) **[*8*]**, které obsahuje návrhy, jak by se měla zlepšit prevence, připravenost a schopnosti reakce na teroristické útoky zasahující kritickou infrastrukturu. Vymezuje pojmy hrozba a evropská kritická infrastruktura, stanovuje oblasti kritické infrastruktury, určuje potenciál kritické infrastruktury podle tří faktorů:

- *Rozsah – ztráta prvku kritické infrastruktury se hodnotí podle velikosti zeměpisné oblasti, které by mohly být ovlivněny jeho ztrátou nebo nedostupností (mezinárodní, vnitrostátní, místní).*
- *Závažnost – stupeň dopadu nebo ztráty může být hodnocen jako žádný, minimální, mírný nebo velký. Mezi kritéria, která by mohla být použita pro hodnocení závažnosti, jsou veřejný dopad, hospodářský dopad, vliv na životní prostředí, vzájemná závislost, politický dopad.*
- *Vliv času – toto kritérium zjišťuje, kdy by mohla mít ztráta prvku vážný dopad (tj. okamžitě, za 24-84 hodin, za týden, jindy).*

Sdělení také upozorňuje, že každé odvětví a členský stát si musí v rámci příslušné oblasti působnosti a v souladu s postupem EU určit infrastrukturu, která je pro ně kritická, a organizace nebo osoby odpovědné za bezpečnost. **[*8*]**

V listopadu 2005 přijala komise Zelenou knihu o Evropském programu na ochranu kritické infrastruktury (*Green Paper on European Programme for Critical Infrastructure Protection* EPCIP). Hlavním cílem této knihy je zapojit velké množství subjektů a získat od nich konkrétní informace o vhodném přístupu pro EPCIP. Účinná ochrana kritické infrastruktury vyžaduje komunikaci, koordinaci a spolupráci jak na národní, tak na evropské úrovni, a to mezi všemi subjekty – vlastníky a provozovateli infrastruktur, řídícími orgány, odbornými subjekty a průmyslovými asociacemi, stejně jako všech úrovní státní a veřejné správy a také veřejnosti. **[*9*]** Předkládá také možnosti k vybudování Výstražné informační sítě kritické infrastruktury (*Critical Infrastructure Warning Information Network* CIWIN), s cílem posílit sdílení informací o ochraně kritické infrastruktury mezi členskými státy EU. Tento systém by měl mít dvě hlavní funkce – zajistit fórum pro výměnu informací s důrazem na výměnu osvědčených postupů a budování důvěry na úrovni EU a systém včasného varování pro KI, která umožní rychlou výměnu informací mezi členskými státy a Evropskou komisí.

Jednotlivé kapitoly Zelené knihy uvádějí účel a rozsah působnosti EPCIP. Navrhuje základní principy pro zformování základu EPCIP a společný rámec. Definuje základní pojmy ochrany kritické infrastruktury včetně pojmu KI, který „zahrnuje fyzické zdroje, služby a zařízení informačních technologií, sítě a zařízení infrastruktury, které pokud by byly porušeny nebo zničeny, by měly závažný dopad na zdraví, bezpečí, bezpečnost nebo ekonomický blahobyt

občanů nebo efektivního fungování vlád.“ Uvádí také přehled sektorů kritické infrastruktury (viz příloha 1). **[*9*]**

V roce 2006 bylo vydáno Sdělení komise o Evropském programu na ochranu kritické infrastruktury *(Communication from the Commission on a European Programme for Critical Infrastructure Protection)*, které obsahuje zásady, postupy a nástroje navrhované s cílem zavést systém EPCIP. Cílem je zlepšení ochrany kritických infrastruktur v EU, která bude zohledňovat veškerá ohrožení, s prioritním zaměřením na terorismus. Sdělení obsahuje opatření pro usnadnění rozvoje a provádění EPCIP pomocí akčního plánu EPCIP, CIWIN, skupiny odborníků, procesu sdílení informací o ochraně kritické infrastruktury a analýzy vzájemných souvislostí. Jsou zde také zmíněny otázky, kterými by se měly zabývat vnitrostátní programy na ochranu kritických infrastruktur, krizové plánovaní jako klíčový prvek procesu ochrany kritické infrastruktury a zřízení a efektivní využití příslušných finančních nástrojů. **[*10*]** EPCIP má také své klíčové zásady, mezi které patří:

- *Subsidiarita – odpovědnost, hlavně na národní úrovni.*
- *Doplňkovost – existence stávajících norem.*
- *Důvěrnost sdílených informací.*
- *Spolupráce zainteresovaných subjektů (vlastníků, provozovatelů, státu atd.).*
- *Proporcionalita – nelze chránit vše.*
- *Odvětvový přístup.*

V roce 2008 byla přijata Směrnice Rady o určování a označování evropské kritické infrastruktury a posouzení potřeby zvýšit její ochranu (*Council Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection).* Směrnice stanovuje postup pro určování a označování evropské kritické infrastruktury (ECI). Poskytuje také společný přístup k posouzení těchto infrastruktur s cílem zlepšit jejich ochranu. Členské státy by měly využít řadu kritérií pro identifikaci těchto potenciálních infrastruktur. Určování a označování ECI členskými státy by mělo být dokončeno nejpozději v lednu 2011. Proces určování a označování ECI je jedním z klíčových prvků EPCIP. Směrnice obsahuje také pravidla pro zpracování plánů bezpečnosti provozovatelů evropské kritické infrastruktury, povinnosti o předkládání zpráv a vyhodnocování rizik a další ustanovení. Zaměřuje se především na odvětví energetiky a dopravy. Nabízí ale zahrnutí i dalších odvětví v rámci své působnosti, zejména informační a komunikační technologie (ICT). **[*11*]**

V minulém roce přijala EU opatření na ochranu informačních a komunikačních technologií, které jsou často označovány jako kritické informační sítě. Tyto elektronické komunikační služby a sítě jsou páteří evropského hospodářství a jsou životně důležité pro občany, podniky a vlády. Jednotlivé členské státy mají značně odlišné přístupy a možnosti, jak řešit ochranu kritických informačních infrastruktur.

Proto v březnu 2009 přijala Evropská komise sdělení vyzývající k přijetí následujících opatření:

- *Připravenost a prevence – rozvoj spolupráce, výměny informací a předávání osvědčených postupů mezi členskými státy prostřednictvím Evropského fóra.*
- *Detekce a reakce – podporovat rozvoj evropského sdílení informací a varovný systém.*
- *Zmírnění a obnovení – podnítit užší spolupráci mezi členskými státy prostřednictvím národních a mezinárodních plánů a pravidelných cvičení pro rozsáhlé sítě.*
- *Mezinárodní spolupráce – vedení diskuzí, stanovení priorit EU pro dlouhodobou odolnost a stabilitu internetu, navrhnout zásady a pokyny, které budou mezinárodně propagovány.*
- *Stanovení kritérií pro evropské kritické infrastruktury v odvětví informačních a komunikačních technologií.*

V současné době probíhá spolupráce mezi experty USA a EU. Diskuze se soustředily na čtyři hlavní témata – výměna informací o opatření národní ochrany kritické infrastruktury, závislost různých ekonomických sektorů na druhém, zkušenosti a metodika pro určení kritické infrastruktury a osvědčené postupy v ochraně sítí a informací. Základem pro spolupráci mezi EU a USA je Evropský program na ochranu kritické infrastruktury, který představuje široký rámec pro činnosti související s ochranou kritické infrastruktury v EU. **[*12*]**

2.3 Vývoj v České republice

Základní povinností a tedy i funkcí státu je ochrana životů, 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. Vyžaduje také i odpovídající vědeckou podporu, která je nezbytná a nezastupitelná.

V České republice je bezpečnostní výzkum realizován ve značném rozsahu, ale je roztříštěn a není jednotně koordinován. V mnoha případech souvisí s resortní příslušností jednotlivých vědeckých pracovišť (Ministerstvo zahraničních věcí, vnitra, obrany, zdravotnictví, průmyslu a obchodu atd.). Částečně omezená je také spolupráce mezi těmito pracovišti a pracovišti působícími na vysokých školách. Kvůli tomu, že je vzájemná spolupráce, podpora a komunikace mezi složkami, které se podílejí na zabezpečení bezpečnosti země, limitována jejich resortními zájmy, není v základních bezpečnostních dokumentech zachycena komplexnost bezpečnostního systému a jeho řízení. **[*13*]**

Prvotní činnosti v rámci kritické infrastruktury se zaměřily na ochranu počítačových sítí, a to v souvislosti s usnesením Bezpečností rady státu (BRS) č. 123 z roku 2000, na jehož základě byl zpracován projekt *Strategie výstavby informačních systémů na podporu krizového plánování a řízení ve státní správě.*

V roce 2001 BRS projednala materiál *Informace ke zpracování definice a stanovení rozsahu základních funkcí státu za krizových situací* **[*14*]**. Dokument popisuje danou problematiku a definuje základní funkce státu, které je nezbytné zachovat v období krizových situací. Provedená analýza po povodních v letech 1997 a 1998 a analýzy zahraniční literatury týkající se odezvy na živelní a jiné pohromy, vedly ke zpracování materiálu, který se týkal ochrany kritické infrastruktury. **[*15*]**

Komplexněji se otázkami kritické infrastruktury začal zabývat v roce 2002 Výbor pro civilní nouzové plánování (VCNP), který je jedním z pracovních výborů Bezpečnostní rady státu. Na 17. schůzi dne 24. září 2002 projednal tento výbor usnesení *Rozsah základních funkcí státu za krizových situací* a materiál *Zpráva o národní kritické infrastruktuře a návrh zásad na její zabezpečení*, která se zabývala samotným vymezením pojmu a jednotlivých oblastí KI. Podle tohoto materiálu se kritickou infrastrukturou 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 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. **[*2*]**

V červnu 2003 byl vydán nový materiál *Analýza zabezpečení základních funkcí státu a prvků kritické infrastruktury v ČR za krizových situací*, který představoval první ucelený a souhrnný přehled situace v jednotlivých odvětvích kritické infrastruktury. Projekt KI obsahoval tři fáze:

- *Informace o jednotlivých oblastech včetně právních dokumentů.*
- *Přehled subjektů KI (rozčleněn na tři části – subjekty kritické infrastruktury s celostátním, regionálním a s lokálním významem).*
- *Zajištění vzájemných vazeb a závislostí.*

V jednotlivých sektorech jsou uvedeny produkty nebo služby a také gestor daného produktu a služby. V ČR je tak vytvořen Seznam subjektů kritické infrastruktury, v němž je specifikována národní, regionální a lokální úroveň. **[*16*]**

V roce 2006 byla vydána *Zpráva o stavu řešení problematiky kritické infrastruktury* **[*17*]**, která poprvé srovnávala kroky České republiky se zahraničím v oblasti ochrany kritické infrastruktury.

O rok později projednal VCNP materiál *Zpráva o řešení problematiky kritické infrastruktury v České republice*, jejíž součástí byla podrobná analytická část zabývající se situací v jednotlivých oblastech kritické infrastruktury a stavem řešení této problematiky v České republice. Stanovil i novou definici 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." **[*18*]**

Materiál projednávala také Bezpečnostní rada státu 3. července 2007 a svým usnesením č. 30 uložila ministru vnitra předložit materiál, který bude obsahovat harmonogram dalšího postupu zpracování dokumentů *Komplexní strategie České republiky k řešení problematiky kritické infrastruktury* a *Národní program ochrany kritické infrastruktury*. **[*18*]** Tento Harmonogram byl zpracován a schválen 25. února 2008 usnesením vlády ČR č. 170.

Cílem Komplexní strategie ochrany kritické infrastruktury v České republice je zajištění fungování KI tak, aby nedocházelo k jejímu selhání při zohlednění všech možných rizik a hrozeb. Strategie by měla vycházet z analýzy řešení problematiky KI v České republice a také by měla brát v úvahu mezinárodní a evropský kontext. Harmonogram dalšího postupu byl schválen usnesením vlády ze dne 2. března 2009 č. 222. Problematika ochrany KI v České republice bude poté zapracována do novely krizového zákona, která má současně aplikovat Směrnici Rady EU o evropských KI z 8. prosince 2008 č. 2008/114/ES.

2.4 Vývoj v Severoatlantické alianci

Na pojetí řešení problematiky ochrany kritické infrastruktury v České republice mají vliv kromě EU také země Severoatlantické aliance. Kritickou infrastrukturou se zde zabývá Hlavní výbor pro civilní nouzové plánování (*Senior Civil Emergency Planning Committee* SCEPC), který je seniorním poradním výborem Severoatlantické Rady v oblasti civilního nouzového plánování. Hlavní výbor koordinuje a dohlíží na práci osmi podřízených plánovacích výborů.

V roce 2003 Výbor pro civilní ochranu schválil dokument o kritické infrastruktuře, kde se zaměřil na definování vzájemných závislostí jednotlivých prvků KI a pojednával také o schopnostech státu reagovat na mimořádnou událost, resp. krizovou situaci a vytyčil deset schopností, které by mohly ovlivňovat prvky kritické infrastruktury: centrální schopnost reakce, zásobování (doplňování) základních služeb, místní schopnost reakce, dekontaminace, místní očista, vakcinace a ošetřování, péče o hromadně zraněné, hromadná evakuace, zjišťování ohrožení a jejich pojmenování, informování, varování a vyrozumění veřejnosti. Podle výboru patří mezi nejkritičtější z uvedených schopností hromadná evakuace a informování, varování a vyrozumění veřejnosti. **[*19*]**

V letech 2003-2004 byly vydány Ministerské směrnice, které kladly důraz na zapojení všech plánovacích výboru do prací na ochranu KI a na vzájemnou koordinaci. Byly také připraveny možné scénáře řešící situace po útocích na předem vytipovaných oblastech KI. NATO tak rozlišila následující oblasti kritické infrastruktury: energetika, informační a komunikační systémy, doprava, veřejné služby, strategické průmyslové sektory, zdravotní péče, telekomunikace, bankovnictví a finance, nouzové služby, zachování kontinuity práce úřadů.

Členské a partnerské státy NATO se svými příspěvky omezily na zprávy o postupu jednotlivých států v uvedené oblasti. Budoucí postup NATO bude směřovat na mezinárodní spolupráci v oblasti vzdělávání k dosažení potřebných znalostí z oblasti kritické infrastruktury účastníků z civilní i vojenské sféry. **[*20*]**

3 VÝZNAM KRITICKÉ INFRASTRUKTURY SPOLEČNOSTI V ČESKÉ REPUBLICE

3.1 Vymezení kritické infrastruktury společnosti

Moderní společnost je závislá na dobře fungující kritické infrastruktuře, zejména na technologické, kterou tvoří dodávky vody a potravin, elektřiny a tepla apod. Její selhání by mělo neblahé důsledky 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: **[7]**

- *V současnosti je společnost zcela závislá na normálním průběhu operací technologické infrastruktury (produkty a služby) a infrastruktury státu (veřejné služby). Tato závislost přináší sníženou odolnost vůči nepříznivým vlivům.*
- *Jednotlivé infrastruktury společnosti jsou vzájemně provázané, což zvyšuje jejich složitost a vnímavost vůči poruchám.*
- *Ke snížení zranitelnost je potřeba značných finančních prostředků, kterých je nedostatek.*
- *Deregulace rozdělila infrastruktury mezi různé vlastníky.*
- *Civilizované prostředí, jako forma technologické infrastruktury, se snaží přebírat některé funkce za přírodu, a proto se musíme stále více a více 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.*

Ze společenského hlediska se kritickou infrastrukturou 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. Mimo ekonomické bezpečnosti rozlišujeme i bezpečnost fyzickou, která se týká ochrany fyzických zařízení před škodami v důsledku působení fyzických sil, a 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. **[7]**

Obecně se infrastruktura společnosti skládá z ekonomické, sociální a „nehmotné“ infrastruktury: **[7]**

- *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.

3.2 Charakteristika kritické infrastruktury

Infrastrukturu charakterizují určité vlastnosti vycházející z jejich fyzických prvků a z procesů používajících tyto prvky při plnění úkolů infrastruktury. Pro infrastrukturu je typická konektivita (propojitelnost), která se definuje následovně: **[*21*]**

Propojitelnost je závislost mezi aspoň dvěma infrastrukturami. Prostřednictvím tohoto spojení stav jedné infrastruktury ovlivňuje nebo koreluje se stavem jiné infrastruktury, např. závislost elektrické energie na ostatních infrastrukturách (ropa jako palivo pro generátory atd.)

Závislost se může týkat také infrastruktury jako celku tzn., že na sobě mohou být vzájemně závislé celé infrastruktury. Tato vzájemná závislost může být fyzická, kybernetická, logická a územní. Přitom platí: **[*21*]**

- *Infrastruktury jsou fyzicky vzájemně závislé, jestliže stav jedné z nich je závislý na materiálním výstupu druhé.*
- *Kybernetická vzájemná závislost znamená, že stav jedné infrastruktury závisí na informacích z jiné infrastruktury. Předpokládá existenci informační infrastruktury.*
- *Územně vzájemná závislost infrastruktury nastává, pokud události v území mohou měnit stavy infrastruktur.*
- *Logická vzájemná závislost znamená, že stav jedné infrastruktury závisí na stavu jiné infrastruktury, přičemž mechanismus propojení není fyzický, kybernetický nebo územní. Jedná se o závislost přenášené přes toky, kterými jsou předpisy, finance, legislativa apod., jedná se např. o finanční trhy.*

Kvůli vzájemné závislosti může porucha či selhání jedné dílčí infrastruktury způsobit poruchu nebo selhání druhé dílčí infrastruktury. Je proto důležité zajistit celý soubor dílčích infrastruktur systémově, tzn. hledat řešení problému bezpečnosti systému systémů. **[*22*]**

Infrastrukturu mohou charakterizovat také typy poruch a selhání (kaskádní a eskalující poruchy, porucha ze stejných příčin – např. živelní pohroma), provozní stav, míra těsnosti vztahů a propojení a charakteristiky infrastruktury (časové, územně prostorové, organizační, vlastnické a institucionální).

3.2.1 Provozní spolehlivost

Z hlediska fungování společnosti je důležité bezpečné poskytování služeb tzv. provozní spolehlivost. Provozní spolehlivost dílčích infrastruktur i kritické infrastruktury je to, co člověk může ovlivnit. Provozní spolehlivost systému znamená, že systém plní stanovené

požadavky a jeho provoz vyhovuje stanoveným podmínkám. Tato souhrnná vlastnost se rozkládá do dvou základních vlastností, kterými jsou zranitelnost a odolnost.

Odolnost je třeba chápat jako jistou funkční schopnost kritické infrastruktury plnit úkoly i za abnormálních a kritických podmínek. Pro dosažení tohoto stavu je nutné, aby kritická infrastruktura měla určitou adaptační kapacitu.

Z provozní spolehlivosti vyplývá, že hodnocení kritické infrastruktury specifikují tři základní vlastnosti – pružná odolnost (resilience), zranitelnost a schopnost adaptace. **[*23*]**

Pružná odolnost kritické infrastruktury je mírou schopnosti KI absorbovat změny stavu vyvolané možnou pohromou (včetně interakcí).

Zranitelnost kritické infrastruktury je neschopnost KI reagovat na výskyt možné pohromy (včetně interakcí).

Adaptace kritické infrastruktury je schopnost KI přizpůsobit strukturu prvků, vazeb a toků kritické infrastruktury tak, aby dopady pohromy (včetně interakcí) nebyly pro kritickou infrastrukturu nepřijatelné.

3.2.2 Kritičnost

V souvislosti s kritickou infrastrukturou lze kritičnost definovat jako relativní míru dopadů četností výskytu poruch a selhání. **[*24*]**

Stanovení kritičnosti se vztahuje k velikosti dopadů a ztráty funkčnosti infrastruktury na společnost. Na kritičnost má také vliv lidský systém, tedy jeho veřejná správa, podnikatelské subjekty, vzdělávací a vědecké instituce a občanská sdružení.

Stanovení kritičnosti může být popsána následovně: **[*25*]**

- *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.

3.2.3 Poruchy kritické infrastruktury

Poruchy a selhání kritické infrastruktury mohou souviset nejen s fyzikálně-chemickými procesy (koroze, opotřebení), ale také chybným řízením a projektováním. I když jsou poruchy přirozené, dochází k vývoji novějších technologií, které jsou složitější a vyznačují se síťovou strukturou, proto se u nich riziko poruch zvyšuje.

U kritické infrastruktury můžeme rozlišovat tyto typy poruch: **[7]**

- *Kaskádní porucha – porucha v jedné infrastruktuře je příčinou poruchy nějakého prvku či subsystému v jiné infrastruktuře, což vyvolá nefunkčnost takovéto infrastruktury.*
- *Eskalující porucha – porucha v jedné infrastruktuře zhoršuje parametry poruchy v jiné infrastruktuře.*
- *Společná porucha – dvě a více infrastruktur mají současně poruchu a tyto poruchy mají obdobnou příčinu. K tomuto typu dochází většinou vlivem přírodních pohrom.*

3.3 Řízení rizik kritické infrastruktury

Řízení rizik kritické infrastruktury vyžaduje systémový přístup, neboť činnost každého prvku závisí na tom, jak funguje celek a účinnost celku je zase podmíněna fungováním jednotlivých prvků. Úkolem řízení rizik je omezit příčiny a důsledky negativních jevů působících na systém daného typu.

Řízení rizik se skládá ze čtyř vzájemně provázaných fází: **[7]**

- *Identifikace rizik, která spočívá v určení rizik.*
- *Ohodnocení rizik, které se zabývá určováním rizikových událostí na základě analýzy. Posuzuje se pravděpodobnost výskytu, potenciální dopad, vážnost rizik a odhad času, ve kterém se riziko může objevit.*
- *Strategie zvládnutí rizik (schopnost plánovat).*
- *Monitoring rizik (neustálé kontrolování nových rizikových událostí, které nebyly stanoveny).*

3.4 Význam kritické infrastruktury v České republice

Kritická infrastruktura má pro společnost v České republice velký význam, neboť zajišťuje bezpečný chod státu, fungování ekonomiky a veřejné správy a základní životní potřeby obyvatelstva. Její poškození by mělo dopady hospodářské, politické, sociální, psychologické a také dopady na životní prostředí.

4 PRVKY KRITICKÉ INFRASTRUKTURY A JEJICH CHARAKTERISTIKA

Jednotlivé prvky kritické infrastruktury jsou v současné době členěny do devíti oblastí a třiceti sedmi produktů a služeb (příloha 1). **[*18*]**

4.1 Energetika

Energetika je nejzranitelnějším prvkem kritické infrastruktury. Bez ní se nedokážou obejít mnohé prvky kritické infrastruktury, např. systém dodávky vody, kanalizační systém, přepravní síť, komunikační a informační systémy, bankovní a finanční sektor, nouzové služby apod.

Energetickou infrastrukturu tvoří energetické společnosti zajišťující energetické transformace (rafinérie, elektrárny, teplárny) a dopravu energie (ropovody, plynovody, elektrovody, teplovody). Převážná většina těchto společností je zprivatizována a jejich podnikání se tak řídí obchodním zákoníkem.

Energetický systém ohrožují různé pohromy, např. technologické havárie kritických prvků, vazeb a toků v systému. Nebezpečná může být také vada materiálu a jeho stárnutí či nedostatečná údržba. K dalším hrozbám patří chyby nebo selhání řídicího systému, lidské chyby, přírodní pohromy, teroristický útok, kriminální čin nebo válka.

Nejvíce zranitelné jsou pozemní a nadzemní objekty, a to především venkovní elektrická vedení, nad zemí umístěné části a armatury plynovodů a produktovodů a bezobslužné objekty, kterými jsou malé transformátory, spínací stanice, redukční stanice a výměníkové stanice. Energetické, chemické i jaderné technologie a provozy jsou projektovány tak, aby zvládly chyby obsluhy a selhání zařízení. Téměř nechráněné jsou tzv. dlouhé liniové stavby (přenosová vedení, tranzitní a vysokotlaké plynovody, ropovody a produktovody) vedoucí územím, které není nijak chráněno a je veřejně přístupné. Jsou jen dálkově monitorovány a řízeny prostřednictvím řídících a dispečerských systémů. Největší problémy jsou u elektřiny, protože tu nelze skladovat.

4.1.1 Elektřina

Elektroenergetiku můžeme chápat jako celostátně plošný systém s vazbami na systémy okolních států. Pokud dojde k narušení její rovnováhy a závada není odstraněna, může nastat tzv. blackout. Pokud se setkají další nepříznivé okolnosti, může dojít i k domino efektu.

Nejzranitelnějšími prvky elektrizační soustavy jsou stožáry vedení 400 kV a transformátory 400/110 kV. Nejvážnější hrozbu pro přenosovou soustavu představuje koordinovaný vícenásobný teroristický útok, který by byl zaměřen současně na několik kritických míst systému. Z přírodních pohrom je nejzávažnější orkán a tvorba námrazy. **[*26*]**

Jedno z nejzávažnějších ohrožení ekonomického vývoje je tedy výpadek zásobování elektřinou velkého rozsahu, tzv. blackout. Příčinou je vzájemná závislost, která může vyvolat

kaskádové a dominové šíření krizových situací. Příklady důsledků déletrvajících výpadků dodávky elektřiny jsou známy ze zahraničí. Například na severovýchodě USA a v Kanadě v roce 2003 došlo k poruchám v důsledku zkratu při kontaktu vodiče venkovního vedení se stromem. Toto přetížení vyvolalo kaskádovité šíření poruchy, které vyřadilo 256 elektráren. Událost zasáhla 50 milionů obyvatel a měla vliv také na provoz některých služeb (poruchy v zásobování vodou, ochromena železniční a letecká doprava, výpadky mobilních telefonních sítí apod.). Dalším blackout zažila téhož roku Itálie, kde příčinou byla bouřka, která vyřadila mezistátní vedení zásobující Itálii ze Švýcarska. Výpadek elektřiny postihl 56 milionů obyvatel. U nás jsou zkušenosti s výpadky elektřiny v souvislosti s orkánem Kyrill v roce 2007 a vichřicí Emma v roce 2008, při kterých došlo k výpadku elektřiny v důsledku popadaných stromů a silného větru. Téměř milion domácností bylo bez proudu a došlo také k nefunkčnosti některých služeb, např. vysílačů mobilního signálu.

Odlehčit sítě může decentralizace zdrojů. Zde je možné využít obrovský potenciál stovek městských výtopen, které je možno zrekonstruovat tak, aby kromě tepla vyráběly také elektřinu, což by přineslo energetickou nezávislost.

4.1.2 Plyn

Česká republika je závislá na dovozu zemního plynu ze zahraničí. Spotřebu plynu pokrývá ze tří čtvrtin ruský plyn a zbývající čtvrtinu plyn norský. Zemní plyn je do naší republiky přepravován mezinárodními systémy dálkové dopravy plynu tvořenými tranzitními soustavami zúčastněných států. Tranzitní plynovod zajišťuje hlavně přepravu ruského plynu ve směru východ – západ do států EU.

Současná provozní konfigurace tranzitního plynovodu umožňuje i paralelní přepravu plynu ve směru západ – východ. Tato možnost byla využita i během loňské plynové krize, kdy byly přepravovány dodávky zemního plynu až na Slovensko. Našeho státu se však tato krize díky zásobám plynu nijak výrazně nedotkla.

Česká republika vlastní šest podzemních zásobníků plynu s celkovou kapacitou cca 2,3 miliardy m^3 zemního plynu. Díky těmto opatřením je náš stát schopen vydržet přibližně 50-60 dní bez dodávek ruského plynu. **[*27*]**

Energetická bezpečnost ČR je výrazně ovlivňována a formována v rámci EU, která usiluje o snížení své spotřeby plynu z Ruska. K dosažení tohoto cíle by měl přispět zejména systém plynovodů, z nichž některé jsou již realizované (plynovod Baku-Tbilisi-Erzurum tzv. Jihokavkazký plynovod). Nejvíce je prosazován plynovod Nabucco, který by měl vést přes Turecko, západní Balkán do střední Evropy s možností prodloužení do ČR. Potenciálním zdrojem plánovaných evropských plynovodů má být plyn z vybraných zemí Kaspického moře. **[*27*]**

4.1.3 Tepelná energie

Teplárenství je ta část energetiky, která kryje potřeby tepla bytových domů, objektů občanské vybavenosti a průmyslových podniků. Teplo je zajišťováno prostřednictvím soustav

centralizového zásobování teplem, které jsou tvořeny vzájemně propojenými zdroji tepla, tepelnými sítěmi, popřípadě předávacími stanicemi a vnitřními spotřebitelskými zařízeními.

Základní jednotku teplárenství tvoří teplárny, které vyrábí teplo i elektrickou energii. Teplo se dodává dvěma způsoby a to pomocí páry a teplonosné vody. Při použití teplonosné vody, mívá tepelná síť dvě potrubí. K cirkulaci teplé vody pak slouží čerpací stanice, které jsou na trase potrubí. Teplota vody se pohybuje kolem 100 až 110 °C, někdy i více kvůli rozdílu mezi přívodní a vratnou vodou. Teplou páru pak dodávají parní elektrárny většinou ve větších městech.

Teplárenství s kombinovanou výrobou elektřiny a tepla je jedním z nejdůležitějších prostředků snížení energetické náročnosti národní ekonomiky.

4.1.4 Ropa a ropné produkty

Česká republika je závislá na dodávkách ropy, které získává z ropovodů Družba začínající v Rusku a ropovodu IKL vedoucí z italského Terstu. Případné přerušení dodávek či okamžité zastavení může vyvolat vznik krizové situace, na kterou je vypracován typový plán.

V ČR je legislativa pro řešení ropných krizí poměrně dobře a rozsáhle upravena. Nouzové zásoby ropy jsou zabezpečovány prostřednictvím Správy státních hmotných rezerv (SSHR) ve vybraných ropných produktech. Podle vyhlášky SSHR č. 452/2002 Sb. mají nouzové zásoby ropy vydržet minimálně na 90 dní průměrné spotřeby předcházejícího roku. Pokud je průměrný měsíční dovoz ropy a ropných produktů natolik snížen nebo je důvodně snížení očekáváno, vyhlašuje vláda stav ropné krize, který může vyvolat i sekundární situace, např. narušení finančních toků, dodávek energií nebo funkčnosti veřejné dopravní soustavy. **[*28*]**

V roce 2001 se ČR stala členem Mezinárodní energetické agentury IEA (*International Energy Agency)*, která je autonomní mezinárodní organizací při OECD (*Organization for Economic Cooperation Development*) sdružující hospodářsky vyspělé státy zavázané přijímat společná opatření ke krizovým stavům způsobených zásobování ropou. Projednávají se zde situace na světovém trhu ropy, stav nouzových zásob v členských zemích IEA, bezpečnost dodávek ropy aj. **[*28*]**

4.2 Vodní hospodářství

Vodní hospodářství je jeden z nejzranitelnějších prvků kritické infrastruktury, neboť není možné ochránit spolehlivě vodní zdroje a tisíce kilometrů distribučních systémů.

Systém dodávky vody a čištění odpadních vod se skládá z těchto základní částí: **[*29*]**

- *Systém dodávky surové vody určené pro úpravu a konzumaci a jiné použití. Tento systém zahrnuje vodní nádrže, přehrady a studně se zásobou surové vody, vodní potrubí a čerpací stanice.*
- *Systém úpravy surové vody na pitnou nebo užitkovou. Tento systém zahrnuje mechanické čištění, filtraci, biologické čištění a chemickou úpravu.*

- *Distribuční systém upravené vody, tj. čerpací stanice, potrubní síť upravené vody, nádrže a tlakové rezervoáry.*
- *Systém čištění odpadních vod, který zahrnuje kanalizační síť a čistící stanice odpadních vod.*

Úkolem systému je zásobovat města nebo průmyslové objekty pitnou, užitkovou nebo technologickou vodou a vyčistit odpadní vody od škodlivých látek na úroveň danou platnými normami. Podle účelu použití vody jsou navrženy parametry jednotlivých částí celého systému, tj. výkon, stupeň úpravy surové vody a způsob čištění odpadní vody.

Dodávky vody a kanalizace může selhat vlivem různých událostí, např. vlivem technologických závad, lidskou chybou, přírodních pohrom, haváriemi zařízení či objektů nebo teroristickým útokem.

K nejzranitelnějším objektům patří zařízení s otevřenou hladinou, které tvoří vodárenské nádrže, úseky recipientů s jímacími objekty surových vod určených k úpravě na vody pitné, prameniště podzemních vod, vodojemy, přerušovací komory distribučních systémů.

4.2.1 Zásobování pitnou a užitkovou vodou

Při krizových situacích může dojít k situaci, kdy systém zásobování vodou nefunguje. Tento problém řeší nouzové zásobování pitnou vodou, které lze zabezpečit pouze vyhlášením krizového stavu. Upřednostňuje se využití podzemních vodních zdrojů před povrchovými z důvodu jejich menší zranitelnosti.

Zabezpečení pitné vody zajišťují orgány státní správy neprodleně a nejpozději do pěti hodin od ukončení dodávky vody. Organizační zabezpečení systému nouzového zásobování obyvatelstva vodou vychází za krizových situací z platných právních norem a smluvních vztahů a požadavku. Příprava je realizována zpracováním a schválením krizových plánů a přijetím nezbytných opatření. **[*30*]**

4.2.2 Zabezpečení a správa povrchových vod a podzemních zdrojů vody

Jakost povrchových i podzemních vod je ohrožována různými zdroji znečištění. Nebezpečné jsou skládky nebezpečných odpadů a negativně působí také havarijní znečištění. Dochází k celé řadě případů ekologických katastrof s následným ohrožením stavu jakosti vod. Nejpočetnější skupinou znečišťujících látek jsou látky ropného původu, dále pak látky chemické.

V současné době existuje pozorovací síť podzemních vod, která byla projektována v letech 1956-1962. Síť se skládá z mělkých a hlubokých vrtů a pramenů. Mělké vrty slouží ke sledování pohybu a složení kvartéru říčních vod a hluboké vrty slouží ke sledování hydrogeologické struktury podzemní vody.

4.2.3 Systém odpadních vod

Odpadní vody jsou definovány podle zákona č. 138/1973 Sb., o vodách, jako „vody použité na sídlištích, obcích, domech, závodech, ve zdravotnických zařízeních a jiných objektech či zařízeních, pokud po použití mají změněnou jakost, jakož i jiné vody, z nichž odtékající, pokud mohou ohrozit jakost povrchových nebo podzemních vod."

K odvádění odpadní vody slouží systém odpadních vod neboli kanalizace, které vedou do čističek, kde se voda vyčistí a vypouští do řeky. Díky úpravám v oblasti legislativy i v oblasti ekonomických nástrojů a programů došlo k postupnému snižování množství vypouštěného znečištění do odpadních vod, což zlepšuje i jakost vod povrchových.

4.3 Potravinářství a zemědělství

V současné době je společnost vystavena mnoho rizikovým faktorům, ke kterým patří i různé chemické škodliviny a karcinogenní látky v životním prostředí vznikající v důsledku lidské činnosti. Proto se zvyšuje zájem o bezpečnost potravin, které spotřebitelé konzumují.

4.3.1 Produkce potravin

Základní strategickou úlohou zemědělství by měla zůstat produkce potravin potřebných pro život společnosti. Obzvlášť v době rostoucích rizik je třeba upozornit na přehodnocení a zlehčování konceptu potravinové bezpečnosti. Dnes zemědělství nenaplňuje svoji základní funkci. Malé zemědělské firmy jsou ohrožovány zemědělskými politikami, které podporují vysoké vstupy, liberalizaci obchodu a orientují se na export. Takové zemědělství pak klade minimální požadavky na životní prostředí. Velké společnosti mají velký vliv na konkurenci – ovlivňují ceny a nastavují tak standardy pro zemědělský sektor.

4.3.2 Péče o potraviny

Bezpečnost potravin zajišťuje Ministerstvo zemědělství a Ministerstvo zdravotnictví. Starají se i o legislativní prostředky pro ochranu a bezpečnost potravin. Dohled nad zemědělskou výrobou, zpracováním, přepravou, distribucí potravin a surovin živočišného původu mají krajské veterinární správy a Městská veterinární správa v Praze.

V oblasti bezpečnosti potravin byl také rozvinut evropský Systém rychlého varování pro potraviny a krmiva (*Rapid Alert System for Food and Feed* RASFF), umožňující uživatelům získat důležité informace v oblasti bezpečnosti potravin. Tento systém je vzájemně propojenou sítí, která spojuje členské země Evropské unie, Norsko, Lichtenštejnsko a Island s Evropskou komisí a Evropským úřadem pro bezpečnost potravin. Systém RASFF slouží k ohlášení rizikových potravin a krmiv, aby se zamezilo jejich oběhu na evropském trhu. Tento systém funguje i v ČR a národním kontaktním místem tohoto systému je Státní zemědělská a potravinářská inspekce. **[*31*]**

4.3.3 Zemědělská výroba

Současné tendence v zemědělské výrobě spočívají v omezování snahy o maximální výnosy díky používání pesticidů a minerálních hnojiv. Prosazuje se tzv. trvale udržitelné zemědělství, tedy ekologické obdělávání krajiny, které vylučuje převážnou část použití umělých hnojiv a pesticidů, přídatných látek v krmivech a geneticky modifikovaných organismů. Díky tomu také dochází k bezpečnosti potravin, protože nepřicházejí do kontaktu s chemickými látkami.

4.4 Zdravotní péče

Kritickou zdravotnickou infrastrukturu tvoří zejména zdravotnická zařízení neodkladné péče, resortní organizace zdravotnické logistiky a další účelová zařízení nutná k zajištění nezbytné zdravotní péče jako minimální úrovně poskytované zdravotní péče obyvatelstvu za krizových situací.

Je důležité zajistit funkčnost kritické infrastruktury zdravotnictví pro poskytování zdravotní péče a ochrany veřejného zdraví při mimořádných událostech a za krizových situací. K možným nebezpečím, která mohou ohrozit chod nemocnice, patří fyzické poškození budov (povodně, bouře, požár), výpadky kvůli místnímu narušení (výpadku) infrastruktury (dopravní cesty, elektrický proud), hromadný příjem pacientů, migrace z oblastí postižené katastrofou, vznik epidemie následkem dlouhodobého výpadku zásobování vodou. Pro snížení hrozby přerušení provozu je cílené zlepšení odolnosti zdravotnického zařízení vůči možným rizikům.

4.4.1 Přednemocniční neodkladná péče

Přednemocniční neodkladná péče (PNP) je definována jako péče o postižené na místě jejich úrazu nebo náhlého onemocnění, v průběhu jejich transportu k dalšímu odbornému ošetření a při jejich předání do zdravotnického zařízení. Zahrnuje zdravotnickou záchrannou službu včetně letecké zdravotnické záchranné služby a nezbytné transportní kapacity dopravy zraněných. **[*32*]**

PNP je poskytována při stavech, které bezprostředně ohrožují život postiženého, mohou vést prohlubováním chorobných změn k náhlé smrti, způsobí bez rychlého poskytnutí odborné první pomoci trvalé následky, působí náhlé utrpení a bolest a působí změny chování a jednání ohrožující postiženého nebo jeho okolí. **[*32*]**

4.4.2 Nemocniční péče

V České republice je nemocniční péče poskytována sítí nemocnic a lékařských zařízení. Tato zdravotní zařízení jsou soukromá i veřejná a některá z nich jsou vytipována jako objekty kritické infrastruktury.

Pokud dojde ke krizové situaci, která trvá desítky dnů a déle, je pro systém zdravotnictví důležitá připravenost systému nouzového hospodářství a systém hospodářské mobilizace. Týká se to krizových stavů při vojenském ohrožení.

Ke službám, které lékařská zařízení zajišťují, patří ambulantní, lůžková, preventivní, neodkladnou péči, zařízení zajišťující léčiva a zdravotní pomůcky apod.

4.4.3 Ochrana veřejného zdraví

Každá společnost musí chránit veřejné zdraví občanů a mít vytvořenou i potřebnou legislativu, která tyto povinnosti vymezuje a stanovenou i soustavu orgánů ochrany veřejného zdraví s definovanou působností a pravomocí. V ČR takovýto právní předpis tvoří zákon č. 258/2000 Sb., o ochraně veřejného zdraví, který zpracovává i příslušné předpisy Evropských společenství.

Podle zákona je ochrana veřejného zdraví souhrn činností a 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. Zákon obsahuje požadavky na vodu, chemické přípravky a vodárenské technologie a hygienické požadavky na koupaliště a sauny, podmínky vnitřního prostředí staveb, hygienické požadavky na venkovní hrací plochy, na provoz zdravotnických zařízení, na předměty běžného užívaní, podmínky ochrany před hlukem, vibracemi a neionizujícím zářením, podmínky nakládání s nebezpečnými chemickými látkami apod.

4.4.4 Výroba, skladování a distribuce léčiv a zdravotnických prostředků

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.

4.5 Doprava

Doprava má obrovský význam pro rozvoj hospodářství státu a zabezpečení sociálních potřeb obyvatelstva. Její ohrožení může způsobit narušení bezpečnosti, ekonomické a sociální stability společnosti a zachování nezbytného rozsahu dalších základních funkcí státu při krizových situacích. Ochránit kritickou dopravní infrastrukturu úplně je ale nemožné. Hlavním cílem jsou proto opatření snižující potenciální rizika ohrožení dopravní infrastruktury, což vyžaduje značné finanční náklady.

Přepravní systém obstarává dopravu osob a nákladů. Patří sem všechny způsoby dopravy, které mezi sebou spolupracují a vytváří logistickou dopravní síť. Doprava je společně s energetikou považována za základ hospodářské prosperity. Přepravní síť je tvořena samostatnými celky a pro každý z nich je charakteristický určitý druh dopravního prostředku, který je doplněný komplexem provozních a administrativních částí tvořící podsystémy. Tyto celky mají schopnost samostatného provozu.

V ČR je přepravní síť složena z železničního, silničního, leteckého a vodního dopravního systému. Tyto systémy mohou být ohroženy přírodními pohromami, velkými dopravními

nehodami, technologickými haváriemi objektů nacházejícími se v jejich blízkosti, kriminálními činy, teroristickými útoky a válkou.

4.5.1 Silniční doprava

Silniční doprava se v současné době velmi rozvíjí a realizuje největší přepravní výkony v osobní i nákladní dopravě. Hustota přepravy na dálnicích a silnicích I. třídy představuje neustálé riziko vzniku dopravní nehody s následky jak pro účastníky silničního provozu, tak pro ostatní obyvatelstvo, přírodu a infrastrukturu. Navíc se vzrůstající silniční dopravou po vstupu do EU se zvyšují rizika s nedostačující kapacitou hlavních přepravních tepen. **[*33*]**

Bezpečnost silniční dopravy je jedním z kvalitativních kritérií, kterými se hodnotí silniční a provozní podmínky na silniční síti. Úseky s vysokým procentem dopravních nehod se označují jako kritické nehodové lokality. Ve smyslu rezoluce Rady 2000/731/ES o zvyšování bezpečnosti silniční dopravy se přijímají opatření na odstranění příčin vzniku dopravních nehod. **[*33*]**

Údržba dálnic a silnic I. třídy spadající pod správu Ředitelství silnic a dálnic ČR je zajišťována třinácti středisky správy a údržby dálnic, resp. rychlostních silnic, která vykonávají správu a údržbu komunikace a jeho součástí, zabezpečují informační službu o sjízdnosti svěřeného úseku, předkládají návrhy na jejich zlepšení.

4.5.2 Železniční doprava

Železniční doprava hraje i v současné době důležitou roli v dopravním zabezpečení života společnosti kvůli své přepravní rychlosti, objemu přepravních úkonů a poměrně vysoké spolehlivosti. Spolu se silniční dopravou je hlavním druhem dopravy u nás.

Železniční doprava je kvůli své složitosti zranitelná vůči teroristickým útokům či živelným pohromám. Případná havárie na železnici by mohla mít nepříznivý vliv na život obyvatel, ohrozit jejich životy, poškodit životní prostředí. Také odstranění případných následků bývá nákladné a obtížné, protože může dojít k poruchám mostů, tunelů či trolejového vedení.

4.5.3 Letecká doprava

Letecká doprava je nejvíce rostoucím odvětvím dopravy nejen u nás, ale i ve světě. Nabízí nejbezpečnější a nejrychlejší způsob dopravy osob a je nepostradatelná i v dopravě mnoha druhů zboží. Také tato doprava může být ohrožena technickými poruchami, teroristickým útokem, počasím a v neposlední řadě také přírodními katastrofami. Příkladem může být nedávný výbuch sopky na Islandu, který omezil leteckou dopravu nejen na samotném ostrově, ale v celé Evropě na několik dní.

V letecké dopravě jsou kladeny vysoké nároky na použitý materiál při výrobě letadel a v oblasti ochrany jsou kladeny vysoké nároky na dokonalou organizaci a řídící činnost.

4.5.4 Vnitrozemská vodní doprava

Vnitrozemská vodní doprava se podílí na přepravě velmi málo. Nejvýznamnější je pro ČR mezinárodní doprava po labské vodní cestě. Samotný provoz vodní dopravy má v porovnání s ostatními druhy dopravy malý vliv na životní prostředí a je bezpečný. Problémy v této dopravě způsobují splavnosti některých řek.

4.5.5 Současný stav dopravní infrastruktury

Údržba pozemních komunikací a železnic zaostává kvůli nedostatečným finančním prostředkům, nedokonalé koordinaci a dlouhodobého přibývání komunikací, jejichž stav je havarijní a jejichž další provoz je možný jen za cenu neúměrně náročné údržby. S ohledem na bezpečnostní a technické parametry je stávající síť silnic a dálnic i železniční trati v ČR v nevyhovujícím stavu. **[*34*]** Je proto nutné hledat nové zdroje financování.

Bezpečnost v dopravě můžeme rozdělit na vnitřní, kterou se rozumí bezpečnost dopravního provozu, vytváření podmínek pro snížení nehodovosti u všech druhů dopravy a tvorba pravidel pro přepravu nebezpečného zboží, a vnější, kterou rozumíme ochranu proti terorismu, vandalismu, přírodním živlům apod.

Téměř 95 % všech dopravních nehod zaviní účastníci provozu na pozemních komunikacích a jsou proto klíčovým aspektem silniční dopravy. Bezpečnostní parametry železniční dopravy jsou v ČR obecně velmi dobré, obzvlášť ve srovnání se silniční dopravou. Největší bezpečností se vyznačuje letecká doprava, i když následky případných nehod jsou vždy katastrofální. **[*34*]**

4.6 Komunikační a informační systém

Komunikační a informační systém kritické infrastruktury zahrnuje takové fyzické systémy a systémy informačních technologií, které jsou nezbytné k zachování komunikace a zpracování dat mezi subjekty zařazených do KI. Omezení nebo ohrožení daných systému by mělo vliv na chod dalších systémů, které jsou s informačním systémem propojeny. **[*29*]**

Strukturu informačních a komunikačních systémů můžeme rozdělit do tří základních částí: **[*29*]**

- *Procesní struktura, která popisuje logiku informačního systému. Popisuje, jaká data se mají kam a kdy šířit, jak se s nimi bude zacházet, zpracovávat a uchovávat.*
- *Technická struktura (hardware) popisující technické prostředky a prostředí realizace informačního systému. Skládá se z výpočetní techniky, periferní a podpůrné techniky, komunikační techniky a z transportních médií.*
- *Programová struktura (software), která představuje vytvořené programy a aplikace realizující část procesní struktury na technické struktuře. Skládá se z řídicích systémů, z produkčních a servisních systémů.*

Jednotlivé prvky a části této infrastruktury jsou vzájemně závislé. Pokud dojde k výpadku procesní struktury, ztrácí význam technická i programová struktura.

Komunikační a informační systémy jsou dále rozděleny na několik podskupin – služby pevných telekomunikačních sítí, služby mobilních telekomunikačních sítí, radiová komunikace a navigace, satelitní komunikace, televizní a radiové vysílání, poštovní a kurýrní služby, přístup k internetu a datovým službám.

Pohromy, které mohou způsobit škody na informačních a komunikačních systémech, mohou být technologického, lidského, přírodního či úmyslného původu. Aby byly tyto systémy chráněny, je důležité určit v každém určitém místě rizika, která jsou spojena s možnou pohromou, a stanovit možné škody, které mohou vznikat při uskutečnění rizika.

4.7 Bankovní a finanční sektor

Finanční systém je tvořen souborem trhů, institucí, zákonů, regulací a technik, prostřednictvím kterých jsou realizovány finanční transakce. Dochází zde k hotovostním a bezhotovostním úhradám, jsou obchodovány obligace, akcie a jiné cenné papíry, určovány úrokové sazby atd. Na finančním systému jsou závislí spotřebitelé, podnikatelé, investoři a také občané, proto musí pracovat rychle, efektivně a kvalitně. Finanční systém je snadno ovlivňován různými společenskými změnami, např. politickými převraty, válkami, sociálními změnami či živelnými pohromami, v jejichž důsledku se může negativně měnit situace na finančních trzích. **[*29*]**

Bankovní a finanční sektor mají na starosti Ministerstvo financí a bankovní sektor. Ministerstvo financí zabezpečuje chod státních financí, příjmy a výdaje státního rozpočtu, závazky vůči státní správě, obyvatelstvu, zahraničí a legislativu. Bankovní sektor zahrnuje centrální banku (Česká národní banka ČNB), obchodní banky a další finanční instituce. ČNB dohlíží na emisní činnost, měnovou politiku, bankovní dohled, správu státních rezerv, banku státu a mezibankovní operace. Komerční banky zabezpečují vedení účtů podnikové sféře, obyvatelstvu a veřejnému sektoru a zároveň zabezpečují operace na finančním trhu a jsou nositelé plateb v tuzemsku i zahraničí.

Banky zacházejí se svým kapitálem tak, aby se co nejvíce zhodnotil, což přináší různá rizika, např. kreditní, tržní, vnější rizika, dále rizika spojená s řízením a rozhodováním a bezpečnostní rizika.

4.7.1 Správa veřejných financí

Veřejné finance představují vztahy vznikající v souvislosti s tvorbou, rozdělováním a užitím peněz patřícím občanům a tedy i veřejnoprávním orgánům a organizacím, které s těmito penězi nakládají a spravují je. Správu veřejných financí má na starosti Ministerstvo financí.

Veřejné finance jsou rozdělovány na principu nenávratnosti, neekvivalence a nedobrovolnosti. Patří sem státní rozpočet, rozpočty obcí, svazku obcí a krajů a speciální fondy, např. Státní fond životního prostředí.

4.7.2 Bankovnictví

Bankovní systém je v ČR rozdělen od roku 1990 na dva stupně, které tvoří centrální banka zajišťující měnovou stabilitu a obchodní banky podnikající na základě ziskového principu. Bankovnictvím se zabývají dva zákony – zákon č. 21/1992 Sb., o bankách a zákon č. 6/1993 Sb., o České národní bance. Bankovní služby můžeme rozdělit podle různých parametrů, např. poskytují úvěry, provádějí platební styk se zahraničím, směnárenskou činnost či operují s cennými papíry. Díky rozvoji moderních technologií vzniklo přímé bankovnictví, které umožňuje komunikaci klienta a banky pomocí internetu nebo mobilního telefonu, což sebou nese určité riziko podvodu či lidského omylu.

4.7.3 Pojišťovnictví

V ČR je pojišťovnictví zakotveno v zákoně č. 363/1999 Sb., o pojišťovnictví, který upravuje podmínky provozování pojišťovací a zajišťovací činnosti pojišťovny a její činnost. Dále je upravováno občanským zákoníkem a vyhláškami Ministerstva financí, které vykonává i dozor.

Úkolem pojišťoven je ochrana občanů a organizací před nepříznivým dopadem nahodilých událostí. Pojišťovny poskytují pojistnou ochranu občanům či organizacím, bezporuchový chod ekonomiky státu a poskytují také poradenskou činnost.

4.7.4 Kapitálový trh

Kapitálový trh je místo, kde dochází ke směně kapitálu prostřednictvím cenných papírů na burze. Burza cenných papíru se řídí zákonem č. 214/1992, o burze cenných papírů a dalšími předpisy, jako jsou burzovní pravidla, burzovní řád atd.

4.8 Nouzové služby

Nouzové služby představují minimální rozsah činností nutných k zabezpečení ochrany životů, zdraví a majetku občanů. Spočívají především v zabezpečení vnitřního pořádku a bezpečnosti, ochraně před účinky mimořádných událostí a plnění dalších opatření v oblasti ochrany obyvatelstva. **[*15*]**

4.8.1 Hasičský záchranný sbor ČR a příslušné jednotky požární ochrany

Hasičský záchranný sbor (HZS) České republiky byl zřízen na základě zákona č. 238/2000 Sb., o Hasičském záchranném sboru České republiky. HZS ČR řeší jednak preventivní připravenost a jednak přímé řízení a koordinaci záchranných a likvidačních prací prostřednictvím svých zásahových složek, vyčleněných orgánů krizového řízení působících v krizových štábech, operačních střediscích apod. při velkých mimořádných událostech a krizových stavech. Prioritním cílem je záchrana lidských životů, majetku, kulturních hodnot a ekosystémů ve vazbě na územní rozvoj. V oblasti prevence se HZS zaměřuje na plánování nezbytných opatření opět pro ochranu obyvatelstva, jeho majetku s respektováním ekosystému ve správním území. Dále se účastní na tvorbě technologií v preventivních

oblastech se zaměřením na bezpečnost a zabezpečení subjektů z pohledu protipožární prevence. V rámci Ministerstva vnitra je zřízeno Generální ředitelství HZS ČR, které plní funkci strategické koordinace územních složek HZS. Také plní funkci odborného garanta v dalších specifických oblastech. **[*35*]**

4.8.2 Policie ČR

Policie České republiky (PČR) je ozbrojený bezpečnostní sbor České republiky s působností na celém území republiky. Zabezpečuje vnitřní bezpečnost a veřejný pořádek. Vznikla na základě zákona č. 273/2008 Sb., o Policii České republiky a je řízena Ministerstvem vnitra. PČR plní úkoly zejména ve věcech vnitřního pořádku a bezpečnosti, zejména chrání bezpečnost osob a majetku, spolupůsobí při zajišťování veřejného pořádku, vede boj proti terorismu, vede vyšetřování trestných činů, vyhlašuje celostátní pátrání, zajišťuje pohotovostní ochranu jaderných zařízení ochranu ústavních činitelů a důležitých objektů apod.

4.8.3 Armáda ČR

Armáda České republiky (AČR) je hlavní složkou ozbrojených sil ČR, které dále tvoří Vojenská kancelář prezidenta republiky a Hradní stráž. Úkoly armády popisuje zákon č. 219/1999 Sb., o ozbrojených silách ČR. Vrchním velitelem ozbrojených sil ČR je prezident republiky. Hlavním posláním AČR je co nejefektivnější a nejlepší zabezpečení obrany na území ČR. Je zapojena do integrované vojenské struktury NATO, do systému obranného, operačního a civilního nouzového plánování, do organizačních aspektů jaderných konzultací a do společných cvičení a operací.

4.8.4 Radiační monitorování

Monitorování radiační situace na území ČR je zajišťováno hlavně celostátní Radiační monitorovací sítí (RMS), jejichž řízením je pověřen Státní úřad pro jadernou bezpečnost (SÚJB). Právní rámec tvoří zákon č. 18/1997 Sb., o mírovém využívání jaderné energie a ionizujícího záření, tzv. atomový zákon.

Od roku 2007 provádějí monitorování radiační situace na území ČR složky RMS:

- *Síť včasného varování*
- *Síť včasného zjištění*
- *Síť termoluminiscenčních dozimetrů*
- *Síť monitorování radioaktivních látek v ovzduší*

Data získána pomocí RMS slouží pro hodnocení radiační situace, pro potřeby sledování a posuzování stavu ozáření. V případě radiační havárie se na základě měření stanovují opatření vedoucích ke snížení nebo odvrácení ozáření.

4.8.5 Předpovědní, varovná a hlásná služba

Předpovědní, varovná a hlásná služba má především preventivní charakter, ale je důležitá v průběhu mimořádné události, kterou může být povodeň, únik nebezpečné látky do životního prostředí, sesuv půdy apod.

Předpovědní služba se v ČR používá především při povodních a je zabezpečována Českým hydrometeorologickým úřadem ve spolupráci se správci povodí. V souvislosti s povodněmi je zde ještě hlásná povodňová služba, která informuje povodňové orgány a občany o vývoji povodňové situace a předává zprávy a hlášení potřebná k vyhodnocení opatření na ochranu před povodněmi.

4.9 Veřejná správa

Veřejnou správou se rozumí správa veřejných záležitostí, která je uskutečňována ve veřejném zájmu. Subjektem veřejné správy je v první řadě stát a dále jiné subjekty, které k tomu byly zmocněny zákonem. Veřejná správa je tvořena dvěma subsystémy a to státní správou a samosprávo, které zabezpečují plnění ekonomických, sociálních a politických úkolů stanovené státem tak, jak jsou určeny ve státních cílech a zabezpečované v právním řádu.

V současnosti je zvyšován požadavek přípravy lidí a nezbytnost investic do celoživotního vzdělávání pracovníků veřejné správy.

4.9.1 Státní správa a samospráva

Státní správa je veřejná správa uskutečňována státem. Tvoří ji správní úřady, které rozlišujeme podle působnosti na ústřední správní úřady a na územní správní úřady. Celý systém státní správy řídí vláda, která je oprávněna vydávat prováděcí předpisy, řídit, kontrolovat a sjednocovat činnost ministerstev a jiných ústředních správních úřadů, kontroluje prostředky státního rozpočtu a jmenuje vedoucí některých správních úřadů. Rozdělení její působnosti uvádí Ústava ČR a zákon č. 2/1969 Sb. (kompetenční zákon).

Samospráva je veřejnou správnou uskutečňovanou jinými veřejnoprávními subjekty než státem, tzn. obcemi a kraji. Představuje výkonné působení a ovlivňování společenského života prostředky nestátního charakteru.

4.9.2 Sociální ochrana a zaměstnanost

Sociální ochrana je zajišťována prostřednictvím systému sociálního zabezpečení. Celý tento systém je členěn do dílčích částí a to podle charakteru a délky trvání sociální události, která má být řešena. Mezi tyto části patří subsystém sociální pomoci (zahrnuje sociální dávky a sociální služby), subsystém státní sociální podpory a subsystém sociálního zabezpečení (zahrnuje důchodové a nemocenské pojištění).

Systém sociálního pojištění se zaměřuje na sociální situace, na které je možné se dopředu připravit, např. ztrátu příjmu v důsledku nemoci, stáří či ztráty zaměstnání. Systém státní

sociální podpory je podporou příjmu rodiny v některých životních situacích (péče o těžce zdravotně postiženou osobu, péče o nezaopatřené dítě). Sociální systém pomoci řeší zejména situace sociální a hmotné nouze (pokles příjmů pod životní minimum, sociální prevence).

4.9.3 Výkon justice a vězeňství

Výkon justice a vězeňství zajišťuje Ministerstvo spravedlnosti ČR. Tato služba je nutná pro zachování výkonu spravedlnosti, která tvoří jednu ze základních funkcí státu. Případné nedostatky v této oblasti mohou způsobit sekundární krizové situace.

5 MIMOŘÁDNÉ UDÁLOSTI OHROŽUJÍCÍ KRITICKOU INFRASTRUKTURU

Česká republika se stejně jako ostatní státy na úrovni mezinárodního společenství začala v posledních letech zabývat otázkou zranitelnosti kritické infrastruktury v souvislosti s mimořádnými událostmi, které mohou ohrozit jak obyvatelstvo tak také základní funkce státu. Důležité je v této souvislosti zvyšování prevence, připravenosti, zvládání následků mimořádných událostí a v neposlední řadě také obnova po mimořádné události.

5.1 Základní pojmy

Mimořádná událost (MU) je podle zákona č. 239/2000 Sb., o Integrovaném záchranném systému (IZS) škodlivé působení sil a jevů vyvolaných činností člověka, přírodními vlivy, a také havárie, které ohrožují život, zdraví, majetek nebo životní prostředí a vyžadují provedení záchranných a likvidačních prací.

Krizová situace je podle zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů, mimořádná událost, při níž je vyhlášen krizový stav. Je to taková situace, kdy hrozící nebezpečí nelze odvrátit nebo způsobené následky odstranit běžnou činností správních orgánů a složek integrovaného záchranného systému.

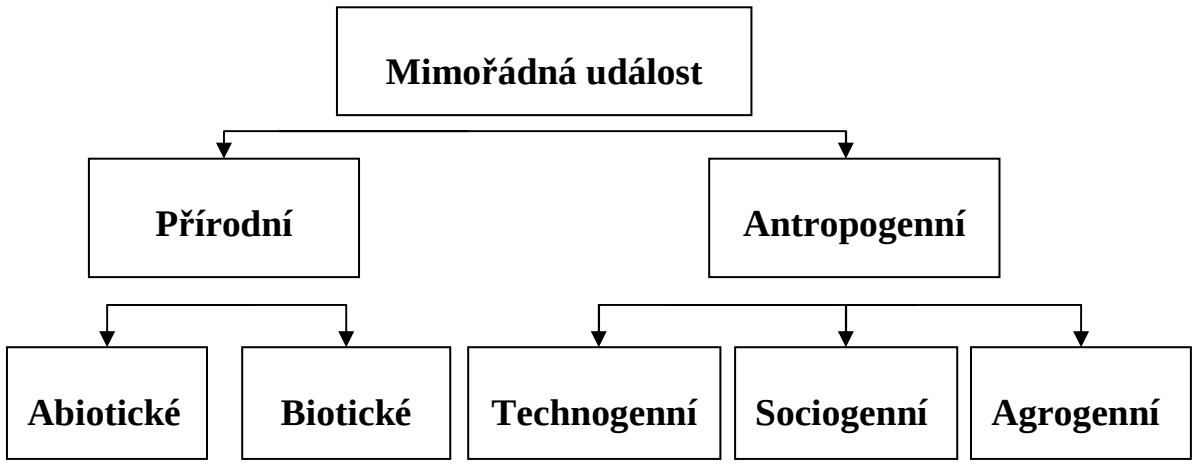
Živelná pohroma je neovládaná mimořádná událost vzniklá v důsledku působení ničivých přírodních sil. Objevuje se zpravidla náhle a neočekávaně. **[*36*]**

Katastrofa je náhle vzniklá mimořádná událost tak velkého rozsahu, že k likvidaci jejich následků se nedostává v postiženém území dostatek sil a prostředků a ohrožení není možné odvrátit běžnou činností správních úřadů a složek záchranného systému. **[*37*]**

Závažné havárie je podle zákona č. 59/2006 Sb., o prevenci závažných havárií, mimořádná, částečně nebo zcela neovladatelná, časově a prostorově ohraničená událost (např. závažný únik, požár nebo výbuch), která vznikla nebo jejíž vznik bezprostředně hrozí v souvislosti s užíváním objektu nebo zařízení, v němž je nebezpečná látka vyráběna, zpracována, používána nebo skladována, a vedoucí k vážnému ohrožení nebo k vážnému dopadu na životy a zdraví lidí, hospodářských zvířat a životního prostředí nebo k újmě na zdraví.

5.2 Rozdělení mimořádných událostí

Mimořádné události (MU) vyvolávají rizika vůči lidské společnosti, životnímu prostředí a kritické infrastruktuře a neustále jich přibývá. Nejčastěji se mimořádné události hodnotí podle jejich příčin nebo následků. Podle působící příčiny, můžeme MU rozdělit na přírodní MU a antropogenní MU, tedy způsobené člověkem. Přírodní se dále dělí na MU způsobené neživou přírodou (abiotické) a způsobené živou přírodou (biotické). Antropogenní MU dále rozdělujeme na technogenní, sociogenní interní, sociogenní externí a agrogenní. Technogenní MU souvisí s provozními haváriemi a haváriemi spojenými s infrastrukturou. Do sociogenních interních MU řadíme vnitrostátní společenské, sociální a ekonomické MU. Sociogenní externí MU jsou vojenského charakteru a agrogenní MU se týkají zemědělství a půdy (obr. 1)



Obrázek 1 Rozdělení mimořádných událostí **[*38*]**

Mimořádné události lze rozdělit podle dalších kritérií – doby trvání (krátkodobé, střednědobé, dlouhodobé), rychlosti vzniku MU (bodové, prahové), doby trvání, velikosti zasaženého území.

Často je používána také klasifikace podle World Health Organization (WHO). Ta rozděluje katastrofy do dvou hlavních skupin – přírodně-klimatické a antropogenní (tabulka 1).

Tabulka 1 Klasifikace katastrof dle WHO **[*36*]**

Přírodně-klimatické (voda, oheň, země, vzduch*)*	**antropogenní (sociálně – ekonomické*)***	
	válečný konflikt	**civilizační katastrofy**
tektonické – zemětřesení - požáry - sesuvy - tsunami - hladomor - epidemie **telurické** – sopečná činnost - bahnotok - sopečné povodně - žhavá sopečná mračna **topologické** - povodně - sesuv půdy - laviny **meteorologické** - cyklóny - nadměrná horka, sucha - mrazy - krupobití a přívalové deště	MU vojensko-politického charakteru v době míru: - náhodný jaderný výbuch - pád jaderné bomby - nacionalistické konflikty - teroristická a diverzní činnost - emigrační vlny	- doprava - vodní stavby - průmysl - toxické odpady - velké požáry - jaderná energie

5.2.1 Přírodní mimořádné události

Přírodní mimořádné události vznikají v důsledku působení přírodních sil. Způsobují škody na majetku, přírodě, poškozují zdraví a mnohdy způsobují i smrt. Vznikají rychlým nebo pozvolným přírodním procesem, který způsobují děje probíhající uvnitř nebo vně Země, vlivem rozdílů teplot nebo jiných faktorů. Rozsah přírodních mimořádných událostí závisí na koncentraci lidí, průmyslu, dopravy, rizikových technologií a také na připravenosti obyvatel likvidovat následky a zabránit sekundárním jevům (hladomor, nákazy, požáry atd.).

Mezi přírodní mimořádné události patří povodně včetně tsunami, zemětřesení, velký sesuv půdy, laviny, sopečný výbuch, atmosférické poruchy (vichřice, tajfuny, uragány, orkány, tornáda), rozsáhlé mrazy, sucha, pád meteoritu a velký lesní požár, epifytie, epizootie, epidemie, přemnožení přírodních škůdců, parazité, přemnožení plevelů aj.

5.2.2 Antropogenní mimořádné události

Antropogenní mimořádné události způsobuje vždy člověk svou činností nebo prostřednictvím strojů, staveb apod. Tyto mimořádné události jsou způsobené buď záměrně (války, teroristické akce, žhářství) nebo neopatrností. Narůstající vědeckotechnický pokrok zvyšuje rizika všech těchto katastrof a v současné době zahrnují skoro 70 % všech katastrof. Antropogenní katastrofy jsou obvykle dlouhodobé v porovnání s přírodními katastrofami. **[*37*]**

Technogenní mimořádné události zahrnují radiační havárie velkého rozsahu, technologické havárie spojené s únikem nebezpečných látek, ropné havárie, rozsáhlé dopravní havárie, důlní neštěstí aj. Do agrogenních MU patří eroze půdy, nevhodné používání hnojiv, agrochemikálií, vysychání a znehodnocování vodních zdrojů aj. Sociogenní lze ještě rozdělit na vnitřní, kam řadíme narušení finančního hospodářství státu, narušení dodávek ropy, elektrické energie, plynu, tepla, potravin, pitné vody apod., a vnější, mezi které patří vojenské MU.

5.3 Mimořádné události ohrožující kritickou infrastrukturu v České republice

K nejvýznamnějším poruchám kritické infrastruktury dochází vlivem nepříznivého působení sil a jevů, které mají nejen zemský původ ale také kosmický původ, např. dočasné vyřazení satelitních systému v důsledku slunečních erupcí nebo jiných zdrojů kosmického záření. Dopady takovýchto jevů tvoří celé řetězce příčin a následků, které v daném místě závisí na velikosti iniciačního jevu a zranitelnosti daného prvku kritické infrastruktury. **[*39*]**

Závažnější rizika pro kritickou infrastrukturu v České republice představují jak přírodní katastrofy, tak i selhání techniky a technologických postupů a také vliv člověka.

Z přírodních pohrom můžeme jmenovat přirozené a zvláštní povodně, vichřice, orkány a dokonce byla zaznamenána i tornáda, sesuvy půdy, bahnotoky a laviny, sněhové kalamity, krupobití, dlouhá období sucha, dlouhotrvající tropické teploty, požáry, lesní požáry, zemětřesení, epidemie, epizootie a epifytie.

Mezi technogenní mimořádné události můžeme zařadit především průmyslové havárie a nehody související s přepravou nebezpečných látek a škodlivin.

V současné době nabývají na významu také rizika úmyslně způsobená lidmi. Může se jednat jak o jednotlivce, tak o menší skupiny osob, kteří z důvodu nedbalosti, nemoci nebo nízkých pohnutek mohou významně poškodit některé prvky kritické infrastruktury. Je nutné počítat také s napadením kritické infrastruktury v rámci teroristického útoku. **[*39*]**

Závažnější poruchy kritické infrastruktury mohou mít vliv na další pohromy a negativně ovlivnit obyvatelstvo a životní prostředí. Také může dojít k závažným poruchám kritické infrastruktury jako důsledek jiné pohromy. V takovém případě dojde k zhoršení podmínek pro provádění záchranných a likvidačních následků původní pohromy a může to vést k jejímu vystupňování až po závažné ohrožení obyvatelstva a životní prostředí.

V České republice není závazné rozdělení mimořádných událostí, a proto se tyto události rozdělují ve většině případů podle původu právě na přírodní a antropogenní. Definovány jsou obecně mimořádná událost a krizová situace, se kterou souvisí typové plány obsahující základní, obecné postupy k řešení jednotlivých krizových situací.

Česká republika, EU i NATO řeší pohromy a katastrofy v souvislosti s jejich dopadem porušení kritické infrastruktury. Zlepšení ochrany obyvatelstva, majetku a životního prostředí lze dosáhnout třemi základními způsoby: **[*39*]**

- *Zvýšit odolnost všech prvků kritické infrastruktury.*
- *Zabezpečit důsledné ochrany jednotlivých prvků kritické infrastruktury.*
- *Lepší využití a zlepšení již plánovaných úkolů a opatření k zabezpečení ochrany obyvatelstva.*

6 BEZPEČNOST A OCHRANA KRITICKÉ INFRASTRUKTURY V ČESKÉ REPUBLICE

6.1 Legislativa v oblasti ochrany kritické infrastruktury

V České republice zatím není schválen žádný zákon, který by pojem kritická infrastruktura a problematiku její ochrany upravoval. Pro ochranu KI byla ale již učiněna řada kroků, jako deklarování základních funkcí státu za krizových situací a možností jejich zabezpečení nebo vytvoření přehledů národních, regionálních a lokálních subjektů KI. Dále se vyvíjejí aktivity ve výzkumu postupů k zachování funkčnosti jednotlivých oblastí kritické infrastruktury. Objevuje se otázka, zda převzít přístupy k ochraně KI ze zahraničí anebo si vytvořit vlastní. Hlavní roli má v každém případě stát, který má za povinnost chránit občany, majetek a životní prostředí a zároveň sám je zřizovatelem řady subjektů kritické infrastruktury. **[*40*]**

V problematice kritické infrastruktury lze využít nejlépe zákon č. 240/2000 Sb., o krizovém řízení (krizový zákon). Správním úřadům je tímto zákonem uloženo vést přehled možných zdrojů hrozeb a rizik, provádět analýzy ohrožení. V případě vzniku krizové situace pak musí odstraňovat zjištěné nedostatky, které by mohly vést ke vzniku krizových situací. Platí to i u subjektů kritické infrastruktury a snížení jejich zranitelnosti. Státní i soukromé subjekty jsou povinny na základě tohoto zákona přijmout opatření k zajištění především fyzické a informační bezpečnosti. **[*41*]**

Přehled některých dalších zákonů pro oblast kritické infrastruktury:

- *Zákon č.238/2000 Sb., o Hasičském záchranném sboru České republiky*
- *Zákon č. 239/2000 Sb. o integrovaném záchranném systému*
- *Zákon č. 241/2000 Sb., o hospodářských opatřeních pro krizové stavy a o změně některých souvisejících zákonů*
- *Zákon č. 189/1999 Sb., o nouzových zásobách ropy, o řešení stavů ropné nouze a o změně některých souvisejících zákonů*
- *Zákon č. 458/2000 Sb., o podmínkách podnikání a o výkonu státní správy v energetických odvětvích a o změně některých zákonů*
- *Zákon č. 406/2000 Sb., o hospodaření energií*
- *Zákon č. 12/2002 Sb., o státní pomoci při obnově území postiženého živelní nebo jinou pohromou*
- *Zákon č. 585/2004 Sb., o branné povinnosti a jejím zajišťování*
- *Zákon č. 20/1966 Sb., o péči zdraví lidu, ve znění pozdějších předpisů*
- *Zákon č. 21/1992 Sb., o bankách*
- *Zákon č. 6/1993 Sb., o České národní bance*

V blízké době se připravuje novela krizové zákona, která se zaměřuje právě na ochranu kritické infrastruktury. Cílem této novely je upravit vztahy a kompetence v oblasti krizového řízení na krajské a obecní úrovni. Definuje také odpovědnost za zpracování krizových plánů krajů a vymezuje zpracovatele krizového plánu obce s rozšířenou působností. Do zákona by měla být také zapracována směrnice Rady EU 2008/114/ES o určování a označování

evropských kritických infrastruktur a posuzování potřeby zvýšit jejich ochranu. Měla by také určovat práva a povinnosti subjektů KI, které budou muset na výzvu příslušného správního úřadu poskytnout informace nezbytné k určení prvků KI a prvků evropské KI. Mezi další povinnosti subjektů KI bude vypracování plánů krizové připravenosti, umožnění kontroly ze strany ministerstva či jiného správního úřadu a určení styčného bezpečnostního zaměstnance, který bude spolupracovat a komunikovat s příslušnými státními orgány.

6.1.1 Základní pojmy v oblasti kritické infrastruktury

Problematika kritické infrastruktury byla projednávána několikrát Bezpečnostní radou státu a v průběhu roku 2007 zde byly stanoveny následující pojmy týkající se této problematiky: **[*18*]**

Kritickou infrastrukturou se rozumí výrobní a nevýrobní systémy a služby, jejichž nefunkčnost by měla závažný dopad na bezpečnost státu, ekonomiky, veřejnou správu a zabezpečení základních životních potřeb obyvatelstva dalších oblasti nezbytné pro zachování základních funkcí státu.

Ochrana kritické infrastruktury je proces, který při zohlednění všech rizik a hrozeb směřuje k zajištění fungování subjektů kritické infrastruktury a vazeb mezi nimi.

Subjekty kritické infrastruktury jsou vlastníci a provozovatelé výrobních a nevýrobních systémů vytvářející produkty nebo poskytující služby kritické infrastruktury.

Objekt kritické infrastruktury jsou vybrané stavby a zařízení veřejné infrastruktury a další prvky, které vlastní nebo provozují subjekty kritické infrastruktury.

6.1.2 Bezpečnostní strategie ČR

Bezpečnostní strategie České republiky vychází ze závěrů Bezpečnostních strategií jak v EU, tak také NATO. Bezpečnostní strategie **[*42*]** je charakterizovaná jako soubor základních zásad, hodnot, omezení a předpokladů vytvořených k řízení činností, jimiž bude dosahováno plnění hlavních bezpečnostních cílů. Stanovuje priority a určuje vhodné proporce mezi svými jednotlivými součástmi a stanovuje jejich místo a úlohu při plnění cílů. Vypracovává metody využívání politických, ekonomických, duchovních a vojenských zdrojů země při zabezpečování cílů státní politiky za všech okolností, v míru i za války.

Vnitřní bezpečnost je ovlivňována řadou hrozeb a rizik, jejichž úroveň se pravidelně posuzuje a následně promítá do úkolů příslušných složek. V oblasti hrozeb a rizik přetrvávají a v mnoha případech se i zvyšující bezpečnostní rizika nevojenského charakteru jako jsou náboženské a etnické konflikty nebo hospodářské problémy, dále zneužití nebezpečných látek, přírodní a průmyslové katastrofy, organizovaný zločin, narušení pořádku a majetku občanů, narušení informačních a řídicích systémů. Aktuální jsou i hrozby teroristického útoku. Bezpečnostní hrozbu představují také státy, nevládní skupiny a organizace, které nerespektují principy mezinárodního práva a demokracie a dopouštějí se násilí. Vysoce nepravděpodobná je konvenční agrese proti ČR i NATO, nelze ji však vyloučit. **[*42*]**

Uvedené hrozby jsou jedny ze základních podkladů pro krizové plánování a počítá se s nimi při plánování ochrany KI.

Otázkou bezpečnosti se zabývá také Bezpečnostní informační služba (BIS), která představuje vnitřní zpravodajskou službu. Tato instituce získává, shromažďuje a vyhodnocuje závažné informace důležité pro bezpečnost, ochranu ústavního zřízení a významných ekonomických zájmů republiky.

6.1.3 Krizové plánování

Krizové plánování **[*43*]** v ČR je nástrojem krizového řízení a je souhrnem plánovacích činností, procedur a vazeb uskutečňovaných orgány krizového řízení a jimi určenými státními nebo veřejnými institucemi, právnickými nebo podnikajícími osobami k realizaci cílů a úkolů při zajišťování bezpečnosti státu a jeho obyvatelstva za krizových situací. Podle zákona č. 240/2000 Sb., o krizovém řízení se krizové plánování soustřeďuje na proces zpracování, aktualizace a ověřování krizových plánů a dokumentů, které s nimi souvisí.

Cílem krizového plánování je zajistit připravenost daného území a organizaci na řešení krizových situací, předcházet krizovým situacím a omezit jejich účinky, upravit proces předávání a poskytování informací, zjistit a zabezpečit potřeby pro realizaci vlastních krizových opatření a poskytování pomoci vyžádané jinými organizacemi.

V plánovacím procesu existují čtyři základní prvky jeho prospěšnosti: koordinování plánovacího úsilí (specifikace cílů), příprava možností změn plánu, stanovení měřitelných kritérií, vytváření podmínek pro rozvoj manažerů.

Při plánování musíme vzít v úvahu chování člověka postiženého mimořádnou událostí a také sociální dopady. Tyto přístupy respektujeme při plánování ochrany kritické infrastruktury.

Plánování ochrany kritické infrastruktury prochází několika etapami: **[*44*]**

- *Identifikace problému (identifikace hrozeb, příčin, analýza rizik, přijetí zmírňujících příčin).*
- *Analýza zranitelnosti (skryté příčiny, nebezpečné podmínky apod.) a transfer technologií. Zranitelnost můžeme určit jako fyzickou, demografickou, sociální, psychologickou, ekonomickou, organizační.*
- *Určení záměrů a cílů.*
- *Vyhodnocení zranitelnosti.*
- *Příprava a návrh postupů (preventivní opatření k ochraně obyvatelstva a jejich majetku na základě závěrů z analýz možných rizik bezpečnostních hrozeb, návrh strategií).*
- *Zpracování vlastního dokumentu a jeho přijetí (příprava plánovací dokumentace pro zvládání MU nebo krizových situací).*
- *Stanovení zásad pro přípravu a využití disponibilních sil, prostředků a zdrojů při řešení MU nebo krizových situací.*

- *Stanovení úkolů pro zajištění funkcí státu při MU, vymezení kompetencí jednotlivých složek krizového řízení a stanovení zásad jejich kooperace.*
- *Vytvoření organizační struktury bezpečnostního systému na jednotlivých stupních řízení.*
- *Sledování jeho účinnosti a vyhodnocování (návrhy na korekce plánu).*

6.2 Bezpečnost a ochrana kritické infrastruktury v České republice na základě literární rešerše

Bezpečnost kritické infrastruktury je soubor opatření, který při zohlednění povahy kritické infrastruktury a všech možných rizik i hrozeb směřuje k zajištění fungování prvků, vazeb a toků kritické infrastruktury tak, aby za žádných okolností nedošlo k jejich úplnému selhání. **[*29*]**

Pokud by došlo k nefunkčnosti kritické infrastruktury, vyvolalo by to ve většině případů situaci srovnatelnou s mimořádnou událostí nebo dokonce krizovou situací. **[*20*]** Může tak dojít k ohrožení obyvatelstva, jeho majetku, zdraví nebo životům. Proto by se ochranou kritické infrastruktury měl zabývat v první řadě stát (veřejná správa) a jeho výkonné složky jako je policie a jí podobné složky, které mají na starosti převážně fyzickou ochranou KI. Tyto složky mají za úkol zabránit těm příčinám, které mohou vést k selhání KI. V případě selhání KI pak mají za úkol především usměrnit činnosti tak, aby nedošlo k panice a ke zbytečným ztrátám na životech a zdraví lidí a majetku, k narušení bezpečí lidí tzn., že je třeba rozpracovat činnosti v rámci příslušných plánů kontinuity veřejné správy a krizových plánů spojených s KI. **[*45*]**

Zásadní roli v ČR v oblasti připravenosti zvládnutí selhání KI a zvládání dopadů selhání KI mají hasiči, kteří jsou dle mezinárodních pravidel cvičeni jako výkonná složka, na kterou se spoléhá, že má materiálně technické vybavení i připravenost takovou, že dokáže vytvořit základ odezvy státu v území na vzniklou situaci, což se od roku 2000 několikrát osvědčilo. Na selhání KI se však musí ještě důkladně připravit. **[*45*]**

Orgány veřejné správy by měly v oblasti ochrany KI tvořit a sjednocovat metodické a plánovací postupy k ochraně KI a organizovat potřebná opatření. **[*46*]** Úkolem veřejné správy by mělo být prosazování národní a mezinárodní politiky, zpracování potřebné legislativy a nařízení, výměna informací s mezinárodními organizacemi, včetně vlád a soukromým sektorem, hodnocení hrozeb a zranitelnosti, opatření krizového plánování a řízení, stanovení finančního zatížení pro soukromý sektor. **[*20*]**

Protože jsou jednotlivé oblasti kritické infrastruktury mezi sebou provázány a většina prvků kritické infrastruktury patří soukromým vlastníkům, je důležité sdílení informací mezi veřejnou správou a soukromým sektorem. Většina publikací a článků se otázkou spolupráce mezi privátním a státním sektorem a bezpečným sdílením informací zabývá. Veřejná správa je v postavení, kdy musí najít způsob, jak motivovat podnikatelský sektor k tomu, aby investoval do bezpečnosti. Podnikatelské subjekty se totiž otázkou bezpečnosti moc nezaobírají, neboť jim jde v první řadě o zisk než o bezpečnost. Je nutné nalézt tedy způsob

společných investic státu se soukromým sektorem a politický konsenzus k nutným legislativním změnám. **[*47*]**

Otázka způsobu sdílení informací je důležitá také mezi jednotlivými složkami IZS, neboť jsou předurčeny k prvotnímu represivnímu zásahu vedoucí k eliminaci vlivů působící MU. Je tedy nutné zabezpečit sdílení informací mezi státem, krajem, obce s rozšířenou působností a obcí, ale také dotčenými složkami IZS a dotčenou podnikatelskou sférou.

Příkladem spolupráce mezi veřejnou správou a vlastníky (provozovateli) KI na strategické úrovni může být Nový Zéland, kde v každé důležité lokalitě existují smíšení týmy (veřejná správa a vlastník KI) zabývající se ochranou KI z hlediska tzv. život podporujících funkcí, a v nichž veřejná správa hraje roli zasvěceného supervizora. **[*7*]**

Problémy ochrany KI jsou mnohaoborové (technické, manažerské či organizační oblasti na různých úrovních), kvůli rozmanitosti systémů KI. Procesní model pro ochranu kritické infrastruktury a technologií je proto založen na principech, metodách a postupech rizikového inženýrství. Hodnotí se všechny relevantní pohromy – tzv. „all hazard approach“ **[*45*]**, tj. používají se postupy:

- *Hodnocení ohrožení (hazard assessment)*
- *Hodnocení rizika (risk assessment)*
- *Řízení rizik (risk management)*
- *Řízení bezpečnosti (safety management)*

Pro strategický přístup k bezpečnosti kritické infrastruktury a její ochranu platí, že nic není absolutně bezpečné. Prvky i sítě KI mohou také dříve nebo později selhat. **[*23*]** Proto je nutné účinné a efektivní řízení bezpečnosti území, které se musí opírat o současné znalosti a jejich správná vyhodnocení v souvislostech, která platí v daném území.

Základní roli v ochraně kritické infrastruktury má výzkum, který v současné době řeší vnitřní propojení (vzájemnou závislost) mezi infrastrukturami, postupy a cíle ochrany KI z manažerského pohledu na úrovni státu, možné rozdělení úkolů ochrany KI mezi veřejný a privátní sektor, nároky na řídící personál vlastníků KI a technologií a obecný rámec pro bezpečnost KI. **[*45*]**

Většina odborných publikací také klade důraz na vzdělanost úředníků, kteří se tématem kritické infrastruktury zabývají a to jak v soukromém tak veřejném sektoru. Je důležité zajistit jim i vhodný praktický trénink pro zvládání krizových situací a tedy podporovat a financovat vědu i v této oblasti. Podle **[*46*]** by se příslušné informace o ochraně KI měli dostat také k obyvatelstvu, které by si mělo vytvořit návyky k sebeochraně a soběstačnosti v případě nefunkčnosti kritické infrastruktury.

Často je zmiňována potřeba nové legislativy v oblasti ochrany KI. Některé zákony (zejména krizový zákon) již umožňují v této oblasti nějaké zabezpečení vykonávat. Podle článku **[*46*]** by bylo nutné uvažovat o právní úpravě spíše v souvislosti s finanční účastí státu na udržování funkčnosti kritické infrastruktury. Velkým problémem jsou vlastníci a provozovatelé, kteří se

zvyšováním bezpečnosti příliš nezaobírají, navíc z důvodu konkurenčního postavení ani nejsou ochotni odkrýt zranitelnost svých podniků. Je tudíž potřeba vytvořit partnerství mezi veřejným a soukromým sektorem.

Do řízení veřejných věcí by mělo být zavedeno procesní řízení, které se opírá o řízení znalostí, je proaktivní a systémové. Pro rychlou odezvu na selhání infrastruktury a na rychlou obnovu její činnosti je potřeba vytvořit a procvičovat programy na zajištění připravenosti pro rychlou odezvu. **[*29*]**

Různé materiály z oblasti ochrany KI navrhují řešení na konkrétní situace zejména v oblasti energetiky, např. hledáním reakce na blackout. Podle článku **[*47*]** by se měly rozebírat všechny systémy současně nebo alespoň ty, které se mohou vzájemně ovlivňovat a kdy výpadek jednoho způsobí kolaps druhého. Je ale velmi obtížné shromáždit všechny potřebné informace pro sestavení modelu zachycujícího všechny takto provázané systémy.

Odborné publikace ukazují, že problematika ochrany kritické infrastruktury je komplexním problémem. Základní koncept ochrany musí vycházet z územního plánování a z činností na něho navazujících. Jelikož stávající kritickou infrastrukturu nelze jedním mávnutím vyřadit a nahradit ji moderní, která by splňovala všechny požadavky, existuje mnoho úkolů i na úseku odezvy. Důležité místo v této oblasti mají i následující dokumenty: **[*45*]**

- *Speciální plány odezvy pro KI, které zpracovává vlastník či provozovatel KI.*
- *Plány kontinuity ze strany vlastníka či provozovatele KI, které zajišťují přežití, minimální funkčnost KI pro splnění nároků území, jehož obslužnost závisí na této infrastruktuře.*
- *Plány kontinuity ze strany správce území a ochránce veřejného blaha a veřejných zájmů, kterým je veřejná správa, která zajišťuje bezpečnost a rozvoj území.*
- *Krizové plány ze strany vlastníka či provozovatele KI, které zajistí přežití jeho podnikání a nevyvolají nepřijatelné dopady na základní chráněné zájmy.*

6.2.1 Financování ochrany kritické infrastruktury

Ke zvýšení ochrany objektů kritické infrastruktury budou nutné značné finanční prostředky. Zejména v oblasti zvyšování odolnosti objektů proti působení rizik a zálohování prioritních částí kritické infrastruktury, včetně využití zálohování a rozmístění záloh v území.

Určitou možnost financování by mohla přinést legislativní úprava v souvislosti s ochranou kritické infrastruktury obdobně, jako při finančním zabezpečení krizových opatření obsažených v krizovém zákoně. Je zde ale také možnost využít finanční zdroje z EU. Od roku 2007 do roku 2013 bude financování oblasti kritické infrastruktury probíhat prostřednictvím rámcového programu Bezpečnost a ochrana svobod **[*20*]**, který obsahuje program Prevence, připravenost k obraně proti terorismu a zvládání jeho následků. Program by měl umožnit komunitární financování projektů, které předloží národní, regionální a místní orgány.

Další možnost se nabízí ve využití příspěvků EU na financování aktivit na podporu prevence, tj. připravenost a reakce na teroristické útoky, kde přes dvě třetiny financí bude věnováno na přípravu Evropského programu ochrany kritické infrastruktury. **[*20*]**

6.2.2 Vlastní pohled na bezpečnost a ochranu kritické infrastruktury

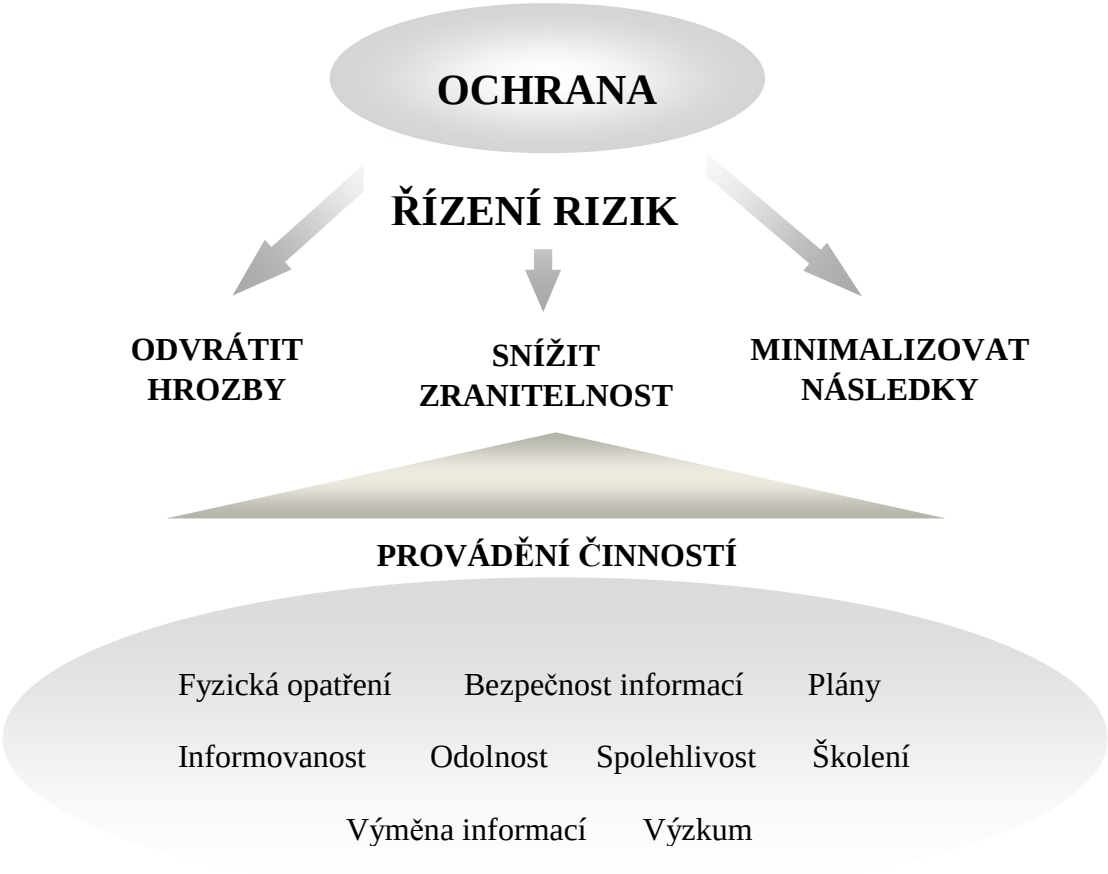
Pro Českou republiku je dle mého názoru jedním z nejdůležitějších sektorů kritické infrastruktury energetika a informační systémy. Elektřina je základem fungování dnešní společnosti a je nezbytná pro fungování dalších sektorů. Lze ji ale zabezpečit záložními zdroji, které však při dlouhodobějším výpadku mohou dojít nebo kvůli dalšímu kolapsu vypadnout. Ztrátu klíčových informací ale nahradit nelze. Informační systémy mohou být snadno zneužitelné pro trestnou činnost. Proto je třeba klást důraz na jejich bezpečnost. S tím souvisí také zabezpečení sdílení informací mezi státním a soukromým sektorem.

Bezpečností a ochranou kritické infrastruktury by se měl zabývat v první řadě stát, neboť má přístup k informacím, může vydávat legislativní nařízení, zpracovává plány a také vlastní některá zařízení kritické infrastruktury. Dalším subjektem, který by se měl podílet na ochraně KI je soukromý sektor, který vlastní velkou část zařízení kritické infrastruktury. V neposlední řadě by se na ochraně kritické infrastruktuře mělo podílet také obyvatelstvo, které by mělo dostávat příslušné informace o ochraně KI a mělo by být připraveno na případné omezení nebo výpadky některých prvků KI.

Jedním ze základních úkolů státu je zajistit bezpečnost obyvatelstva, majetku a životního prostředí, což stát zabezpečuje prostřednictvím příslušných zákonů, státních složek a finančních prostředků. Středem zájmu veřejného sektoru je tedy lidská bezpečnost a funkčnost jednotlivých odvětví KI. Velkou část objektů a zařízení KI ale vlastní soukromé podniky, kterým jde v první řadě o zisk než o bezpečnost. Stát může vydat legislativní opatření k dodržování určitého stupně ochrany, ale může tyto subjekty také motivovat, nejlépe prostřednictvím peněz, neboť ty hrají v této oblasti nejdůležitější roli. Příkladnou motivací by podle mého názoru bylo rozdělení bezpečnosti podniků do čtyř stupňů. Při splnění prvních dvou stupňů zabezpečení vyplývajících ze zákona by subjekty žádné výhody nedostávaly, pokud by ale plnily dobrovolně vyšší než státem dané bezpečnostní opatření a aktivně se na něm podílely, poskytoval by jim stát daňové úlevy a dotace.

V oblasti ochrany kritické infrastruktury je důležité monitorování základních zařízení nebo zavedení systémů proti poškození. Pro většinu prvků kritické infrastruktury jsou vytvořeny typové plány pro různé druhy nebezpečí. V současně době mají také subjekty KI ze zákona povinnosti zpracovat Plány krizové připravenosti, aby byly schopny zabezpečit svoji funkčnost. Je nutná také příprava specialistů v rámci KI a výměna odborných poznatků a zejména zkušeností na mezinárodní úrovni. Vzdělávat by se mělo také obyvatelstvo, aby bylo v případě výpadku KI soběstačné. Měla by být zpracována jasná, jednoduchá a srozumitelná metodika k plánům k ochraně jednotlivých prvků KI, aby tyto plány nebyly moc rozsáhlé a byly srozumitelné.

Ne všechny objekty a zařízení KI lze chránit před všemi hrozbami, např. rozvodné sítě elektrické energie, které jsou příliš rozsáhlé. Proto se v této oblasti uplatňuje řízení rizik, které se soustřeďuje na oblasti největšího rizika. Zahrnuje tři činnosti – odvrácení hrozeb, snížení zranitelnosti a minimalizování následků (obr. 2). Ochranu KI je potom potřeba provádět prostřednictvím zvýšení bezpečnosti informací, fyzických opatření, vytváření plánů, informovaností, zvýšení spolehlivosti a odolnosti systémů, výměny informací mezi subjekty KI a vzdělaných pracovníků a především zvyšováním aktivity v oblasti výzkumu, který by se měl zaměřit na kritickou infrastrukturu jako celek a zkoumat vzájemnou závislost těch prvků KI, které mohou zapříčinit nefunkčnost dalších zařízení KI.



Obrázek 2 Ochrana kritické infrastruktury podle **[*48*]**

V oblasti bezpečnosti a ochrany kritické infrastruktury jsou nejdůležitější preventivní opatření, protože dokážou eliminovat velkou část vážných dopadů pohrom. Tyto opatření jsou zaměřeny buď na odstranění či snížení rizika nebo na přenesení této hrozby na jinou organizaci, např. pojišťovnu. Pro zajištění bezpečnosti je důležité prosazovat spolupráci a vzájemné sdílení informací, zvyšovat informovanost v daném území o možných rizicích,

koncepcích, ochraně a postupech a také jsou nutné legislativní úpravy. Jednotlivé subjekty KI by měli mít vypracované seznamy možných hrozeb popisující jejich obecnou povahu, intenzitu, délku, možné důsledky a na základě tohoto seznamu vytvořit možné scénáře vývoje dané hrozby vždy v nejhůře možném dopadu. Tyto scénáře je pak nutné pravidelně kontrolovat a aktualizovat.

7 ZÁVĚR

Ve své bakalářské práci jsem popsala historii a vývoj kritické infrastruktury v USA, Evropské unii a v České republice. Charakterizovala jsem základní prvky kritické infrastruktury a možné mimořádné události, které je mohou ohrožovat. Jsou zde uvedeny také opatření, která jsou nutná ke zvýšení ochrany kritické infrastruktury. Základem jsou preventivní opatření, tedy předcházení nebezpečným situacím, které mohou v důsledku mimořádných událostí nastat. Pokud už toto nebezpečí nastane, je důležité být připraven a mít k dispozici plány k řešení takové situace.

V oblasti ochrany kritické infrastruktury bude důležité vytvoření správné legislativy, na které se v současné době intenzivně pracuje. Souvisí s tím změna krizového zákona a také vydání Komplexní strategie ČR k řešení problematiky kritické infrastruktury, jejíž součástí by měl být Národní program ochrany kritické infrastruktury.

Problematika kritické infrastruktury je obtížným a dlouhotrvajícím úkolem, která z hlediska bezpečnosti státu nabývá stále většího významu především proto, že ochrana kritické infrastruktury vytváří podmínky pro zvládání mimořádných událostí a krizových situací.

SEZNAM POUŽITÝCH ZDROJŮ

[1] http://www.justice.gov/criminal/cybercrime/critinfr.htm

[2] LINHART, Petr; RICHTER, Rostislav. Ochrana kritické infrastruktury [on-line]. *112 – odborný časopis požární ochrany integrovaného záchranného systému a ochrany obyvatelstva.* 2003. Dostupný z http://www.hzscr.cz/soubory/casopis_112_rok_2003.pdf

[3] Patriot Act. K dispozici na http://epic.org/privacy/terrorism/hr3162.html

[4] The National Strategy for Homeland Security. K dispozici na www.dhs.gov/xlibrary/assets/nat_strat_hls.pdf

[5] ŠENOVSKÝ, Pavel. Stav řešení kritické infrastruktury na území USA [online]. VŠB-TU. Ostrava 2008, 2. vyd., 71 s. Dostupný z homen.vsb.cz/~sen76/publikace/ki_v2.7z

[6] History of National Infrastructure Protection Plan. Dostupné z http://www.semp.us/publications/biot_reader.php?BiotID=594

[7] MOZGA, J., VÍTEK M., KOVAŘÍK F., Kritická infrastruktura společnosti., Hradec Králové: Gaudeamus, 2008, 1. vydání, 156 s.

[8] Sděleni Komise Radě a Evropskému parlamentu. Ochrana kritické infrastruktury při boji proti terorismu. Brusel, 2004.

[9] Komise Evropských společenství. Zelená kniha o Evropském programu na ochranu kritické infrastruktury. Brusel, 2005

[10] The European Programme for Critical Infrastructure Protection (EPCIP), Brusel 2006, MEMO/06/477

[11] Council Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Brusel, 2008

[12] http://ec.europa.eu/ceskarepublika/press/press_releases/10241_cs.htm

[13] Program bezpečnostního výzkumu ČR 2010-2015, Ministerstvo vnitra ČR, Praha 2008

[14] Usnesení BRS č. 204/2001 k Informacím ke zpracování definice a stanovení rozsahu základních funkcí státu za krizových situací

[15] DRYMLOVA, Veronika. Plán znovuobnovení kritické infrastruktury na místní úrovni [Diplomová práce]. České Budějovice: JU, 2008. 324 s. Dostupné z http://theses.cz/id/g1sgqv

[16] HORÁK, R. SALIGER, T. NAVRÁTIL J. Řešení kritické infrastruktury s možností využití nástrojů EU. In *Ochrana obyvatelstva 2007 – Ochrana kritické infrastruktury*. Ostrava: VŠB - Technická Univerzita Ostrava, Fakulta Bezpečnostního inženýrství, 2007. 456 s.

[17] Usnesení VCPN č. 222/2006 ke Zprávě o stavu řešení problematiky kritické infrastruktury

[18] Usnesení BRS č. 30/2007 ke Zprávě o řešení problematiky kritické infrastruktury v České republice

[19] ŘÍHA J. Kritická infrastruktura a riziko mimořádné události. *Urbanismus a územní rozvoj*. 2007, roč. 10, č. 4. Dostupný z http://www.uur.cz/images/publikace/uur/2007/2007-04/08_kriticka.pdf

[20] MARTÍNEK, B. Východiska a principy zajištění ochrany kritické infrastruktury v České republice. *112 – odborný časopis požární ochrany, integrovaného záchranného systému a ochrany obyvatelstva.* 2008, č. 4.
Dostupné z http://web.mvcr.cz/archiv2008/casopisy/112/2008/duben/strana_22.html

[21] STEIN W., HAMMERLI B., POHL H., POSCH R. P. Critical Infrastructure Protection – Status and Perspectives. Workshop on CIP, Frankfurt am Main, www.informatik2003.de

[22] PROCHÁZKOVÁ D., BALOG K. Bezpečnost systému systémů. In: *Environmentálne aspekty požiarov a havárií*. Trnava 2008. ISBN 978–80–8096–052–0,

[23] PROCHÁZKOVÁ, D. Bezpečnost kritické infrastruktury z pohledu bezpečnosti systému systémů. In *Crisis management: Ochrana obyvatelstva*. Brno: Univerzita obrany, 2008. s. 435

[24] www.bizmanual.com

[25] PROCHÁZKOVÁ D. Kritická infrastruktura a její problémy. Ostrava: VŠB a SPBI, 2008, 77 s. ISBN 978-80-7385-034-0.

[26] BENEŠ I. Energetika a geopolitika - Důvody k zodolnění zásobování elektřinou. In *Ochrana obyvatelstva 2009*. Ostrava: VŠB - Technická Univerzita Ostrava, Fakulta Bezpečnostního inženýrství, 2009. s. 349.

[27] *Asociace pro mezinárodní otázky* [online]. 2009 [cit. 2010-04-24]. Bruselský rybář v Kaspickém moři & plynová bezpečnost ČR. Dostupné z WWW: http://www.amo.cz/publikace/bruselsky-rybar-v-kaspickem-mori--plynova-bezpecnost-cr.html

[28] LINHART, P. BEČIČKOVÁ, M. Některé otázky ropné bezpečnosti v České republice. In *Ochrana obyvatel 2007 : Ochrana kritické infrastruktury*. Ostrava: VŠB - Technická Univerzita Ostrava, Fakulta Bezpečnostního inženýrství, 2007. s. 456.

[29] Kolektiv autorů. Zranitelnost kritické infrastruktury. Ostrava: Sdružení požárního a bezpečnostního inženýrství 2008, 102 s.

[30] *EAGRI* [online]. 2003 [cit. 2010-04-21]. Koncepce zabezpečení obyvatelstva pitnou vodou za krizových situací. Dostupné z: <http://eagri.cz/public/eagri/voda/zabezpeceni-pitne-vody-za-krizovych/koncepce-zabezpeceni-obyvatelstva-pitnou.html>.

[31] GRÁF, Ladislav Systém rychlého varování pro potraviny a krmiva. In *Crisis management: Ochrana obyvatelstva*. Brno: Univerzita obrany, 2008. s. 440

[32] *Zdravotnická záchranná služba Královéhradeckého kraje* [online]. 2007 [cit. 2010-04-22]. Přednemocniční péče. Dostupné z WWW: <http://www.zzskhk.cz/prednemocnicni-pece.html>.

[33] BEDNÁŘ, Kamil Ochrana a rozvoj dopravní infrastruktury. In *Crisis management: Bezpečnost - Připravenost - Ochrana obyvatelstva*. Brno: Univerzita obrany, 2006. s. 356

[34] Usnesení vlády č. 882/2005: Dopravní politika České republiky na léta 2005-2013. K dispozici: http://www.mdcr.cz/cs/Strategie/Dopravni_politika/Dopravni_politika.htm

[35] KOVÁŘÍK, František Kritická infrastruktura a Hasičský záchranný sbor ČR. In *Ochrana obyvatel 2007: Ochrana kritické infrastruktury*. Ostrava: VŠB - Technická Univerzita Ostrava, Fakulta Bezpečnostního inženýrství, 2007. s. 456.

[36] ŠTĚTINA, J. a spol.: Medicína katastrof a hromadných neštěstí, 1. vyd. Praha: Grada Publishing s.r.o., 2000, 421 s

[37] ADAMEC V. ŠENOVSKÝ M, ŠENOVSKÝ P. Ochrana kritické infrastruktury. 1. vyd. Ostrava: Sdružení požárního a bezpečnostního inženýrství, 2007, 141 s.

[38] SZCZYPKA P. Population Protection Against Sociogenic Threats. In *Ochrana obyvatelstva 2008*. Ostrava: VŠB - Technická Univerzita Ostrava, Fakulta Bezpečnostního inženýrství, 2008. s. 413.

[39] KOVAŘÍK, Jaroslav Kritická infrastruktura a ochrana obyvatelstva. In *Ochrana obyvatel 2007: Ochrana kritické infrastruktury*. Ostrava: VŠB - Technická Univerzita Ostrava, Fakulta Bezpečnostního inženýrství, 2007. s. 456

[40] NITRA J. Ochrana kritické infrastruktury. *112 – odborný časopis požární ochrany integrovaného záchranného systému a ochrany obyvatelstva 2007.*

[41] Lukáš, L. Kritická infrastruktura České republiky. In: Sborník 9. mezinárodní konference Internet a bezpečnost, Zlín 20. března 2007, ISBN 978-80-7318-548-0

[42] Usnesení vlády ČR č. 1253/2003. Bezpečnostní strategie České republiky. Praha 2003

[43] Usnesení bezpečnostní rady státu č. 87/2000 Sb., k obecným zásadám krizového plánování. Praha 2000

[44] HORÁK Rudolf. Bezpečnostní východiska pro ochranu kritické infrastruktury

[45] PROCHÁZKOVÁ, Dana Procesní model pro ochranu kritické infrastruktury. In *Ochrana obyvatel 2007: Ochrana kritické infrastruktury*. Ostrava: VŠB - Technická Univerzita Ostrava, Fakulta Bezpečnostního inženýrství, 2007. s. 456.

[46] ADAMEC, Vilém Ochrana kritické infrastruktury v ČR. In *Crisis management: Ochrana obyvatelstva*. Brno: Univerzita obrany, 2006. s. 356.

[47] ŠENOVSKÝ, Michail; ŠENOVSKÝ, Pavel Strategie ochrany kritické infrastruktury. In *Ochrana obyvatelstva 2008*. Ostrava: VŠB - Technická Univerzita Ostrava, Fakulta Bezpečnostního inženýrství, 2008. s. 413.

[48] National Infrastructure Protection Plan: Partnering to enhance protection and resiliency, 2009

SEZNAM PŘÍLOH

PŘÍLOHY

Příloha 1 Přehled prvků kritické infrastruktury v EU **[*9*]**

	Sektor	**Produkt nebo služba**
I	Energie	1 Produkce ropy a plynu, úprava, zacházení a skladování včetně produktovodů 2 Výroba elektřiny 3 Přeprava elektřiny, plynu a ropy 4 Distribuce elektřiny, plynu a ropy
II	Informační, telekomunikační technologie, ICT	5 Ochrana informačních systémů a sítí 6 Použití nástrojů automatizačních a kontrolních systémů (SCADA = Systém kontroly a sběru dat atd.) 7 Internet 8 Zabezpečení pevných telekomunikací 9 Zabezpečení mobilních telekomunikací 10 Radiová komunikace a navigace 11 Satelitní komunikace 12 TV vysílání
III	Pitná voda	13 Zajištění pitné vody 14 Kontrola kvality vody 15 Zachycování a kontrola objemu vody
IV	Potraviny	16 Zajištění potravin a zabezpečení jejich nezávadnosti a bezpečnost
V	Zdraví	17 První pomoc a lékařská pomoc 18 Léky, séra, vakcíny a léčiva 19 Bio-laboratoře a bio-agens
VI	Finanční	20 Platební služby/struktura plateb (soukromé) 21 Systém převodů veřejných financí
VII	Veřejný a legislativní pořádek a bezpečnost	22 Udržování veřejného a legislativního pořádku, bezpečí a bezpečnosti 23 Soudní správa a vazba
VIII	Civilní správa	24 Vládní funkce
		25 Ozbrojené složky
		26 Státní správa
		27 Nouzové služby
		28 Poštovní a kurýrní služby
IX	Doprava	29 Silniční doprava 30 Železniční doprava 31 Letecká doprav 32 Říční doprava 33 Námořní doprava

X	Chemický a jaderný průmysl	34 Doprava, výroba a skladování/nakládání s chemickými a jadernými látkami 35 Doprava všech typů včetně produktovodů pro nebezpečné výrobky (chemické a jaderné látky)
XI	Vesmír a výzkum	36 Vesmír 37 Výzkum

Příloha 2 Přehled prvků kritické infrastruktury v ČR **[*18*]**

Poř.	**Oblast KI**	**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	Potravinářství 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. Výroba, skladování a distribuce léčiv a zdravotnických prostředků
5	Doprava	5.1. Silniční
		5.2. Železniční
		5.3. Letecká
		5.4. Vnitrozemská vodní
6	Komunikační a informační systémy	6.1. Služby pevných telekomunikačních sítí
		6.2. Služby mobilních telekomunikačních sítí
		6.3. Radiová komunikace a navigace
		6.4. Satelitní komunikace
		6.5. Televizní a radiové vysílání
		6.6. Poštovní a kurýrní služby
		6.7. Přístup k internetu a k datovým službám
7	Bankovní a finanční sektor	7.1. Správa veřejných financí
		7.2. Bankovnictví
		7.3. Pojišťovnictví
		7.4. Kapitálový trh
8	Nouzové služby	8.1. Hasičský záchranný sbor ČR a příslušné jednotky požární ochrany
		8.2. Policie ČR (vnitřní bezpečnost a veřejný pořádek)
		8.3. Armáda ČR (zabezpečení obrany)
		8.4. Radiační monitorování včetně podkladů pro rozhodování o opatření vedoucích ke snížení nebo odvrácení ozáření
		8.5. Předpovědní, varovná a hlásná služba

9	Veřejná správa	9.1. Státní správa a samospráva
		9.2. Sociální ochrana a zaměstnanost (sociální zabezpečení, státní sociální podpora, sociální pomoc)
		9.3. Výkon justice a vězeňství