Vysoká škola báňská - Technická univerzita Ostrava

Fakulta bezpečnostního inženýrství

Katedra požární ochrany a ochrany obyvatelstva

Kritická infrastruktura a její ochrana

Student:	**Bc. Zdeněk Svoboda**
Vedoucí diplomové práce:	**Ing. Danuše Kratochvílová**
Studijní obor:	**Bezpečnostní plánování**
Datum zadání diplomové práce:	**30. listopadu 2009**
Termín odevzdání diplomové práce:	**30. dubna 2010**

VŠB - Technická univerzita Ostrava
Fakulta bezpečnostního inženýrství
Katedra požární ochrany a ochrany obyvatelstva

Zadání diplomové práce

Student: **Bc. Zdeněk Svoboda**

Studijní program: N3908 Požární ochrana a průmyslová bezpečnost

Studijní obor: 3908T007 Bezpečnostní plánování

Téma: Kritická infrastruktura a její ochrana
Critical Infrastructure and Its Protection

Zásady pro vypracování:

Cíl práce:
Navrhnout možné způsoby ochrany subjektů a objektů kritické infrastruktury.

Charakteristika práce:
Kritickou infrastrukturou jsou chápány výrobní a nevýrobní systémy a služby, jejichž nefunkčnost by měla závažný dopad na bezpečnost státu, ekonomiku, veřejnou správu a zabezpečení základních životních potřeb obyvatelstva, a proto je nutné zabezpečit ochranu vybraných objektů a subjektů kritické infrastruktury (KI). Jelikož ochrana KI je proces, který při zohlednění všech rizik a hrozeb směřuje k zajištění fungování subjektů a objektů KI, výsledkem diplomové práce by měly být navrženy možné způsoby ochrany subjektů a objektů KI.

Seznam doporučené odborné literatury:

•Beneš, I.: Zkušenosti s ochranou kritické infrastruktury v ČR, In: Sborník [CD-ROM], Lázeň Bohdaneč, 2006
•Commission of the European communities: GREEN PAPER on a European programme for critical infrastructure protection (Zelená kniha) [online], Brusel, 2005,
•Ministerstvo vnitra GŘ HZS ČR: Zpráva o řešení problematiky kritické infrastruktury, čj. PO-386-21/PLA-2006, usnesení Výboru pro civilní nouzové plánování č. 191 ze dne 21. března 2006
•ŠENOVSKÝ, M.; ADAMEC, V.; ŠENOVSKÝ, P.: Ochrana kritické infrastruktury. 1. vyd. Ostrava: Edice SPBI, 2007 136 str., ISBN 978-80-7385-025-8
•Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů

Formální náležitosti a rozsah diplomové práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí diplomové práce: **Ing. Danuše Kratochvílová**

Konzultant diplomové práce: doc. Ing. Vilém Adamec, Ph.D.

Datum zadání: 30.11.2009
Datum odevzdání: 30.04.2010

VYSOKÁ ŠKOLA BÁŇSKÁ - TECHNICKÁ UNIVERZITA OSTRAVA
Fakulta bezpečnostního inženýrství

Bradáčová

Ing. Isabela Bradáčová, CSc.
vedoucí katedry

u. z. dlmuk

prof. Dr. Ing. Aleš Dudáček
děkan fakulty

Místopřísežné prohlášení

„Místopřísežně prohlašuji, že jsem celou diplomovou práci vypracoval samostatně pod vedením vedoucího diplomové práce a uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal“.

Dne 26. dubna 2010

Bc. Zdeněk Svoboda

Poděkování:

Rád bych poděkoval Ing. Danuši Kratochvílové, vedoucí diplomové práce, za ochotu, odborné vedení, cenné rady, připomínky a značnou podporu při zpracování uvedené problematiky. Dále bych rád poděkoval kolegům z oddělení krizového řízení Policie České republiky Krajského ředitelství policie Moravskoslezského kraje Ing. Miloši Zajícovi a z oddělení krizového řízení Policie České republiky Krajského ředitelství Olomouckého kraje Mgr. Vladimíru Obšilovi, včetně kolegům z oddělení krizového řízení Hasičského záchranného sboru Olomouckého kraje za cenné rady a ochotu při poskytnutí materiálů ke zpracování uvedené problematiky.

Anotace

SVOBODA, Z.: *Kritická infrastruktura a její ochrana*. Diplomová práce, VŠB – TU Ostrava, 2010, 74 s.

Diplomová práce pojednává o kritické infrastruktuře a její ochraně. Práce je rozdělena do několika kapitol. V počátečních kapitolách diplomové práce jsou uvedeny všeobecné informace ke kritické infrastruktuře od jejího vývoje až po současný stav, hlavně v České republice. V diplomové práci jsou prezentovány některé vhodné metody pro analýzu rizik. Závěrečné kapitoly diplomové práce se zabývají vybraným subjektem kritické infrastruktury, analýzou rizik vybraného subjektu pomocí metody Check list. Na základě výsledků je navržena ochrana subjektu kritické infrastruktury.

Klíčová slova: kritická infrastruktura, oblasti kritické infrastruktury, subjekt kritické infrastruktury, mimořádná událost, riziko, ochrana kritické infrastruktury.

Annotation

SVOBODA, Z.: *Critical Infrastructure and Its Protection*. The thesis, VŠB – TU Ostrava, 2010, 74 pages

The thesis deals with critical infrastructure and its protection. The work is dividend into several chapters. The first chapters give general information on critical infrastructure and its development to the present state, mainly in the Czech Republic. Some suitable risk analysis methods are presented in the thesis. The final chapters of the thesis deal with the elected subject of critical infrastructure analysing risks of the elected subject by means of the Check list method. On the basis of the results the critical infrastructure protection of the subject is protected.

Key words: critical infrastructure, critical infrastructure sectors, subject of critical infrastructure, extraordinary event, risk, critical infrastructure protection.

OBSAH

1. Úvod

Při výběru z vyhlášených témat pro diplomové práce jsem se rozhodoval podle toho, co je nejbližší mé profesi, kterou je komisař skupiny krizového řízení Policie České republiky. Proto také nakonec mé rozhodnutí padlo na téma „Kritická infrastruktura a její ochrana“. Společný prvek s mou současnou profesí, jenž je zahrnutý do kritické infrastruktury a její ochrany, spočívá především v oblasti ochrany bezpečnosti osob, majetku a plnění dalších úkolů na úseku vnitřního pořádku a bezpečnosti a krizového řízení.

Zvyšující se zranitelnost moderní společnosti je předmětem dlouhodobých diskusí, jak na úrovni Evropské unie, tak i v České republice. V rámci zabývání se problematiky zranitelnosti moderní společnosti si ti, kteří se této problematice věnují, kladou hlavní otázky související s ohrožením obyvatelstva, zachováním základních funkcí státu, zvyšováním prevence, připravenosti a zvládání následků jakékoliv mimořádné události. K tomu samozřejmě patří i rychlé zabezpečení fáze obnovy postiženého území mimořádnou událostí. I Česká republika stejně jako státy mezinárodního společenství se musela začít zabývat mírou zranitelnosti obyvatelstva, hospodářských subjektů, stavem zabezpečení základních funkcí státu zejména v krizových situacích a zabezpečení základních životních potřeb obyvatelstva v situacích, které se vymykají označení „běžný chod a fungování“. Proto je úkolem vlády státu zajistit nezbytně plynulé fungování základních životně důležitých prostředků a adekvátně je chránit, posilovat a starat se o jejich spolehlivý chod. Toto téma ochrany životně důležitých zdrojů, infrastruktur a služeb spadá do problematiky, kterou nazýváme kritická infrastruktura neboli životně důležitá infrastruktura [13].

Cílem mé diplomové práce je navrhnout možné způsoby ochrany subjektů nebo objektů kritické infrastruktury z hlediska jejího zabezpečení proti mimořádným událostem, které kritickou infrastrukturu ohrožují. V jednotlivých kapitolách diplomové práce vysvětlím podstatu infrastruktury, rizika, která ji ohrožují, a popíšu vybrané metody pro analýzu rizik. Závěrem diplomové práce pak bude navržení způsobu ochrany vybraného subjektu nebo objektu kritické infrastruktury.

Co mě vede k tomuto tématu. Jak jsem na začátku uvedl, společný prvek s mou současnou profesí spočívá především v ochraně bezpečnosti osob, majetku a další úkoly na úseku vnitřního pořádku a bezpečnosti a krizového řízení. Jediný poznatek, který jsem v současnosti získal a ještě získávám, je studium na Vysoké škole báňské, Technická univerzita Ostrava, Fakulta bezpečnostního inženýrství, obor Bezpečnostní plánování, forma

magisterského kombinovaného studia. V průběhu studia jsem se seznámil v rámci předmětu „Ochrana kritické infrastruktury“ blíže s touto problematikou, s legislativou a orientací v ní. Rozhodl jsem se zaměřit na tuto problematiku v rámci diplomové práce, protože ji vnímám jako velmi důležitou oblast pro zachování základních funkcí státu za krizových situací a zachování důležitých potřeb pro obyvatelstvo. Její ohrožení nebo napadení se nedotýká pouze státu a obyvatel v něm, ale i mě samotného včetně mé rodiny a přátel. Pojem kritická infrastruktura je poměrně málo známý a problematika ochrany kritické infrastruktury je relativně mladým odvětvím. Podklady pro mou práci jsem čerpal převážně z platné legislativy, dostupné literatury, internetových stránek, studijních materiálů získaných v průběhu studia od pedagogů a také konzultací s odborníky, kteří v této oblasti nebo jí podobné v současné době pracují nebo v minulosti pracovali.

2. Rešerše

2.1. Literární zdroje

ŠENOVSKÝ M., ADAMEC V., ŠENOVSKÝ P., *Ochrana kritické infrastruktury*, 1. Vydání Ostrava: Edice SPBI Spektrum, 2007, 141 stran, ISBN: 978-80-7385-025-8

Tato publikace popisuje informace z oblasti ochrany životně důležité kritické infrastruktury. V úvodní části jsou popisovány všeobecné informace o vývoji a současném stavu ochrany kritické infrastruktury u nás i v zahraničí. V další části publikace jsou popisovány teoretické pasáže věnované základním principům ochrany kritické infrastruktury, stanovení kritických prvků a možné směry k eliminaci kritických prvků v posuzovaných systémech [1].

Zelená kniha o Evropském programu na ochranu kritické infrastruktury

Zelená kniha má celkem 9 kapitol. Hlavním cílem zelené knihy bylo zapojit do programu ochrany kritické infrastruktury velké množství zainteresovaných subjektů – vlastníků a provozovatelů infrastruktur, regulační orgány, profesní organizace a odvětvová sdružení, stejně jako všechny úrovně státní a veřejné správy a také veřejnosti. Úkolem bylo získat tak od nich konkrétní informace o politikách vhodných pro European Programme for Critical Infrastrukture Protection (dále jen „EPCIP“). Zelená kniha předkládala možnosti, kterých mohla Evropská Komise využít, aby splnila požadavek Evropské Rady zřídit EPCIP a vytvoření Varovné informační sítě kritické infrastruktury (CIWIN), s cílem zavést Evropský program na ochranu kritické infrastruktury. Evropská komise od předložení zelené knihy očekávala konkrétní reakce na možnosti politik, které jsou v dokumentu popsány [2].

Směrnice rady 2008/114/ES, ze dne 8. prosince 2008, o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu

Cílem této směrnice je určit a označit evropskou kritickou infrastrukturu a posoudit potřebu zvýšit její ochranu. Proto se směrnice soustředí na odvětví energetiky a dopravy a měla by být přezkoumána s ohledem na posouzení jejího dopadu a nutnosti zahrnout do její oblasti působnosti další odvětví, mimo jiné odvětví informačních a komunikačních technologií. Tato směrnice určuje primární a konečnou odpovědnost za ochranu evropské kritické infrastruktury, kterou nesou členské státy a vlastníci (provozovatelé) těchto infrastruktur. Směrnice stanovuje provedení členským státům přijmout nezbytná opatření pro dosažení souladu s touto směrnicí do 12. ledna 2011 s tím, že přijatá opatření musí obsahovat odkaz na tuto směrnici. Přezkum směrnice bude zahájen 12. ledna 2012. V přílohách této směrnice

je uveden seznam odvětví evropské kritické infrastruktury, postup vypracování plánu bezpečnosti provozovatele evropské kritické infrastruktury a postup při určení kritické infrastruktury, která může být označena za evropskou kritickou infrastrukturu, členskými státy podle článku 3 [10].

2.2. Legislativní zdroje

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

Tento zákon vymezuje pojem a působnost integrovaného záchranného systému a jeho složek, pravomoc státních orgánů a orgánů územních samosprávných celků, vymezuje práva a povinnosti právnických a fyzických osob při přípravě na mimořádné události a při záchranných a likvidačních pracích, při ochraně obyvatelstva před a po dobu vyhlášení stavu nebezpečí, nouzového stavu, stavu ohrožení státu a válečného stavu, kterým se všeobecně říká krizové stavy [6].

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

Tento zákon stanoví působnost a pravomoc státních orgánů a orgánů územních samosprávných celků, práva a povinnosti právnických a fyzických osob při přípravě na krizové situace, které nesouvisejí se zajišťováním obrany České republiky před vnějším napadením, a při jejich řešení [7].

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

Zákon upravuje přípravu hospodářských opatření pro stav nebezpečí, nouzový stav, stav ohrožení a válečný stav a přijetí hospodářských opatření po vyhlášení krizových stavů. Dále stanoví pravomoc vlády a správních úřadů, práva a povinnosti fyzických a právnických osob při přípravě a přijetí hospodářských opatření pro krizové stavy [8].

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

Tento zákon stanoví podmínky pro účinnou ochranu života a zdraví občanů, majetku před požáry, pro poskytování pomoci při živelních pohromách a jiných mimořádných událostech stanovením povinností ministerstev a jiných správních úřadů, právnických a fyzických osob,

postavení a působnosti orgánů státní správy a samosprávy na úseku požární ochrany a jednotek požární ochrany [9].

3. Vymezení pojmů

Strategie – podle [1] je dlouhodobý plán činností zaměřený na dosažení nějakého cíle a podle [14] je dlouhodobý záměr činnosti k dosažení určitého cíle.

Infrastruktura – představuje v obecném smyslu slova množinu prvků, které jsou strukturované, navzájem propojené a poskytují určitému celku rámcovou podporu. Tento pojem se obvykle používá pouze pro struktury, které jsou vytvořeny uměle [1].

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 [1].

Ochranou kritické infrastruktury – se rozumí proces, který při zohlednění všech rizik a hrozeb směřuje k zajištění fungování subjektů kritické infrastruktury a vazeb mezi nimi [1].

Subjekty kritické infrastruktury – jsou vlastníci a provozovatelé výrobních a nevýrobních systémů vytvářející produkty nebo poskytující služby kritické infrastruktury [1].

Objekty kritické infrastruktury – jsou vybrané stavby a zařízení veřejné infrastruktury a další prvky, které vlastní nebo provozují subjekty kritické infrastruktury [1].

Mimořádná událost – je škodlivé působení sil a jevů vyvolaných činností člověka, přírodními vlivy, a také haváriemi, které ohrožují život, zdraví, majetek nebo životní prostředí a vyžadují provedení záchranných a likvidačních prací [6].

Krizová situace – je mimořádná událost, při níž je vyhlášen stav nebezpečí nebo nouzový stav nebo stav ohrožení státu (dále jen „krizové stavy“) [7].

Fyzická ochrana kritické infrastruktury – je soubor bezpečnostních opatření plánovaných a realizovaných k ochraně subjektů a objektů kritické infrastruktury před útoky fyzických osob [5].

Hrozba – je jakýkoli fenomén, který má potenciální schopnost poškodit zájmy a hodnoty chráněné státem. Míra hrozby je dána velikostí možné škody a časovou vzdáleností (vyjádřenou obvykle pravděpodobností čili rizikem) možného uplatnění této hrozby [17].

Riziko – je možnost, že s určitou pravděpodobností vznikne událost, kterou považujeme z bezpečnostního hlediska za nežádoucí. Riziko je vždy odvoditelné a odvozené z konkrétní hrozby. Míru rizika, tedy pravděpodobnost škodlivých následků vyplývajících z hrozby

a ze zranitelnosti zájmu, je možno posoudit na základě tzv. analýzy rizik, která vychází i z posouzení naší připravenosti hrozbám čelit [18].

Areál – je samostatná budova, komplex budov nebo jinak ohraničený prostor, ve kterém je dislokován útvar nebo jeho organizační článek [32].

Zbraň – se rozumí zbraň střelná včetně střeliva a doplňků zbraně, zbraň bodná a sečná [28].

4. Historický vývoj kritické infrastruktury

Přístupy k ochraně kritické infrastruktury se dlouhodobě vyvíjely nejen u nás, ale i v zahraničí. Vývoj v posledních 50 letech zaznamenal různorodost priorit v její ochraně. Za hlavní prioritu v polovině minulého století byla označena hrozba jaderného napadení. Tato hrozba se postupem času zeslabovala, hlavně z důvodu postupného odzbrojení na základě podepsaných dohod mezi Spojenými státy americkými a Sovětským svazem. Druhý důvodem pak byl pád komunismu ve východním bloku. Místo této hrozby se stále více začala objevovat hrozba v podobě živelných pohrom. Ale největší zlom v přístupu k ochraně kritické infrastruktury nastal po 11. září 2001, kdy došlo k teroristickému útoku ve Spojených státech amerických. Na základě této události se do popředí dostala ochrana kritické infrastruktury před teroristickými útoky [1].

Za období Československé socialistické republiky nebyl pojem kritická infrastruktura neznámý. V období budování socialismu měly různé etapy v této oblasti různé priority. Od 80. let minulého století byla priorizována potřeba hlavně zvýšení odolnosti objektů národního hospodářství proti účinkům zbraní hromadného ničení. Již v této době se nepohlíželo na hodnocení zranitelnosti jenom z důvodu účinků zbraní hromadného ničení, ale v příslušných platných pokynech této doby bylo uvedeno, že při hodnocení zranitelnosti se musí brát v úvahu mimo jiné i rizika živelných pohrom a provozních havárií [1].

První úvahy o přístupu k problematice ochrany kritické infrastruktury se objevily především v USA a Kanadě. Tyto státy vycházely z prudkého vývoje v oblasti informačních a komunikačních technologií a s jejich vzájemným propojením a zasíťováním v rámci celého světa. Vyvstaly tak značné obavy o funkčnosti počítačových sítí v souvislosti se změnou století a tisíciletí. Jedním z prvních materiálů, řešících komplexně problematiku kritické infrastruktury na centrální úrovni velkého státu, byla směrnice prezidenta USA Billa Clintona z roku 1998 známá pod názvem White Paper, v překladu to znamená Bílá kniha. Kritická infrastruktura je v tomto dokumentu pojata jako soubor hmotných a nehmotných systémů, majících rozhodující vliv na zachování základních funkcí státu, především na ekonomiku. Tento soubor systémů zahrnuje oblasti telekomunikace, energetiky, bankovnictví, finančnictví, dopravu, zásobování vodou a záchranné služby. Hlavním smyslem prezidentské směrnice bylo přijetí nezbytných opatření k rychlé eliminaci zranitelnosti kritické infrastruktury vlivem fyzických nebo elektronických útoků, přičemž hlavní důraz byl tehdy přikládán možným útokům na elektronické informační a komunikační systémy. Významným požadavkem Bílé knihy je realizace ochrany kritické infrastruktury u všech subjektů státního,

privátního, veřejnoprávního a jiných sektorů, tedy v celé společnosti. Politika ochrany kritické infrastruktury tak stanovila cíle, představila koncepci, poskytla zdroje a zařadila kritickou infrastrukturu mezi národní životní zájmy řady států [16].

Mezi prvními evropskými státy, zabývajícími se problematikou kritické infrastruktury a její ochranou, byly Velká Británie a Německo. V roce 1999 bylo ve Velké Británii ustaveno Koordinační centrum pro bezpečnost národní infrastruktury (National Infrastructure Security Coordination Centre). Jeho úkolem bylo rozvíjet a koordinovat činnosti k obraně a ochraně kritické národní infrastruktury, v rámci níž byly identifikovány systémy důležité pro zabezpečení funkce státu, jejichž narušení nebo vyřazení by vedlo k ohrožení životů a k závažným negativním hospodářským a sociálním dopadům na společnost. Mezi tyto systémy patří dodávky energií a paliv, dodávky vody, potravin, krmiva, zabezpečení dopravy, všech veřejných služeb včetně zdravotnictví, komunikace, bankovnictví atd. Oblast kritické infrastruktury zahrnuje jak veřejný, tak i privátní sektor [16].

Otázkami ochrany kritické infrastruktury se v roce 1999 začalo zabývat také Německo, kde byl koncem roku 1999 na spolkové úrovni projednán s přijetím příslušných závěrů materiál s názvem Informačně technické ohrožení klíčových infrastruktur v Německu, který byl určitou základní platformou pro další činnost na tomto úseku zejména po roce 2001 [16].

V České republice se problémem ochrany kritické infrastruktury začali zabývat členové Výboru pro civilní a nouzové plánování (dále jen „VCNP“), kteří na schůzi dne 24. září 2002 projednali první materiál na téma kritická infrastruktura, a to Zprávu o národní kritické infrastruktuře. Dohodli se, že následné řešení tohoto tématu a vytváření dalšího materiálu bude projednáváno pod pracovním názvem Projekt Analýzy zabezpečení základních funkcí státu včetně ochrany životně důležité infrastruktury v případě krizových situací. Usnesením VCNP č. 153 ze dne 24. září 2002 byla ustanovena odborná pracovní skupina VCNP k řešení odborné problematiky zachování základních funkcí státu a kritické infrastruktury. Výsledkem práce odborné skupiny byl materiál nazvaný Informace o přípravě koncepčního řešení ke snižování a k eliminaci důsledků informačního boje, cizího zpravodajského pronikání a kriminálního napadání informačních systémů. Skupina se pak scházela podle potřeby, zejména při posuzování zahraničních materiálů a o své činnosti minimálně dvakrát ročně informovala VCNP [13].

V roce 2003 se Bezpečnostní rada státu usnesla, že Ministerstvo vnitra – generální

ředitelství Hasičského záchranného sboru ČR ve spolupráci s dalšími rezorty a ústředními správními úřady stanoví rozsah základních funkcí státu za krizových situací, které jsou nezbytné pro zajištění ochrany životů a zdraví občanů, majetku, životního prostředí a státu samotného.

Pod pojmem rozsah základních funkcí státu při krizových situacích jsou chápány všechny funkce státní a soukromé sféry, které zabezpečují komplexní, tzn. i fyzickou (technickou) základnu, umožňující zachování nezbytného rozsahu základních funkcí státu. Systém legislativních, organizačních a technických opatření, realizovaný státní i soukromou sférou ve stanovených oblastech, musí při krizové situaci zabezpečit základní životní podmínky a potřeby obyvatel na státním území a k tomu nezbytný rozsah řídící a organizátorské práce ve státní i soukromé sféře.

Základní funkcí státu za krizových situací je zabezpečit:

- ochranu života a zdraví obyvatel,
- obranu ČR, svrchovanost státní moci a územní celistvost,
- základní životní podmínky a potřeby obyvatelstva,
- koncentraci a koordinaci výkonu státní správy a územní samosprávy pro řešení krizových situací,
- zákonnost, bezpečnost a vnitřní pořádek,
- ekonomické, materiální, energetické a finanční zdroje pro řešení krizové situace,
- funkčnost orgánů krizového řízení, záchranných sborů, ozbrojených sil, ozbrojených bezpečnostních sborů a havarijních služeb pro krizové situace,
- dopravní obslužnost,
- systémy, jejichž zničení nebo snížení funkčnosti by mělo závažné dopady na obranyschopnost, ekonomickou a společenskou stabilitu a bezpečnost státu.

Výbor pro civilní a nouzové plánování přijal usnesením č. 173 ze dne 24. června 2003 materiál, který představoval první ucelený a souhrnný přehled situace v jednotlivých odvětvích kritické infrastruktury, včetně právních předpisů, první definice základních funkcí státu při krizových situacích a kritické infrastruktury a předpokládaných dopadů a závěrů. Výbor pro civilní a nouzové plánování schválil usnesením č. 179 ze dne 23. září 2003 přehled vybraných subjektů kritické infrastruktury, které by bylo nutné v případě potřeby

a úmyslného útoku chránit. V rámci ochrany kritické infrastruktury v České republice byly vypracovány seznamy subjektů kritické infrastruktury na národní, regionální a místní úrovni. V následujícím období pokračovala další aktualizace tohoto seznamu. V oblasti ochrany kritické infrastruktury v případě krizových situací byl projednán na schůzi Výboru pro civilní nouzové plánování nový pohled na přehled oblastí kritické infrastruktury s vydaným usnesením č. 190 ze dne 23. března 2004. Podstatou tohoto nového pohledu bylo provedeno přepracování obsahu přehledu oblastí kritické infrastruktury, z důvodu chybně nastavené celkové struktury těchto oblastí. Usnesení č. 191 ze dne 22. června 2004 schválené na 24. schůzi Výboru pro civilní nouzové plánování přineslo drobnou korekci ve sloupci odpovědných gestorů za danou oblast kritické infrastruktury. Tímto usnesením po provedené korekci bylo schváleno 10 oblastí kritické infrastruktury ČR [16], které jsou uvedeny v příloze č. 1.

Těchto 10 oblastí tvoří základ pro odborné posuzování v rámci působnosti příslušných ministerstev a dalších ústředních správních úřadů a pro zpracování popisu zranitelnosti systému v každé z uvedených oblastí podle jednotlivých druhů ohrožení.

Odpovědnost za jednotlivé oblasti kritické infrastruktury mají jednotlivá ministerstva a ústřední správní úřady podle jejich kompetencí. Na území České republiky bylo z hlediska kritické infrastruktury stanoveno 42 nejdůležitějších objektů celostátního významu.

Evropská Rada a Evropská Komise se začala zabývat ochranou kritické infrastruktury od roku 2004, kdy zahájila jednání a přípravu programu pro ochranu kritické infrastruktury pod názvem European Programme for Critical Infrastrukture Protection (dále jen „EPCIP“). Na základě jednotného stanoviska členských států Evropské unie Evropská Rada a Evropská Komise potvrdily, že národní kritická infrastruktura zůstává nadále v odpovědnosti a jurisdikci příslušného členského státu Evropské unie. V roce 2006 pak byly předloženy dva dokumenty Evropské Komise. Jednalo se o návrh Směrnice Evropské Rady o určení a stanovení evropské kritické infrastruktury a vyhodnocení potřeb zlepšení její ochrany a Sdělení Evropské Komise o EPCIP [13]. Ke konci roku 2008 přesně dne 8. prosince 2008 pak Evropská unie schválila a vydala v Úředním věstníku Evropské unie Směrnici Rady 2008/114/ES o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu.

5. Infrastruktura

Termín infrastruktura má svůj původ v 19. století ve Francii a během první poloviny 20 století primárně označoval vojenská zařízení. Infrastruktura z francouzského jazyka *infra-structure* (doslova: co je pod stavbami), je v nejobecnějším smyslu slova množina propojených strukturálních prvků, které pak udržují celou strukturu pohromadě. Obvykle se používá pouze pro struktury, které jsou uměle vytvořené [13].

Infrastruktura obecně je množina propojených stavebních prvků, které poskytují rámcovou podporu celku. Termín infrastruktura má různé významy v různých oblastech, ale nejčastěji je chápán ve vztahu k silnicím, letišti či technickému vybavení. Tyto různé prvky mohou být souhrnně pojmenovány jako civilní infrastruktura, městská infrastruktura, či veřejné komunikace a stavby. Infrastruktura může být zřízena a spravována soukromým sektorem nebo státem [13].

5.1. Veřejná infrastruktura

V 80. letech 20. století v USA veřejná infrastruktura vymezena tak, že se vztahuje jak ke specifickým funkcím – dálnice, ulice, silnice a mosty; hromadná doprava, letiště a letecká síť; vodárny a vodní zdroje; čistírny odpadních vod; zpracování komunálního odpadu; výroba a přenos elektrické energie; telekomunikace a zpracování nebezpečného odpadu – tak i ke složeným polyfunkčním systémům [14].

Význam infrastruktury nespočívá jen ve veřejném zařízení, ale i v jeho správě, údržbě a rozvoji, který souvisí se společenskými požadavky a fyzickým světem, aby usnadnil dopravu lidí a zboží, poskytl vodu k pití i technickému využití, bezpečně naložil s komunálním odpadem, poskytl energii, kde je třeba a přenesl informace v rámci a mezi komunitami [14].

V České republice se podle zákona [11] veřejnou infrastrukturou rozumí pozemky, stavby, zařízení a to:

1. dopravní infrastruktura, např. stavby pozemních komunikací, drah, vodních cest, letišť a s nimi souvisejících zařízení,
2. technická infrastruktura, kterou jsou vedení a stavby a s nimi provozně související zařízení technického vybavení, např. vodovody, vodojemy, kanalizace, čistírny odpadních vod, stavby a zařízení pro nakládání s odpady, trafostanice, energetické

vybavení, komunikační vedení veřejné komunikační sítě a elektronické komunikační zařízení veřejné komunikační sítě, produktovody,

3. občanské vybavení, kterým jsou stavby, zařízení a pozemky sloužící např. pro vzdělávání a výchovu, sociální služby a péči o rodiny, zdravotní služby, kulturu, veřejnou správu, ochranu obyvatelstva,
4. veřejná prostranství, zřizované nebo užívané ve veřejném zájmu.

5.2. Kritická infrastruktura

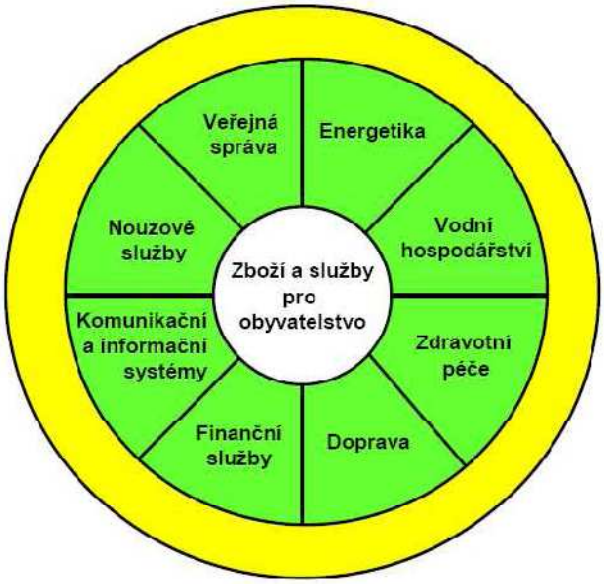
Definice kritické infrastruktury říká, že kritickou infrastrukturou se rozumí výrobní a nevýrobní systémy a služby, jejichž nefunkčnost by měla závažný dopad na bezpečnost státu, ekonomiku, veřejnou správu a zabezpečení základních životních potřeb obyvatelstva. Z definice vyplývá, že úkolem společnosti je tedy kritickou infrastrukturu chránit tak, aby fungovala za běžných, mimořádných i krizových situací. Z tohoto je možno vyvodit, že ochrana kritické infrastruktury je proces, který při zohlednění všech rizik a hrozeb směřuje k zajištění fungování kritické infrastruktury [1].

Na kritickou infrastrukturu musíme pohlížet jako na komplexní systém. Kritická infrastruktura má síťové uspořádání, které se skládá z jednotlivých prvků sítě a spojnic (jednotlivé prvky jsou vzájemně provázané). Stejně jako v každé síti se i zde nachází místa, kde se schází více prvků spojnic, které tvoří uzel. Proto poškození, narušení nebo výpadek některého uzlu má více nebo méně závažný dopad na funkčnost dalších uzlů. Tento výpadek by mohl způsobit následné zhroucení celé kritické infrastruktury. Z tohoto důvodu by mělo být v zájmu ochrany kritické infrastruktury tyto uzly chránit.

Ochrana kritické infrastruktury je založena na snížení zranitelnosti systému neboli zvýšení jeho odolnosti vůči dopadům mimořádných událostí. Pro tyto případy je nutné mít připravená opatření zaměřená na zmírnění a odstranění škod. Z toho vyplývá, že se snažíme pomocí provádění preventivních opatření, např. zvýšením bezpečnosti systému technicko-organizačním opatřením, zabránit vzniku mimořádných událostí nebo alespoň udržet následky způsobené mimořádnými událostmi v co nejnižším rozsahu [1].

Kritická infrastruktura je velice rozsáhlá a očekává se, že stát ji bude nepřetržitě chránit. Problém je ale v tom, že ne všechny subjekty kritické infrastruktury patří do majetku státu. Některé subjekty kritické infrastruktury jsou ve vlastnictví soukromého sektoru a ty mají hlavně zájem o zvyšování svého zisku, před zajištěním ochrany a bezpečnosti kritické infrastruktury. Díky tomu se ochrana kritické infrastruktury stává složitějším procesem.

Z tohoto vyplývá, že stát nemůže investovat státní peníze do ochrany kritické infrastruktury, která je v soukromých rukou, ale ani nemůže přinutit soukromý subjekt, aby investoval své peníze do ochrany kritické infrastruktury, např. ve formě preventivních opatření. Přesto se stát musí zabývat průběžně problematikou ochrany kritické infrastruktury, která je nejenom ve vlastnictví státu, ale i ve vlastnictví soukromých subjektů, protože ji potřebuje k zajištění základních životních potřeb státu a obyvatelstva. Důležitost kritické infrastruktury z pohledu ochrany obyvatelstva je znázorněna na obrázku 1.



Obr. 1: Kritická infrastruktura z pohledu ochrany obyvatelstva
zdroj: ADAMEC, V., *Kritické infrastruktury I*, elektronický studijní materiál ve formátu pdf

V České republice za problematiku ochrany kritické infrastruktury zodpovídá Výbor pro civilní a nouzové plánování, který je stálým pracovním orgánem Bezpečnostní rady státu České republiky.

V rámci průběžného projednávání kritické infrastruktury a její aktualizace, byl zpracován dokument s názvem „Zpráva o řešení problematiky kritické infrastruktury“, který byl předložen k projednání na schůzi Výboru pro civilní a nouzové plánování dne 21. března 2007. Tento dokument se týkal návrhu relevantních gestorů, případně spolugestorů za dané oblasti kritické infrastruktury. V dokumentu se vypustila z celkového přehledu oblast č. 10 – odpadové hospodářství a upravilo se vnitřní členění oblasti č. 4 – zdravotní péče, oblasti č. 8 – nouzové služby a oblasti č. 9 – veřejná správa. Tento návrh dokumentu byl projednán členy Výboru pro civilní a nouzové plánování dne 12. června 2007 a schválen v usnesení č. 277.

Bezpečnostní rada státu ve svém usnesení [12] následně projednala a schválila předložených 9 oblastí a v jejich rámci deklarovala 37 produktů a služeb [1], viz tabulka 1.

Tabulka 1: Oblasti národní kritické infrastruktury schválené v roce 2007 [1, 12]

P.č.	***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 z 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.	Zdravotnická 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 datovým službám.
7.	Bankovní a finanční systém	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 opatřeních 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 (soc. zabezpečení, stát. soc. podpora, soc. pomoc). 9.3. výkon justice a vězeňství.

Kritickou infrastrukturu můžeme na základě jejich technických, strukturálních a funkčních specifik roztřídit na:

- technickou infrastrukturu,
- sociálně-ekonomickou infrastrukturu.

Do technické infrastruktury řadíme – energetiku, vodní hospodářství, dopravu a komunikační a informační systémy.

Do infrastruktury sociálně-ekonomických služeb pak přísluší – zdravotní péče, veřejná správa, finanční služby a nouzové služby.

Mezi oběma oblastmi kritické infrastruktury existuje značná závislost. Například u všech sociálně-ekonomických služeb se vyžaduje neomezená možnost disponovat s technickou infrastrukturou a technická infrastruktura je v případě krize na sociálně-ekonomických službách závislá.

Podíváme-li se na vlastnické vztahy kritické infrastruktury, jedná se z části o státní instituce, ale většinou jsou v rámci privatizace tyto infrastruktury převedeny do vlastnictví soukromých rukou. Tento trend přechodu na soukromě-právní formy podnikání se stále častěji projevuje u veřejných služeb [31].

Usnesení Bezpečnostní rady státu [12] v rámci řešení problematiky kritické infrastruktury pro nejbližší období uložilo dva základní úkoly a to vytvoření:

1. Komplexní strategie ČR k řešení problematiky kritické infrastruktury.
2. Národního programu ochrany kritické infrastruktury.

5.2.1. Komplexní strategie České republiky k řešení problematiky kritické infrastruktury

Komplexní strategie České republiky k řešení problematiky má vycházet z analýzy stavu řešení problematiky kritické infrastruktury v České republice, přičemž by měla vzít v úvahu evropský a mezinárodní kontext této problematiky. Z hlediska národní, krajské i místní úrovně, se musí definovat vazby a vztahy mezi kritickou infrastrukturou a obrannou infrastrukturou.

Na základě usnesení Bezpečnostní rady státu [12] byl Ministerstvem vnitra – generálním ředitelstvím Hasičského záchranného sboru České republiky zpracován návrh tezí Komplexní strategie České republiky k řešení problematiky kritické infrastruktury České

republiky [19]. Tento návrh obsahoval 3 body:

1. Obecná východiska a mezinárodní aspekty.
2. Základní východiska v České republice.
3. Teze k řešení problematiky ochrany kritické infrastruktury.

V závěru přílohy návrhu teze byl zpracován i návrh obsahu Národního programu ochrany kritické infrastruktury.

V bodě prvním Obecná východiska a mezinárodní aspekty se poukazovalo, že připravovaná Komplexní strategie ČR k řešení kritické infrastruktury by se měla zajímat o širší kontext vývoje bezpečnostního prostředí, a to:

- Bezpečnostní hrozby.
- Klíčové oblasti kritické infrastruktury negativně zatížené bezpečnostními hrozbami, mezi které byly zařazeny:
  - Veřejné služby.
  - Veřejný pořádek a bezpečnost.
  - Veřejné zdraví, zdravotnická služba, sociální služby.
  - Informování, varování a vyrozumění veřejnosti.
  - Připravenost obyvatelstva.
  - Energetická a surovinová bezpečnost.

Druhý bod Základní východiska v České republice obsahoval:

- zvyšující se zranitelnost moderní společnosti,
- úkol státu zajistit rozvoj země a bezpečnost občanů,
- ochrana fyzické a kybernetické infrastruktury,
- přímá souvislost se zpracováním krizových plánů a plánů krizové připravenosti,
- dokumenty týkající se obranné infrastruktury,
- dokumenty týkající se kritické infrastruktury.

V bodě třetím byl navržen obsah k problematice ochrany kritické infrastruktury s cílem její ochrany. Cílem ochrany kritické infrastruktury je, při zohlednění všech rizik a hrozeb, zajištění fungování objektů kritické infrastruktury a vazeb mezi nimi. Navrhovaný

obsah měl následujících deset bodů:

1. Stanovení metodického postupu řešení kritické infrastruktury.
2. Rizika narušení kritické infrastruktury.
3. Místo a úloha veřejné správy.
4. Úkoly subjektů kritické infrastruktury.
5. Nouzové služby.
6. Obyvatelstvo.
7. Odborná veřejnost, školství, věda a výzkum.
8. Mezinárodní spolupráce.
9. Vláda ČR.
10. Finanční zabezpečení.

Na základě těchto tezí byl v lednu roku 2008 zpracován a předložen Bezpečnostní radě státu „Harmonogram dalšího postupu zpracování dokumentů Komplexní strategie k řešení problematiky kritické infrastruktury a Národního programu ochrany kritické infrastruktury“. Bezpečnostní rada státu na svém zasedání tento „Harmonogram …“ vzala ve svém usnesení na vědomí [20]. O měsíc později Vláda České republiky na svém zasedání svým usnesením [21] Harmonogram předložený Bezpečnostní radou státu schválila a uložila ministru vnitra ve spolupráci s ostatními ministry a vedoucími ústředních správních úřadů zabezpečit plnění úkolů vyplývající z Harmonogramu a informovat vládu o stavu plnění těchto úkolů do konce roku 2008.

5.2.2. Národní program ochrany kritické infrastruktury

V rámci návrhu tezí a později Harmonogramu byl i návrh obsahu Národního programu ochrany kritické infrastruktury, který by měl být přijatý Vládou České republiky usnesením jako vládní dokument, který by se měl zaměřit na [1, 19]:

- Legislativní úpravy ve vazbě na legislativu v oblasti bezpečnosti (krizové zákony, obrana státu, apod.) a závazné dokumenty zejména Evropské unie.
- Zpracování metodik zabezpečení ochrany kritické infrastruktury – obecná, specifické pro jednotlivé oblasti.
- Úpravy metodik pro zpracování plánů v oblasti bezpečnosti (krizové plány, plány krizové připravenosti, apod.).

- Tvorba a úpravy plánů zachování kontinuity činností subjektů kritické infrastruktury k zajištění minimální funkčnosti kritické infrastruktury.
- Úpravy vnitřních předpisů, norem a standardů pro příslušné sektory kritické infrastruktury z hlediska jejich dostatečnosti pro ochranu kritické infrastruktury.
- Zásady informování (vyrozumění) hlavních vlastníků/dodavatelů činností (služeb) v oblasti kritické infrastruktury.
- Vytvoření podmínek pro nácvik opatření k ochraně kritické infrastruktury (simulátory ohrožení sektorů či subjektů kritické infrastruktury).
- Vytvoření podmínek pro financování opatření ochrany kritické infrastruktury, včetně projektů uplatňovaných v rámci programů Evropské unie.

Národní program ochran kritické infrastruktury by pak měl být podpořen přijetím Komplexní strategie k řešení problematiky kritické infrastruktury.

5.3. Kritéria pro začleňování subjektů kritické infrastruktury do kategorií

Jednotlivé subjekty kritické infrastruktury se zařazují do čtyř kategorií, které zachovává stávající územní princip:

- **Subjekty kritické infrastruktury kategorie III** – jsou subjekty místní úrovně. Dojde-li k narušení těchto subjektů následkem je ovlivnění společenského života v obci nebo části obce. Jejich narušení má za následek převážně špatně fungující zásobování obce, např. zásobování potravinami, elektrickou energií, dopravní obslužností, pitnou vodou apod. U subjektů této kategorie lze nefungování nahradit přijetím zvláštních organizačních opatření nebo je můžeme provizorně řešit s využitím nouzových služeb. Nahrazení lze řešit dodávkou potravin, pitné vody, náhradního zdroje elektrické energie apod.
- **Subjekty kritické infrastruktury kategorie II** – jsou subjekty krajské úrovně. Pokud dojde k narušení těchto subjektů následkem je ovlivnění společenského života ve více obcí, části kraje nebo celého kraje. Pokud dojde k narušení objektů této kategorie, řeší si problém vlastník subjektu samostatně, ve spolupráci s krajem nebo ve spolupráci s hasičským záchranným sborem kraje, do jehož správního obvodu spadá.
- **Subjekty kritické infrastruktury kategorie I** – jsou subjekty národní úrovně. Pokud dojde k narušení těchto subjektů má to dopad na zajištění bezpečnosti státu, zabezpečení základních životních potřeb obyvatelstva na území dvou a více krajů

nebo celého státu. Pokud dojde k narušení objektů této kategorie, řeší si problém vlastník subjektu samostatně, nebo ve spolupráci s ministerstvy a ústředními správními úřady, které odpovídají za oblasti a podoblasti, do jehož správního obvodu spadá. Subjekty kategorie I jsou prakticky nenahraditelné, jejich vyřazení je možné řešit pouze provizorně nebo s využitím předem připravených zdrojů (zásoby plynu, PHM, apod.).

- **Subjekty kritické infrastruktury zvláštní kategorie** – jsou subjekty nadnárodní úrovně. Pokud dojde k narušení těchto subjektů má to dopad na zajištění bezpečnosti států na území dvou a více zemí Evropské unie.

Kategorizace má za cíl vymezit pro jednotlivé kategorie subjektů kritické infrastruktury opatření k zachování potřebných činností a služeb v případě narušení jejich fungování. Požadavky na jednotlivé kategorie jsou přehledně zpracovány do tabulek uvedené v přílohách č. 2 – 5 [1].

6. Ohrožení kritické infrastruktury

Poškození, zničení nebo narušení kritické infrastruktury může být způsobeno jak přírodními katastrofami, tak selháním techniky a technologických postupů, jakož i vlivem člověka, včetně terorismu a organizovaného zločinu [3].

Kritickou infrastrukturu ohrožují mimořádné události, které mají mnoho forem třídění, rizika a hrozby. Pravděpodobnost vzniku mimořádné události vyplývá ze statistik daného oboru techniky. Údaje jsou stále přesnější a pohotovější, protože je dnes díky počítačové technice evidujeme, klasifikujeme a vyhodnocujeme. Na základě toho jsme pak schopni stanovit přesněji míru ohrožení mimořádnou událostí. Obtížněji se stanovuje riziko hlavně nových technologií a nových systémů strojů. Možnost selhání v těchto případech lze obvykle přiblížit s pravděpodobností výpadků funkcí rozhodujících prvků systémů.

Rozlišujeme základní dělení mimořádných událostí, podrobné dělení mimořádných událostí je uvedeno v příloze č. 6. Mimořádné události rozdělujeme na základě podstaty jejich jevů do tří skupin:

1. **Přírodní (naturogenní) mimořádné události**, které vznikají za pomocí přírodních sil. Jsou reprezentovány seismickou aktivitou, vulkanickou činností, extrémními meteorologickými jevy, apod., které mohou být ještě umocněny doprovodnými ději.
2. **Antropogenní mimořádné události** způsobené činností člověka přímo nebo zprostředkovaně. Tyto mimořádné události může člověk způsobit záměrně nebo svou neopatrností.
3. **Kombinované mimořádné události** – zahrnují přírodní mimořádné události vyvolané dlouhodobou nebo krátkodobou činností člověka a antropogenní mimořádné události indukované stupňováním přírodního katastrofického jevu [1]. Pokud ve většině případů dochází k současnému působení mnoha přírodních a antropogenních jevů najednou, jedná se o tzv. dominoefekty a synergické jevy.

   Dominoefekt vyvolává lavinový sled projevů, to znamená, že například povodeň způsobí sesuv půdy, následuje ekonomická katastrofa, porušení produktovodu, výbuch plynu, požár s toxickým účinkem apod. [5].

   Synergický jev znamená, že několik jevů vzniká náhle najednou vlivem jedné příčiny. Typickým příkladem je výbuch, kdy během okamžiku působí v prostředí tlaková vlna, střepinový účinek, vysoká teplota, seismický otřes, rozptýlení nebezpečné látky apod. [5].

Mimořádné události, k jejichž řešení se vyhlašuje jeden z krizových stavů, pak označujeme jako krizové situace. Pro podmínky v České republice byl expertním odhadem stanoven omezený počet mimořádných událostí, při kterých lze očekávat vyhlášení krizových stavů. Tyto krizové stavy vzcházejí z přírodních a antropogenních mimořádných událostí [24]. Výčet typových krizových situací je uveden v příloze č. 7.

Kromě mimořádných událostí ohrožuje kritickou infrastrukturu i řada rizik. Některá rizika vznikají v bezprostřední návaznosti na mimořádné události. Proto se objevují ve výčtu jak mimořádných událostí, tak i rizik. Ohrožení objektů riziky můžeme rozdělit dle příčin narušení a místa výskytu [3].

a) **Vnitřní problémy**
   - příčiny narušení funkcí na objektech a v systémech kritické infrastruktury, které **nemusí být přímo** ovlivněny příslušným subjektem či subjekty, jedná se např. o rizika jako technologické havárie, technické poruchy, nedostatek náhradních dílů, výpadky dodávek energií, výpadky dodávek vody, výpadky dodávek surovin pro výrobu nebo poskytování služeb, kolaps počítačových sítí.
   - příčiny narušení funkcí na objektech a v systémech kritické infrastruktury, které **jsou přímo nebo nepřímo** ovlivněny příslušným subjektem nebo subjekty. Jedná se např. o rizika jako dočasná změna orientace poskytování výroků a služeb z důvodu řešení mimořádných událostí, dlouhodobá nebo trvalá změna orientace poskytování výrobků a služeb z důvodů rozhodnutí managementu subjektu kritické infrastruktury (může být ovlivněno i prorůstáním organizovaného zločinu do firem), krach firmy z ekonomických nebo jiných důvodů, stávka zaměstnanců subjektu kritické infrastruktury.

b) **Vnější problémy**, kde se jedná např. o rizika jako narušení objektu kritické infrastruktury z důvodu živelní pohromy nebo průmyslové havárie v sousedním objektu, narušení objektu kritické infrastruktury způsobené člověkem (teroristický útok, kriminální čin), nedostatek (úbytek) pracovních sil, včetně zvýšené nemocnosti, odmítnutí pracovat (např. při řešení vlastních problémů souvisejících se vznikem mimořádných událostí), stávka zaměstnanců subjektů zajišťujících služby (autodopravci, hromadná doprava).

V návrhu tezí ke Komplexní strategii České republiky k řešení problematiky kritické infrastruktury [19], bylo Ministerstvem vnitra – generálním ředitelstvím Hasičského záchranného sboru České republiky vybráno a navrženo 13 rizik, kdy při jejich výběru vycházelo z uvedených vnitřních a vnějších problémů, která mohou ohrozit kritickou infrastrukturu:

1. technologické havárie,
2. technické poruchy, nedostatek náhradních dílů,
3. výpadky dodávek energií (elektřina, plyn, teplo, nafta, benzín, apod.),
4. výpadky dodávek vody,
5. výpadky dodávek surovin (součástek) pro výrobu nebo poskytování služeb,
6. kolaps počítačových sítí,
7. narušení objektu kritické infrastruktury z důvodu živelní pohromy nebo průmyslové havárie v „sousedním objektu“,
8. narušení objektu kritické infrastruktury způsobené člověkem (teroristický útok, kriminální čin, důsledky války),
9. dočasná změna orientace (priorit) poskytování výrobků a služeb z důvodu řešení mimořádných událostí (krizových situací nevojenských i vojenských),
10. dlouhodobá nebo trvalá změna orientace (priorit) poskytování výrobků a služeb z důvodu rozhodnutí managementu subjektu kritické infrastruktury (může být ovlivněno i prorůstáním organizovaného zločinu do firem),
11. „krach“ firmy z ekonomických nebo jiných důvodů,
12. stávka,
13. nedostatek (úbytek) pracovních sil, včetně zvýšené nemocnosti (pandemie, infekční onemocnění), odmítnutí pracovat např. při řešení vlastních problémů souvisejících se vznikem mimořádných událostí.

7. Strategie ochrany kritické infrastruktury

Problematika ochrany kritické infrastruktury je složitým souhrnným problémem. Obsahuje v sobě prvky preventivní i prvky represivní. Prevence je prvkem nejdůležitějším, protože pokud bude vše spolehlivě fungovat, potom bude fungovat spolehlivě i chod státu a občan tak bude mít vytvořeny adekvátní podmínky pro svůj život. Úroveň ochrany založená na prevenci se přímo odvíjí od množství peněz, které jsme ochotni vydat. Musíme si položit zásadní otázku pro stanovení míry rizika, kterou jsme ochotni akceptovat. Žádný stát na světě není tak bohatý, aby mohl svou kritickou infrastrukturu chránit na 100 %.

Problém, který se vyskytuje, je že kritická infrastruktura není jenom v majetku státu, ale také ji vlastní podnikatelské subjekty. Tento problém se odráží v rozdílných cílech, protože cílem státu je mít na paměti bezpečnost obyvatelstva, zatím co podnikatelským subjektům jde především o zisk. Další problém je, že stát nemůže legálně vkládat státní peníze do ochrany kritické infrastruktury do soukromých rukou a stejně tak nemůže přinutit podnikající subjekty, aby vkládaly své peníze do preventivních opatření pro ochranu kritické infrastruktury. Všichni přesto očekávají, že stát bude kritickou infrastrukturu chránit kontinuálně, a že k tomu bude mít neomezené finanční prostředky a hlavně, že bude ochoten tyto prostředky do zvyšování bezpečnosti vkládat.

Z tohoto vyplývá, že problémy s ochranou kritické infrastruktury jsou zejména finanční, organizační a technické. Strategie je velmi důležitá, protože z ní můžeme odůvodnit nebo stanovit např. ekonomické požadavky ochrany kritické infrastruktury. Ekonomika je velmi důležitá nejenom pro stát, ale i pro podnikatelské subjekty [1].

Zabezpečení ochrany kritické infrastruktury, musí patřit k základním úkolům státu. Stát musí zajistit, že za normálních, abnormálních i kritických podmínek musí zůstat zachovány v provozu základní prvky, vazby a toky systému státu. Tyto prvky jsou základem schopnosti státu dosáhnout za každé situace stability a nastartovat další rozvoj. Ochrana kritické infrastruktury spadá do problematiky krizového řízení.

Konkrétní zájmy státu při ochraně kritické infrastruktury jsou:

- snížení zranitelnosti,
- ochrana lidí, kritických zdrojů a systémů, na nichž závisí existence společnosti,
- vytvoření podmínek pro prevenci a zajištění připravenosti na zvládání narušení kritické infrastruktury jako součásti programu rozvoje území,

– zabezpečení práv občanů a poskytnutí pomoci v případě narušení kritické infrastruktury a zajištění jejich informovanosti o připravených opatřeních k řešení krizové situace, o jejich odpovědnosti, o tom jak mohou pomoci v prevenci a jak by měli reagovat na vzniklou situaci.

Samostatná strategie by se měla zabývat způsoby prosazování zabezpečení ochrany kritické infrastruktury a zásadami řešení jejího narušení. Jde o stanovení strategických směrů k zajištění minimalizace narušení kritické infrastruktury nebo zabránění narušení kritické infrastruktury, včetně stanovení místa a úlohy veřejných institucí i výrobců či poskytovatelů služeb pro obyvatelstvo. Současně je potřebné řešit zásady spolupráce a vzájemné vztahy mezi státním a soukromým sektorem, jako nezbytnou podmínku pro komplexní řešení problému [3].

8. Analýza rizik

Nejdůležitějším krokem k eliminaci rizik a ke snížení možných dopadů rizik je nutné provést analýzu rizik. Analýza rizik je proces, který stanovuje pravděpodobnost uskutečnění hrozeb a dopadu na aktiva. Má za úkol identifikovat pravděpodobnost některé mimořádné události, jakož i možné dopady a škody. Jakékoliv účinné řešení problému je založeno na správně provedené analýze rizik [25].

8.1. Přístup k analýze rizik

Analýza rizik je nezbytným nástrojem k tomu, abychom byli schopni identifikovat zdroj rizik a dokázali se pak vzniklému riziku účinně bránit. Pomocí analýzy rizik roztřídíme, stanovíme žebříček důležitosti různých druhů rizik, vytvoříme analýzu vzniku příčin a následků. Na základě takto získaných výsledků provedeme hodnocení rizik.

Metody analýzy rizik, lze obecně rozdělit na kvantitativní a kvalitativní metody. Způsobů pro získávání dat a informací pro vytvoření analýz existuje velké množství, tak jako existuje také mnoho druhů metod. Jako například simulace na počítači, laboratorní pokusy, nebo pomocí použití jednodušších indexových metod. Nesmíme ale zapomínat, že kromě všech možných metod zůstává nejdůležitější a nezastupitelná lidská inteligence a že všechny metody pouze plní roli pomocného nástroje.

Výběr vhodné metody analýzy rizik velice závisí na tom, zda:

- známe nebo můžeme stanovit rozložení živelných pohrom, nehod, havárií, útoků, apod. v prostoru a v čase a můžeme spočítat četnostní rozložení živelných pohrom, nehod, havárií, útoků, apod. (počet vs. velikost) pro určité území a zvolený časový interval, dále vypočítat a zmapovat ohrožení,
- známe nebo můžeme stanovit rozložení živelných pohrom, nehod, havárií, útoků, apod., stanovit scénáře dopadů ve variantním provedení a pravděpodobnosti jejich výskytů [23].

8.2. Metody pro hledání rizik

Níže jsou uvedeny metody vhodné pro hledání rizik nebo kritických míst v systému. Je potřeba si uvědomit, že nelze přesně určit, které metody je vhodné použít na hledání rizik nebo kritických míst a které vhodné nejsou. Výsledek použité metody hledání rizik by měl být jednoduchý a hlavně srozumitelný nejenom expertům, ale i běžným uživatelům.

8.2.1. Check list (kontrolní seznam)

Kontrolní seznam je postup založený na systematické kontrole plnění předem stanovených podmínek a opatření. Seznamy kontrolních otázek jsou (checklists) zpravidla generovány na základě seznamu charakteristik sledovaného systému nebo činností, které souvisejí se systémem a potenciálními dopady, selháním prvků systému a vznikem škod. Jejich struktura se může měnit od jednoduchého seznamu až po složitý formulář, který umožňuje zahrnout relativní důležitost parametru (váhu) v rámci daného souboru [1, 23].

Analýza kontrolním seznamem se jeví jako optimální metoda, která se začíná používat častěji nejen u nás, ale i v zahraničí. Analýza kontrolním seznamem je proměnlivá metoda. Kontrolní seznam může být rychle použit pro jednoduchá vyhodnocení, ale i pro nákladnější podrobnější výsledky. Je to úsporný způsob jak identifikovat tradičně rozpoznatelné zdroje rizik [1].

8.2.2. Event Tree Analysis – ETA (analýza stromu událostí)

Analýza stromu událostí je postup, který sleduje průběh procesu od iniciační události přes konstruování událostí vždy na základě dvou možností – příznivé a nepříznivé. Metoda ETA je graficko-statistická metoda. Názorné zobrazení systémového stromu událostí představuje rozvětvený graf s dohodnutou symbolikou a popisem. Znázorňuje všechny události, které se v posuzovaném systému mohou vyskytnout. Podle toho jak počet událostí narůstá, výsledný graf se postupně rozvětvuje jako větve stromu [1, 23].

Analýza ETA je vhodná pro analýzu složitých procesů, které mají několik úrovní bezpečnostních systémů nebo postupů pro případ nouze, vhodný pro odezvu na určité iniciační události. Analýza stromem událostí se používá pro identifikaci různých nehod, které se mohou objevit u složitého procesu. Výsledkem jsou scénáře nehody, tj. soubor poruch nebo chyb, které vedou k nehodě [1].

8.2.3. Failure Mode and Efect Analysis – FMEA (analýza selhání a jejich dopadů)

Analýza selhání a jejich dopadů je postup založený na rozboru způsobů selhání a jejich důsledků, který umožňuje hledání dopadů a příčin na základě systematicky a strukturovaně vymezených selhání zařízení. Metoda FMEA slouží ke kontrole jednotlivých prvků projektovaného návrhu systému a jeho provozu. Představuje metodu tvrdého, určitého typu, kde se předpokládá kvantitativní přístup řešení. Využívá se především pro vážná rizika

a zdůvodněné případy. Vyžaduje aplikaci výpočetní techniky, speciální výpočetní program, náročnou a cíleně zaměřenou databázi [23].

Při analýze FMEA je vytvářena tabulka způsobů poruch zařízení a jejich dopadů na systém nebo podnik. FMEA identifikuje jednoduché způsoby poruchy, které buď přímo vedou k nehodě, nebo k ní významně přispějí. Není účinná, ale pro identifikování vyčerpávajícího seznamu kombinací poruch zařízení, které vedou k nehodám. Účelem této metody je identifikovat způsoby poruch jednotlivého zařízení a systému a potencionální dopad nebo dopady každého způsobu poruchy na systém nebo podnik. Tato analýzy typicky vytváří doporučení pro zvýšení spolehlivosti zařízení a tím také pro zlepšení bezpečnosti procesu [1].

8.2.4. Fault Tree Analysis – FTA (analýza stromu poruch)

Analýza stromu poruch je postup založený na systematickém zpětném rozboru událostí za využití řetězce příčin, které mohou vést k vybrané vrcholové události. Metoda FTA je graficko-analytická popř. graficko-statistická metoda. Názorné zobrazení stromu poruch představuje rozvětvený graf s dohodnutou symbolikou a popisem. Hlavním cílem analýzy metodou stromu poruch je posoudit pravděpodobnost vrcholové události s využitím analytických nebo statistických metod. Proces dedukce určuje různé kombinace hardwarových a softwarových poruch a lidských chyb, které mohou způsobit výskyt specifikované nežádoucí události na vrcholu [23].

Metoda používá logická hradla stromu poruch, které popisují vzájemné vztahy mezi vstupy a výstupy popsaných událostí. Účelem této metody je nalezení kombinací poruch zařízení a lidských chyb, které mohou vyústit v nehodu. Hodí se dobře pro analýzy velmi obšírných systémů [1].

8.2.5. Human Reliability Analysis – HRA (analýza lidské spolehlivosti)

Analýza lidské spolehlivosti je postup na posouzení vlivu lidského činitele na výskyt živelních pohrom, nehod, havárií, útoků apod. nebo některých jiných dopadů. Koncept analýzy lidské spolehlivosti HRA směřuje k systematickému posouzení lidského faktoru (Human Factors) a lidské chyby (Human Error). Ve své podstatě přísluší do zastřešující kategorie konceptu předběžného posuzování PHA. Zahrnuje přístupy mikroekonomické (vztah „člověk-stroj“) makroekonomické (vztah systému „člověk-technologie“). Analýza HRA má těsnou vazbu na aktuálně platné pracovní předpisy především z hlediska bezpečnosti práce. Uplatnění metody HRA musí vždy tvořit integrovaný problém bezpečnosti provozu

a lidského faktoru v mezních situacích různých havarijních scénářů, tzn. Paralelně a nezávisle s další metodou rizikové analýzy [1, 23].

Analýza lidské spolehlivosti je systematické hodnocení faktorů, které ovlivňují výkonnost operátorů, údržbářů, techniků a ostatního personálu podniku. Identifikuje situace náchylné k chybám nebo omylům, které mohou vést k nehodám, a může být také použita ke stopování příčin lidských chyb. Účelem analýzy lidské spolehlivosti je identifikovat potenciální lidské chyby a jejich dopady nebo identifikovat příčiny lidských chyb. Systematicky vyjmenovává chyby, které se mohou vyskytnout během normálního, abnormálního nebo nouzového provozu, faktory přispívající k takovým chybám a navrhované změny systému pro snížení pravděpodobnosti takových chyb [1].

8.2.6. Causes and Consequences Analysis – CCA (analýza příčin a dopadů)

Analýza příčin a dopadů je směs analýzy stromu poruch a analýzy stromu událostí. Největší předností CCA je její použití jako komunikačního prostředku: diagram příčin a dopadů zobrazuje vztahy mezi koncovými stavy nehody (nepřijatelnými dopady) a jejich základními příčinami. Protože grafická forma, jež kombinuje jak strom poruch, tak strom událostí do stejného diagramu, může být hodně detailní. Tato technika se používá obvykle nejvíce v případech, kdy logika poruch analyzovaných nehod je poměrně jednoduchá. Jak už napovídá název, účelem analýzy příčin a dopadů je odhalit základní příčiny a dopady možných nehod. Analýza příčin a dopadů vytváří diagramy s nehodovými sekvencemi a kvalitativními popisy možných koncových stavů nehod [1, 23].

8.3. Výpočetní technika a softwarová podpora analýz

V dnešní moderní době velkého rozvoje informačních technologií je k dispozici mnoho softwarových produktů, jejichž výsledkem je sestavení scénáře a hodnocení rizik. Všeobecně známých je asi patnáct. Provedení analýzy rizik bez použití výpočetní techniky a potřebného softwaru není v současné době možné a představitelné. Použití výpočetní techniky nám urychlí provedení analýzy rizik a zároveň nám slouží i k provedení simulace, včetně možnosti propojení s geografickými informačními systémy. Díky tomu můžeme přesněji stanovit rozsah postiženého území, včetně počtu obyvatelstva a rozsah způsobených škod, které vlivem mimořádné události vzniknou.

Softwarové produkty jsou založeny na fyzikálních modelech jednodušších nebo složitějších, což pochopitelně předurčuje lepší nebo horší správnost a spolehlivost výsledků. Většinu z existujícího software lze použít jen k hodnocení určitých typových případů [1, 23].

8.4. Analýza rizik a kritická infrastruktura

V předcházejících kapitolách je uvedeno několik metod k provádění analýz rizik. Samozřejmě, že existuje ještě celá řada metod k provádění analýzy rizik, a to jak v oblasti bezpečnosti informačních technologií, tak i v oblastech dalších. Metody pracují často s velice podobnou strukturou – objekty, ohrožení, slabá místa, pravděpodobnosti. Výsledkem metod je očekávaná výše škody nebo kategorizace rizik [1].

V oblasti kritické infrastruktury aplikace klasických metod analýzy rizik nevede vždy k žádoucímu cíli. Důvodem je to, že pro výpadky infrastruktur a pravděpodobnosti takových výpadků zatím není vypracována odpovídající statistika, není dohotovena katalogizace objektů, slabých míst a ohrožení. Pro analýzu rizik v kritické infrastruktuře byla vytvořena modifikací klasických metod analýzy rizik metoda na bázi posouzení kritičnosti [1].

Výchozím bodem u této metody jsou provozní procesy, které probíhají. V zájmu není prioritně to, kým anebo čím jsou funkční schopnosti těchto procesů ohroženy, ale pouze to, zda proces může být značně narušený nebo by mohl skončit výpadkem. U této analýzy se nepokládá otázka: ***„Jak/čím/kým může být narušen provoz?“***, ale naopak se pokládá otázka: ***„Jaké dopady bude mít v příslušném procesu to, že něco již nebude fungovat (pracovat)?“*** [1].

8.5. Metoda AKIS

Nástrojem k získání rychlého hodnocení jednotlivých sektorů infrastruktury je analýza kritických infrastruktur – metoda AKIS. Práce s touto metodou spočívá v tom, že se nejdříve vytvoří přehled o jednotlivých sektorech infrastruktury, které se dále rozčlení. Identifikují se kritické procesy a zhodnotí se kritičnost. Jednotlivé body s vysokou kritičností se dále posuzují na závislost na informačních technologiích. Po ukončení šetření jako výsledek vznikne matice kritičnosti [1].

V prvním kroku je nutné posuzovaný sektor zobrazit a ujasnit, jak sektor funguje, jak pracuje a jaký má význam pro ekonomiku, jaké vůdčí podniky v sektoru jsou. Sektory můžeme dále rozdělit na jednotlivá odvětví nebo služby. V obecné rovině je možné využít rovněž členění na produkty. Možná je i kombinace různých rozdělení. Po provedeném uspořádání sektoru je nutné pro jednotlivá odvětví nebo služby identifikovat a definovat provozní procesy. Tyto se pak v dalším stávají předmětem posuzování na kritičnost. Toto je velmi důležitý krok pro celkovou analýzu. Procesy, které nejsou zohledněny, nemají pro posuzování kritičnosti význam [1].

K identifikaci procesů jsou k dispozici různé pomůcky. Pokud se jedná o sektor s vysokým národohospodářským významem, je vhodné pracovat v součinnosti s experty. Důležitým předpokladem úspěšné analýzy kritičnosti je věrohodné zacházení s obdrženými informacemi [1].

V hodnocení kritičnosti je nejpodstatnější práce s odborníky. Pokud je to možné, dotazuje se více odborníků, mohou se tak zhodnotit různá subjektivní hodnocení. Aby mohlo být hodnocení srovnatelné je nutná existence možnosti výsledky analyzovat a srovnávat mezi jednotlivými sektory. Proto jsou pro očekávané dopady, tak i pro hodnocené pravděpodobnosti výpadků sestavovány různé několikastupňové škály, např. pro dopady/škody od „nevýznamné“ do „katastrofální“, pro pravděpodobnosti výpadku od „velmi řídký“ do „téměř jistý“. Následně kombinujeme dopad a pravděpodobnost výpadku což představuje kritičnost procesu. Podle hodnocení kritičnosti a provedení hodnocení výsledků anket experty můžeme jednotlivé procesy uspořádat do matice kritičnosti [1].

Na základě této metody nejsou výsledky dostatečně detailní, aby sloužily jako základ ke konkrétním opatřením. Metoda AKIS umožňuje získat rychlý přehled o kritické infrastruktuře a vytvořit tím dobré znalosti, které napomůžou k zachování spolehlivosti infrastruktury na bázi spolupráce mezi státem a hospodářstvím [1].

9. Ochrana kritické infrastruktury

Ochrana kritické infrastruktury je proces, který je zaměřen na takové zajištění fungování subjektů kritické infrastruktury a objektů, které tyto subjekty vlastní nebo provozují, tak aby nedocházelo k jejich selhání při zohlednění všech možných rizik a hrozeb. Smyslem ochrany kritické infrastruktury musí být minimalizace následků narušení funkcí, činností nebo služeb. Snahou je aby narušení bylo krátkodobé, málo četné, zvladatelné, byť provizorním způsobem a územně omezené tak, aby postihlo co nejmenší počet obyvatelstva.

V důsledku existence mezinárodní závislosti a provázání jednotlivých oblastí kritické infrastruktury může narušení kritické infrastruktury jedné oblasti ovlivnit další oblasti a může mít i mezinárodní dopady. Ochrana kritické infrastruktury vyžaduje sdílení odpovědností veřejné správy s privátním sektorem a výměnu informací mezi veřejnou správou a dalšími relevantními organizacemi a také mezinárodní spolupráci.

Vzhledem k tomu, že nefunkčnost kritické infrastruktury ve většině případů vyvolá minimálně situaci, která bude srovnatelná s mimořádnou událostí nebo v horším případě krizovou situací, je nutné navázat systém ochrany kritické infrastruktury na stávající systémy řešení těchto situací, a to především z pohledu veřejné správy. Jejím úkolem bude prosazovat národní a mezinárodní politiku, zpracovávat potřebnou legislativu a nařízení, předávání si informací s mezinárodními organizacemi, včetně vlád a soukromého sektoru, hodnocení hrozeb a zranitelnosti, opatření krizového plánování a řízení, stanovení finančního zatížení pro soukromý sektor.

Ochranu kritické infrastruktury však nelze realizovat bez dodavatelů výrobků a služeb ze státního, ale i soukromého sektoru, to je subjektů kritické infrastruktury, které by měly sehrávat rozhodující úlohu při narušení své ekonomické činnosti a při hledání cest, jak náhradním nebo provizorním způsobem zabezpečit základní životní potřeby obyvatelstva.

Povinnost právnických osob a podnikajících fyzických osob zařazených mezi subjekty kritické infrastruktury konat opatření k zajištění ochrany kritické infrastruktury je tudíž zásadní podmínkou pro úspěšné řešení krizové situace způsobené narušením kritické infrastruktury. Jde zejména o to, aby opatření stanovená rezorty odpovědnými za danou oblast kritické infrastruktury byla akceptována příslušnými subjekty a realizována na objektech kritické infrastruktury. Tyto subjekty by měly povinnost zpracovat stanovenou dokumentaci ochrany kritické infrastruktury a zabezpečit realizaci opatření, která z ní vyplývají.

Úkolem státního a zejména soukromého sektoru je naplnění státní politiky, hodnocení vlastní zranitelnosti a závislosti, opatření krizového plánování a řízení, rozdělení odpovědností, výměna informací s vládou a dalšími organizacemi.

Propojený systém legislativních, organizačních a technických opatření prováděných veřejnou i soukromou sférou v oblastech kritické infrastruktury, umožní za krizové situace zabezpečit základní životní podmínky a potřeby obyvatelstva [3].

10. Nouzové služby

Jednou z oblastí kritické infrastruktury jsou Nouzové služby, které řadíme do infrastruktury sociálně-ekonomických služeb. Subjekty této oblasti jsou:

- Hasičský záchranný sbor České republiky a příslušné jednotky požární ochrany,
- Policie České republiky (vnitřní bezpečnost a veřejný pořádek),
- Armáda České republiky (zabezpečení obrany),
- radiační monitorování včetně podkladů pro rozhodování o opatřeních vedoucích ke snížení nebo odvrácení ozáření,
- předpovědní, varovná a hlásná služba.

Tyto subjekty byly zařazeny do kritické infrastruktury hlavně z toho důvodu, že slouží veřejnosti a jejich hlavním úkolem mimo jiné je chránit obyvatelstvo, jejich zdraví, život a majetek.

Cílem diplomové práce je navrhnout možné způsoby ochrany subjektů a objektů kritické infrastruktury. Rozhodl jsem se pro oblast Nouzové služby a pro navržení ochrany zvolil subjekt Policii České republiky. Důvod pro tento výběr je, jak jsem uvedl v úvodu diplomové práce, že v současné době jsem ve služebním poměru u Policie České republiky.

Než se budu podrobněji zabývat vybranou analýzou rizik, jejím vyhodnocením a návrhem ochrany kritické infrastruktury vybraného subjektu, uvedu v následujícím textu několik údajů o Policii České republiky a vysvětlím význam pojmu „vnitřní bezpečnost a veřejný pořádek“, které je uvedeno v závorce jako druhotné u tohoto subjektu.

Je nutné odlišovat od sebe pojem vnitřní bezpečnost a veřejný pořádek. Tento pojem je spíše častěji definován např. jako ochrana ústavního zřízení, práv a svobod nebo bezpečnosti osob a majetku [28].

10.1. Policie České republiky

Policie České republiky je součástí státního mechanizmu a je zřízena v poměrech právního řádu České republiky jako jednotný ozbrojený bezpečnostní sbor České republiky s působností na celém území republiky.

Pojem policie vychází z řeckého slova „polis“ (znamená město nebo městský stát). Policie České republiky vznikla v roce 1991 přeměnou Veřejné bezpečnosti. Důvodem změny v označení názvu byl rozpad socialistického státu na konci roku 1989 a vzniku státu

demokratického v roce 1990. Při výběru označení se navázalo na předválečné československé pozitivní právo, používané až do roku 1945.

Policie České republiky je podřízena Ministerstvu vnitra České republiky. V čele Policie České republiky stojí policejní prezident Policejního prezídia České republiky, který řídí činnost Policie České republiky a zároveň odpovídá za činnost Policie České republiky ministrovi vnitra. Ministr vnitra policejního prezidenta jmenuje a odvolává.

Základem činnosti Policie České republiky je:

- ochrana celospolečenských zájmů a hodnot, zejména zákonnosti a veřejného pořádku, státu, ústavních základů a institucí, zabezpečení nerušeného výkonu funkce všech orgánů moci zákonodárné, výkonné a soudní,
- ochrana fyzických osob, jejich životů, zdraví, lidské důstojnosti,
- ochrana majetku, a to bez rozdílu jeho vlastníků [26].

Policie České republiky v rámci plnění svých úkolů dále spolupracuje:

- s ozbrojenými silami (Armáda České republiky, Vojenská kancelář prezidenta republiky, Hradní stráž),
- s ozbrojenými bezpečnostními sbory (policie, Celní správa České republiky, Vězeňská služba České republiky, Bezpečnostní informační služba, Úřad pro zahraniční styky a informace, Vojenská policie a Vojenské zpravodajství),
- s dalšími orgány veřejné správy a právnickými a fyzickými osobami.

V rámci integrovaného záchranného systému je nejdůležitější spolupráce se záchrannými sbory a havarijními službami.

Policie České republiky je rozdělena na jednotlivé služby, které odpovídají za plnění svých úkolů. Služby mezi sebou vzájemně spolupracují a jedná se o tyto služby [26]:

1. **Služba kriminální policie a vyšetřování** – funguje na územních odborech (bývalý okres), na krajských ředitelstvích, na útvarech s celostátní působností a na Policejním prezidiu. Zabývá se prověřováním a vyšetřováním většiny trestných činů, provádí operativně pátrací činnost, kriminalisticko-technickou činnost a řídí a organizuje plnění úkolů na úseku pátrání po osobách a věcech.
2. **Služba pořádkové policie** – funguje na základních útvarech policie, tzv. obvodní oddělení policie a na úrovni krajských ředitelství. Provádí ochranu veřejného pořádku, šetří přestupky na úseku veřejného pořádku a občanského soužití, předchází

a odhaluje trestnou činnost menší závažnosti, prověřuje drobnou trestnou činnost a provádí hlídkovou a obchůzkovou službu.

Služba pořádkové policie má i specializované útvary, kterými zajišťuje výkon potápěčských prací, výkon služební kynologie a hypologie. Dalšími specializovanými útvary jsou Pořádkové jednotky, Zásahové jednotky a Útvar rychlého nasazení.

Pořádkové jednotky – jsou určené hlavně k ochraně bezpečnosti osob, majetku a veřejného pořádku při hromadných akcích – shromáždění, pod jednotným velením. Lze je využít i při plnění úkolů integrovaného záchranného systému při mimořádných událostech, které vyžadují nasazení většího počtu sil a prostředků Policie České republiky. Fungují jako stálé pořádkové jednotky v Praze, Brně, Ostravě a Ústí nad Labem a jako nestálé pořádkové jednotky v ostatních krajích.

Zásahové jednotky a Útvar rychlého nasazení – jsou určené hlavně k provádění zákroků proti teroristům, nebezpečným pachatelům nebezpečné trestné činnosti a závažných úmyslných trestných činů, únoscům osob a dopravních prostředků. Lze je taky použít k ochraně nebo obnovení veřejného pořádku, tak jak pořádkové jednotky. Zásahové jednotky fungují zatím na osmi krajských ředitelstvích a v budoucnu budou zřízeny i na nově vzniklých šesti krajských ředitelství. Útvar rychlého nasazení je celostátním útvarem.

3. **Služba dopravní policie** – funguje na základních útvarech policie a na úrovni krajských ředitelství. Provádí výkon dozoru nad silničním provozem, kde šetří a projednává dopravní přestupky, provádí šetření a dokumentaci dopravních nehod a plní úkoly na úseku dopravního inženýrství. Služba dopravní policie se využívá k zabezpečení doprovodů vozidel a kolon.
4. **Služba pro zbraně a bezpečnostní materiál** – funguje na krajských ředitelstvích s rozmístěním po územních odborech a na Policejním prezídiu. Zajišťuje úkoly na úseku střelných zbraní a střeliva, výbušnin, obchodu se zbraněmi, vojenským materiálem a bezpečnostním materiálem. Jedná se o administrativní činnost a kontrolní činnost v této oblasti.
5. **Služba cizinecké policie** – tvoří jeden útvar s celostátní působností. Věnuje se kontrole dodržování pobytového režimu cizinců, provádí pátrání po osobách, které se nelegálně zdržují na území České republiky. Prošetřuje přestupky na úseku pobytového režimu cizinců, šetří přeshraniční trestnou činnost k nedovolenému překračování státních hranic apod.

6. **Ochranná služba** – tvoří dva útvary s celostátní působností, a to: útvar pro ochranu ústavních činitelů a útvar pro ochranu prezidenta České republiky. Z toho vyplývá, že úkolem této služby je zajišťovat ochranu ústavních činitelů včetně prezidenta a bezpečnost chráněných osob při pobytu na území České republiky v rámci mezinárodních dohod. Mimo to zajišťují ochranu objektů a prostorů, které určí vláda na návrh ministra vnitra a objekty, jejichž ochrana vyplývá z mezinárodní dohody, kterou je Česká republika vázána.
7. **Letecká služba** – je to útvar s celostátní působností, který za pomoci vrtulníků provádí podporu pátrání po pohřešovaných osobách, podporuje akce speciálních útvarů, při dopravních akcích, bezpečnostních akcích a akcích ostatních služeb policie. Je možné ji použít v rámci integrovaného záchranného systému a pro účely zdravotnické záchranné služby nebo při pomoci hasičskému záchrannému sboru např. při hašení požárů.
8. **Pyrotechnická služba** – je to útvar s celostátní působností s pobočkami na území České republiky. Úkolem pyrotechnické služby jsou likvidace veškeré nalezené munice a nástražných výbušných systémů.
9. Z hlediska krizového řízení je u Policie České republiky zřízeno mimo jiné i **oddělení krizového řízení**, které funguje na krajských ředitelstvích s rozmístěním po územních odborech a na Policejním prezidiu.
10. U Policie České republiky existují další služby, tzv. servisní složky, které zajišťují provoz a činnost policie. Jedná se např. o Oddělení informačních a komunikačních technologií, Preventivní informační skupina, Ochrana utajovaných informací, Oddělení vnitřní kontroly, Oddělení technické ochrany, Ekonomické oddělení, Oddělení pro řízení lidských zdrojů, Oddělení ochrany objektů a další. Jsou to útvary, které fungují na Policejním prezídiu a krajských ředitelstvích s rozmístěním detašovaných pracovišť po územních odborech.

10.2. Veřejný pořádek

Veřejný pořádek patří mezi tzv. neurčité pojmy správního práva. Ačkoli není v žádném právním předpisu definován, operuje s ním celá řada právních norem. Obvykle je jím míněn ideální stav společnosti, který se vyznačuje řádem, bezpečností a klidem – takovou definici však v právní normě použít nelze, protože jde fakticky o definici kruhem. K ochraně veřejného pořádku jsou příslušné v prvé řadě policie, státní i obecní, a orgány obcí [27].

Veřejný pořádek je ukotven v ustanovení § 2 zákona o policii [29]. Veřejný pořádek je součástí vnitřního pořádku. Jedná se o pravidla chování na veřejnosti, která jsou stanovena právním předpisem a pravidla soužití, která nejsou právně formulovaná. Z toho vyplývá, že veřejný pořádek je stav, kdy jsou tato pravidla zachována, ale tento stav není ve společnosti možné absolutně docílit. Proto je ve veřejném zájmu tento stav chránit.

10.3. Vnitřní pořádek a bezpečnost

Je třeba si uvědomit, že pojem vnitřní pořádek a bezpečnost, je často zaměňován s pojmem veřejný pořádek, veřejná bezpečnost nebo veřejné zdraví. Jde o záležitosti týkající se opatření legislativních, organizačních a věcných, pokud to vyžaduje zájem ochrany bezpečnosti (vnitřní a vnější) nebo veřejného pořádku.

Vnitřní pořádek a bezpečnost se interpretuje různě. Prakticky neexistuje shoda mezi pojmem vnitřní bezpečnost a pojmem vnitřní pořádek, tak jak se používá vazba „… bezpečnost a vnitřní pořádek“. Vnitřní pořádek zahrnuje veřejný pořádek a bezpečnost osob a majetku. Zatím co vnitřní bezpečnost zabezpečuje podstatné náležitosti demokratického právního státu.

10.4. Úkoly Policie České republiky

Policie České republiky plní úkoly ve věcech veřejného pořádku a bezpečnosti a další úkoly v rozsahu jak stanoví zákony. Mimo jiné plní také úkoly v rámci integrovaného záchranného systému při mimořádných událostech a krizových situacích. Přesto těžištěm činnosti Policie České republiky je plnění úkolů v bezpečnostním systému ve spolupráci s orgány činných v trestním řízení, ostatních bezpečnostních složek, zpravodajských služeb apod. [26].

Jedná se zejména o tyto úkoly v oblasti veřejného pořádku a bezpečnosti:

- chrání bezpečnost osob a majetku,
- spolupůsobí při zajišťování veřejného pořádku, a byl-li porušen, činí opatření k jeho obnovení,
- vede boj proti terorismu,
- odhaluje trestné činy a zajišťuje jejich pachatele,
- koná vyšetřování a vyhledávání o trestných činech,
- zajišťuje ochranu státních hranic ve vymezeném rozsahu,

- zajišťuje ochranu státních ústavních činitelů České republiky a bezpečnost chráněných osob, kterým je při jejich pobytu na území České republiky poskytována osobní ochrana podle mezinárodních dohod,
- zajišťuje ochranu zastupitelských úřadů a ochranu objektů zvláštního významu,
- dohlíží na bezpečnost a plynulost silničního provozu a spolupůsobí při jeho řízení,
- odhaluje přestupky, a pokud tak stanoví zvláštní zákon, přestupky objasňuje,
- projednává přestupky, pokud tak stanoví zvláštní zákon,
- vede evidence statistiky potřebné k plnění svých úkolů,
- vyhlašuje celostátní pátrání, přitom je oprávněna zveřejňovat údaje nezbytné k identifikaci hledaných osob,
- získává, soustřeďuje a vyhodnocuje informace sloužící ochraně ekonomických zájmů České republiky,
- na základě vyrozumění orgány vězeňské služby České republiky provádí úkony související s bezprostředním pronásledováním osob, které uprchly z výkonu vazby nebo z výkonu trestu odnětí svobody,
- vyhledává a zadržuje svěřence uprchlé z nařízené ústavní nebo ochranné výchovy,
- plní úkoly státní správy,
- plní úkoly při ochraně místních záležitostí veřejného pořádku [30].

Úkoly Policie České republiky při mimořádných událostech:

- uzavření místa zásahu, zakázání vstupu na určená místa,
- záchrana bezprostředně ohrožených osob, zvířat, majetku nebo evakuace,
- regulace volného pohybu osob a dopravy v místě zásahu a přilehlému okolí,
- poskytování nutných informací příbuzným osobám a hromadným sdělovacím prostředkům,
- dokumentování údajů a skutečností za účelem zjišťování a objasňování příčin vzniku mimořádné události [30].

11. Analýza rizik posuzovaného subjektu

Analýzou rizik se snažíme zkoumat, čím a jak hluboce může být funkčnost posuzovaného subjektu narušena. Cílem je nalezení takových opatření, která zajistí při vzniku mimořádné události posuzovaný subjekt funkční co nejdéle, jak jen to bude možné.

Jak už bylo v předchozích kapitolách zmíněno, v rámci provádění analýzy rizik u subjektů kritické infrastruktury se pokládá otázka, jaké dopady bude mít v příslušném procesu to, když posuzovaný subjekt nebude moci fungovat, vyrábět, pracovat atd. Pokud se jedná o Policii České republiky, znamenalo by to, že by nemohla vykonávat svou činnost v rámci zajištění veřejného pořádku a bezpečnosti a plnění dalších úkolů v rozsahu jak stanoví zákony a mezinárodní dohody.

Aby k takovéto situaci došlo, muselo by být ve stejný den, hodinu, minutu, sekundu, znemožněno plnění úkolů Policii České republiky na celém území státu. V rámci rozmístění služeb policie a útvarů na území státu se jeví tato možnost málo pravděpodobná. Více jako pravděpodobné se jeví znemožnění plnění úkolů na jednotlivých útvarech Policie České republiky s územní působností.

11.1. Metoda Check list

Pro provedení analýzy rizik jsem vybral metodu Check list (kontrolní seznam). Vybranou analýzou budu hodnotit Policii České republiky jako komplexní celek na území kraje nebo územního odboru. K sestavování otázek do kontrolního seznamu jsem napřed stanovil hlavní otázku ***„Zda je Policie České republiky jako subjekt kritické infrastruktury schopna plnit úkoly ve věcech veřejného pořádku a bezpečnosti a další úkoly v rozsahu jak stanoví zákony, součinnostní a mezinárodní dohody, pokud dojde k narušení (ohrožení) její funkčnosti při:“***.

Tabulka 2: Kontrolní seznam

Je Policie České republiky schopna plnit úkoly ve věcech veřejného pořádku a bezpečnosti a další úkoly v rozsahu jak stanoví zákony, součinnostní a mezinárodní dohody, pokud dojde k narušení (ohrožení) její funkčnosti při:				**ANO**	**NE**	**Nutné další údaje**
Vnitřní rizika						
1.	Výpadku dodávek energií	elektrické energie (black out)	krátkodobý? (< 2 hodin)	**X**		
			dlouhodobý? (> 2 hodiny)		**X**	
		plynu	krátkodobý? (< 12 hodin)	**X**		
			dlouhodobý? (> 12 hodin)		**X**	
		tepla	krátkodobý? (< 12 hodin)	**X**		
			dlouhodobý? (> 12 hodin)		**X**	
		pohonné hmoty (dále jen „PHM“)	krátkodobý? (< týden)	**X**		
			dlouhodobý? (> týden)		**X**	
2.	Výpadku dodávky vody		krátkodobý? (< 24 hodin)	**X**		
			dlouhodobý? (> 24 hodin)		**X**	
3.	Kolapsu počítačových sítí		krátkodobý? (< 1 hodiny)		**X**	
			dlouhodobý? (> 1 hodina)		**X**	
4.	Technické poruchy	sítí mobilních operátorů	krátkodobý? (< 3 hodin)	**X**		
			dlouhodobý? (> 3 hodiny)		**X**	
		radiokomunikační sítě (PEGAS)	krátkodobý? (< 3 hodin)	**X**		
			dlouhodobý? (> 3 hodiny)		**X**	
5.	Nedostatek náhradních dílů		krátkodobý? (< týden)	**X**		
			dlouhodobý? (> týden)		**X**	

Je Policie České republiky schopna plnit úkoly ve věcech veřejného pořádku a bezpečnosti a další úkoly v rozsahu jak stanoví zákony, součinnostní a mezinárodní dohody, pokud dojde k narušení (ohrožení) její funkčnosti při:			**ANO**	**NE**	**Nutné další údaje**
Vnější rizika					
6.	Narušení objektu kritické infrastruktury z důvodu	živelní pohromy?	**X**		
		průmyslové havárie?	**X**		
7.	Narušení objektu kritické infrastruktury způsobené člověkem	teroristický útok?	**X**		
		kriminální čin?	**X**		
		válečný stav?	**X**		
8.	Nedostatek pracovních sil	úbytek? (> 50 %)		**X**	
		zvýšená nemocnost (pandemie, infekční onemocnění, apod.)? (> 50 %)		**X**	
		odmítnutí služby? (> 50 %)		**X**	

11.2. Vyhodnocení kontrolního seznamu

Hodnoty z kontrolního seznamu vložíme pro přehlednost do tabulky:

Tabulka 3: Vyhodnocení otázek

název	**počet**
Sumarizace celkového počtu otázek $\sum C_{ot}$	26
Sumarizace součtu všech kladných odpovědí $\sum S_{klo}$	13
Sumarizace součtu všech záporných odpovědí $\sum S_{zo}$	13
Sumarizace součtu všech odpovědí nutné další údaje $\sum S_{nduo}$	0

Dalším krokem bude vyhodnocení kontrolního seznamu provedením součtu všech kladných odpovědí, vyjádřené v %.

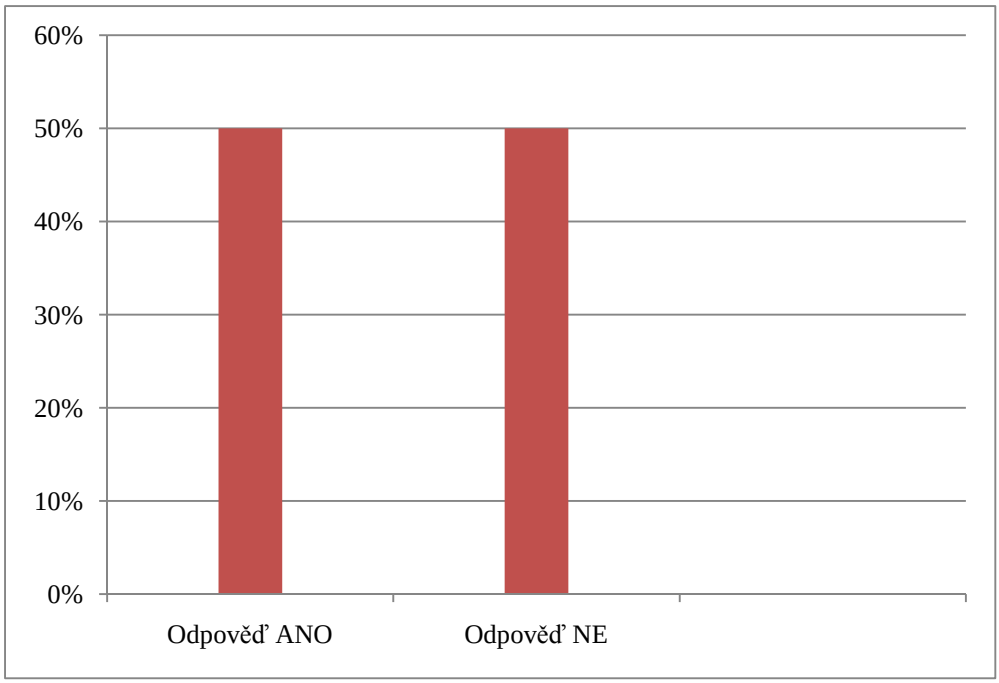
Pro výpočet součtu všech kladných odpovědí v % vycházím z následujícího vzorce:

$$S_{klo} = (\sum S_{klo} / \sum C_{ot}) \cdot 100\ [\%] \qquad (1)$$

Kde S_{klo} součet všech kladných odpovědí

Dosazení do vzorce (1): $S_{klo} = (\sum S_{klo} / \sum C_{ot}) \cdot 100 = (13/26) \cdot 100 = 50\ \%$

Pro názornější zobrazení výsledků, jsem procentuálně vypočítal i záporné odpovědi a vypočítané výsledky společně pak zobrazil v grafu:



Obr. 2: Hodnoty odpovědí v procentech

Podle tabulky s hodnotícími kritérii, viz tab. 8 [1], se zjistí stav hodnocení sledovaného kritéria subjektu kritické infrastruktury.

Tabulka 4: Hodnotící kritéria

Kladné odpovědi v %	Hodnocení sledovaného kritéria
95 a více	výborný
70 – 94	velmi dobrý
50 – 69	dobrý
20 – 49	špatný
do 20	velmi špatný / kritický

Z výsledku analýzy kontrolního seznamu vyplývá, že subjekt Policie České republiky díky 50 % kladných odpovědí se zařadil do sledovaného kritéria **„dobrý“**. Z toho vyplývá, že subjekt podle výsledků by měl při ohrožení uvedenými riziky problém plnit úkoly ve věcech veřejného pořádku a bezpečnosti a další úkoly v rozsahu jak stanoví zákony. Musíme vzít ale v úvahu, že by rizika musela nastat najednou a mít dlouhodobé trvání. K výsledku 50 % kladných odpovědí musíme přistupovat s opatrností.

Musíme si uvědomit, že plnění úkolů by bylo ovlivněno nefungováním techniky nebo nemožností užívání areálů, ve kterých policie sídlí a techniku užívá. Činnost v terénu by byla ohrožena částečně. Nefungovalo by spojení, nepoužívaly by se služební dopravní prostředky, ale dohled nad veřejným pořádkem a bezpečností by se i přes tyto problémy vykonával s využitím náhradních prostředků. V krajním případě by se způsob činnosti policie vrátil do doby, kdy moderní technika byla teprve v počátcích a policie vykonávala svou činnost manuálně.

Při sestavování souboru otázek v kontrolním seznamu jsem vycházel z rizik, která nejvíce mohou ohrožovat kritickou infrastrukturu daného subjektu. Přesto jsem soubor otázek konzultoval s kolegy odborníky, abych se vyhnul subjektivnímu pohledu a ověřil si tak správnost otázek. Z toho vyplývá, že i v praxi při tvorbě jakéhokoliv kontrolního seznamu nebude tento seznam vypracovávat jednotlivec, ale bude na něm pracovat tým tvořený z odborníků pracujících v zainteresovaných oblastech nebo jim příbuzných. Ti tak do sestavování souboru otázek kontrolního seznamu vnesou své kvalifikované názory i cenné

zkušenosti. Tím dojde k podrobnějšímu rozpracování otázek a získání tak konkrétnějších odpovědí na dané otázky. To povede ke zpřesnění a zkvalitnění výsledku analýzy rizik.

12. Ochrana posuzovaného subjektu

Cílem zajištění základní ochrany je dosáhnout snížení zranitelnosti subjektu kritické infrastruktury před riziky, která tento subjekt ohrožují. Rizika úplně eliminovat anebo alespoň zmírnit jejich dopad. Proto se musíme zaměřit na rizika, která znemožní subjektu Policie České republiky plnit úkoly ve věcech veřejného pořádku a bezpečnosti a další úkoly v rozsahu jak stanoví zákony.

K tomu si musíme stanovit cíle a potřeby ochrany kritické infrastruktury. Určíme systém cílů (hlavní cíl, cíle ochranné a cíle pro postupy).

Hlavní cíl – je minimalizace výpadku fungování Policie České republiky.

Cíle ochranné – zajištění činnosti Policie české republiky před výpadkem dodávek potřebných pro výkon policie, např. zabránění výpadku energií.

Cíle pro postupy – určují nám možné změny a opatření k zajištění fungování Policie České republiky při jednotlivých ohroženích, např. opatření ke zvýšení spolehlivosti náhradního zdroje elektrické energie – přezkoumání, co vše je na něho připojeno, zda není potřeba zvýšit jeho kapacitu, umístění zdroje v objektu pro jeho ochranu, zajištění zásob PHM, apod.

Z vyhodnocení odpovědí kontrolního seznamu zjistíme, jaká rizika nejvíce ohrožují činnost policie. Tyto informace získáme ze záporných odpovědí, na základě kterých jsme dále schopni stanovit, které situace jsou nejhorší. Z vyhodnocení záporných odpovědí vyplývají tato rizika:

1. dlouhodobý výpadek dodávek energií – elektrické energie, plynu, tepla a PHM,
2. dlouhodobý výpadek dodávky vody,
3. kolaps počítačových sítí,
4. dlouhodobé technické poruchy sítí – mobilních operátorů a radiokomunikační (PEGAS),
5. dlouhodobý nedostatek náhradních dílů,
6. nedostatek pracovních sil, pokud by klesl pod 50 % skutečného stavu.

Z těchto rizik vyplývá, že nejhorší pro Policii České republiky je dlouhodobý výpadek elektrické energie, následně kolaps počítačových sítí a výpadek radiokomunikační sítě. Jelikož jsou tyto oblasti mezi sebou propojeny, protože jsou závislé na dodávce elektrické energie, může dojít k dominoefektu.

Rozhodující význam pro snížení rizik a tím hrozby vyřazení Policie České republiky z plnění jejich úkolů je cílené zlepšení odolnosti vůči rizikům. Proto se zaměříme hlavně na výše uvedené rizika. Budou-li se rizika systematicky omezovat a odstraňovat, zvýší se tím významně ochrana Policie České republiky. Kromě přípravy na možná ohrožení má zásadní význam snížení zranitelnosti Policie České republiky při výpadku dodavek energií, hlavně elektrické energie a kolapsu počítačových sítí.

12.1. Výpadek dodávky energií

12.1.1. Elektrická energie

Výpadek dodávky elektrické energie patří mezi jedno z nejhorších rizik, protože fungování řady pracovišť naruší již drobné výpadky elektrické energie. Ochranu proti výpadku elektrické energie rozdělujeme na vnitřní a vnější.

Vnitřní ochrana proti přerušení dodávky elektrické energie (např. odpojením nebo poškozením přípojných míst, rozvaděčů, apod.) spočívá v zabezpečení areálů a to fyzickou ostrahou, technickými prostředky a režimovými opatřeními. K tomuto zabezpečení má policie zpracovanou dokumentaci bezpečnostní ochrany areálů a režimových prostorů.

Vnější ochrana je složitá, protože Policie České republiky se nemůže bránit proti výpadkům dodávek elektrické energie z distribuční soustavy, ale musí být na tyto výpadky připravena. Proto je v areálech policie podle významu důležitosti navržen a pořízen náhradní zdroj elektrické energie, jako např. dieselagregáty, přenosné elektrocentrály nebo záložní baterie.

Doporučení: v současnosti je potřeba vzhledem k nárůstu elektronických a elektrických zařízení, potřebných k činnosti policie přezkoumat, zda náhradní zdroje mají dostatečnou kapacitu nebo je potřeba jejich kapacitu navýšit. A s ohledem na mimořádné události, hlavně povodně je potřeba přehodnotit umístění náhradních zdrojů v areálech. Dále je důležité provádět jejich pravidelnou kvalitní údržbu a mít zajištěné ve formě zásob dostatečné množství PHM podle požadované délky doby výroby náhradní elektrické energie.

12.1.2. Plyn a teplo

V případě výpadku dodávek plynu nebo tepla, které se využívá k vytápění areálů policie, rozdělujeme ochranu na vnitřní i vnější jako při výpadku dodávek elektrické energie. **Doporučení:** uvážit hlavně z důvodu financí a skladování, zda není vhodné nakoupit náhradní zdroje tepla, např. přenosné přímotopy.

12.1.3. Pohonné hmoty

Policie České republiky má v některých areálech vybudovány vlastní čerpací stanice s určitým množstvím PHM v zásobnících. Ochrana těchto areálu je prováděna fyzickou ostrahou, technickými prostředky a režimovými opatřeními. K ochraně areálu má zpracovanou dokumentaci bezpečnostní ochrany. Dojde-li k výpadku dodávek PHM, je pro tento případ zpracován Plán ropné nouze, který je součástí krizového plánu a postupovalo by se v souladu s tímto plánem.

Doporučení: provádět pravidelnou údržbu a kontrolu čerpacích stanic. Včas doplňovat zásobníky PHM. Případně uzavřít smlouvu o dodávkách PHM v souladu se zákonem o hospodářských opatřeních pro krizové stavy [8].

12.2. Výpadek dodávky vody

Voda je jedna z nejdůležitějších životních potřeb lidí a zvířat. U Policie České republiky se používá jako voda pitná, pro mytí včetně sprchování a úklidu ploch. Proto musí být dodávána v předepsané kvalitě nepřetržitě a pod požadovaným tlakem. V případě poruchy lze akceptovat nižší kvalitu vody, nesmí být ovšem zdraví škodlivá.

Výpadek dodávek vody může mít různé příčiny:

- nedostatek vody nebo nízký tlak ve vodovodním systému (přerušené vedení, porucha čerpadel, extrémní vedro a sucho),
- znečistění mikroorganismy nebo chemikáliemi (je možno ji používat jako spotřební např. pro WC).

Příčiny výpadku dodávek vody mohou být externí nebo interní.

U **interních příčin** stojí za pozornost kontaminace vody bakteriemi, viry či houbami. Ke kontaminaci může dojít při chybně provedené instalaci, použitím nevhodných materiálů, zvýšením teploty studené vody značně nad 20^{o} C, u nepravidelně využívaných částí vodovodu se stojící vodou, při špatně provedených zkouškách těsnění, nedodržením předpisů při zavádění do provozu atd.

Při výpadku dodávek vody z **externích příčin** závisí reakce na situaci, na prostorovém a časovém rozsahu události. Při běžném provozu je dodávka vody zajištěna dodavatelem. Její přerušení např. kvůli poruše potrubí nepřesáhne obvykle několik hodin. Pokud by došlo k místnímu narušení kvality pitné vody tak, že dodávaná voda by byla pouze spotřební

kvality, bylo by policie upozorněna dodavatelem nebo sdělovacími prostředky. Přechodné zásobování by bylo zajištěno dodavatelem např. pomocí cisteren.

Doporučení: aby nedocházelo k častým poruchám na vodovodním potrubí rozvodů v areálech, je potřeba aby správci areálů zajistili přezkoumání stavu vodovodních potrubí v areálech a případně navrhli a naplánovali jejich výměnu. Při dlouhodobém výpadku dodávky pitné vody zajistit dodávku vody např. pomocí cisteren nebo nákupem balené vody. Pro zajištění hygieny a sociálních zařízení stačí zajistit dodávku užitkové vody např. pomocí cisteren.

12.3. Kolaps počítačových sítí

Informační technologie v současnosti patří k nejdůležitějším potřebám pro činnost Policie České republiky. Veškerá administrativní činnost a nejen ta se provádí výhradně v elektronické podobě a za využití informačních systémů. Data jsou ukládána na serverech s velkým objemem dat. Proto je velmi důležité věnovat bezpečnosti počítačů, serverů s daty a počítačových sítí velkou pozornost. Současně by mělo být stanoveno, jaká je skutečná závislost na informačních technologiích a zda při jejich výpadku nebo ztrátě dat může policie vůbec fungovat.

Policie České republiky používá vlastní vnitřní počítačovou síť oddělenou od veřejné sítě, tím je dostatečně zabezpečena ochrana dat a informačních systémů. Z toho vyplývá, že nemůže dojít k útoku hackerů, ke špionáži a zneužití dat. Nelze ovšem dobře ochránit výpadek informačních technologií vlivem lidského selhání nebo z důvodu závady na hardwaru nebo výpadku softwaru. Také není možné zabránit úniku dat ztrátou nebo jejich vynesením na přenosných discích nebo médiích a následné zneužití.

Ochrana počítačových sítí, serverů a hardwarů u policie je řešena v dokumentaci bezpečnostní ochrany areálu a režimových prostorů. Přesto, že policie používá svou vnitřní počítačovou síť, má nainstalovány ve výpočetní technice ochranné softwary z důvodu používání přenosných disků, ze kterých hrozí přenos virů, trojských koňů, apod. Dále je jednotlivá výpočetní technika zabezpečena heslem, které zná pouze uživatel této výpočetní techniky, v rámci používání výpočetní techniky má uživatel omezena oprávnění, aby nemohl instalovat jiný software a odinstalovávat součásti z výpočetní techniky. Výpočetní technika připojená ne vnitřní síť nesmí být nikdy připojena na síť veřejnou. Pro připojení na veřejnou síť se používá samostatná výpočetní technika, která neobsahuje žádná data, pouze operační software a internetový prohlížeč s omezeným oprávněním.

Přístup do místností k serverům mají pouze oprávněné osoby, které provádí pravidelné zálohování dat a údržbu a tyto místnosti jsou zabezpečeny technickými prostředky a režimovým opatřením.

Doporučení: je třeba uvažovat o zachování základních podkladů v papírové podobě. Zvážit zda nezůstanou zachovány evidence v papírové podobě, spisy, apod. Zachovat papírové tiskopisy (např. pro provedení výslechu, podání vysvětlení, apod.), z důvodu výpadku výpočetní techniky, serveru, při přetížení sítě nebo výpadku elektrické energie. Zabránit přetížení počítačové sítě přezkoumáním její dostatečné kapacity a rychlosti. Aktualizovat pravidelně softwary a pravidelně zálohovat data. Průběžně přizpůsobovat technické zařízení vývojovému trendu. V rámci organizačního opatření pravidelně školit uživatele výpočetní techniky z jejího užívání, zacházení s daty, hlavně na přenosných discích a médiích. Pravidelné obměňování přístupových hesel.

12.4. Technické poruchy

12.4.1. Mobilní síť

Zajištění ochrany mobilních sítí operátorů, je v povinnostech provozovatelů a vlastníků těchto sítí. Pokud dojde k výpadku mobilních sítí, musí policie najít řešení v rámci svých možností, jak nahradit spojení na mobilní telefony jiným způsobem.

Doporučení: při výpadku mobilní sítě použít vlastní radiokomunikační síť. Pokud nelze radiokomunikační síť požít, zajistit předání informací např. spojkou.

12.4.2. Radiokomunikační síť

Zajištění ochrany radiokomunikační sítě (PEGAS) bylo provedeno v rámci návrhu této sítě, která je dostatečně bezpečná. Radiokomunikační síť není možné odposlouchávat a je maskovaná. Pokud dojde ke ztrátě radiostanice a podá se včas informace na dohledové pracoviště, dokáže ji na dálku zničit. Radiokomunikační síť a radiostanice jsou chráněny pravidelně se měnícími klíči v určených cyklech, jinak nebudou fungovat. Pokud radiostanice není naprogramována na správný klíč, nemůže se zaregistrovat na buňkách a tím je vyřazena ze systému. Špatné spojení není kolikrát zaviněno výpadkem radiokomunikační sítě, ale chybou obsluhy radiostanice – lidské selhání. Dalším důvodem je i špatné vykrytí buněk signálem na některých územích, hlavně horských a špatně přístupných terénů.

Doporučení: jedná se především o organizační opatření, např. ztráta radiostanice, její správná obsluha, údržba, apod. Vzdělávat policisty v obsluze radiostanice, aby se odstraňovaly chyby v její obsluze. Zajistit vykrytí hluchých míst výstavbou nových buněk.

12.5. Nedostatek náhradních dílů

Fungování policie závisí na zásobování materiálem a dalších službách. Také tyto dodávky a služby musí být prověřeny z hlediska analýzy rizik. Je třeba prověřit celý logistický řetězec dodávek materiálu od výrobců až po jednotlivá pracoviště.

Externí dodavatelé mohou znamenat v krizové situaci problém. Proto je třeba pro tyto situace stanovit podmínky a zajistit fungování těchto služeb (také z hlediska kontroly kvality). Je vhodné zajistit možnost předání dané služby jinému dodavateli během krátké lhůty.

Doporučení: ve skladech provádět pravidelně kontrolu skladovaného materiálu, jeho použitelnosti. Sledovat teplotu a vlhkost ve skladech. Vyskladnění materiálu zajišťovat podle data a roku nákupu. Vhodně volit umístění skladů pro případ ohrožení mimořádnou událostí.

12.6. Nedostatek pracovních sil

Úkoly Policie České republiky vykonává odborný kvalifikovaný personál, bez kterého je plnění úkolů nemožné. Proto je velmi důležité, aby při jakémkoliv ohrožení bylo možné zajistit nutný počet zaměstnanců na pracovišti. Tato problematika je u policie řešena v plánu vyrozumění, který je součástí plánu akceschopnosti.

Policie České republiky je schopna plnit úkoly do doby než dojde k poklesu počtu pracovních sil pod 50 % skutečného stavu policistů. Potom musí dojít k opatření a doplnění stavu povoláním policistů ze záloh nebo na základě žádosti předložené ministrem vnitra vládě, doplnění stavu Celní správou, Vězeňskou službou nebo Armádou České republiky.

Doporučení: v rámci předcházení snížení početních stavů vlivem infekčních onemocnění a pandemie, provádět očkování policistů proti těmto nemocem.

12.7. Ochrana areálů

Přestože toto riziko nebylo vyhodnoceno záporně, musí Policie České republiky zajišťovat i ochranu areálu, ve kterých působí v případě ohrožení přírodními mimořádnými událostmi, antropogenními mimořádnými událostmi nebo jejich kombinací. Toto ohrožení nemůže zabránit policii plnit úkoly ve věcech veřejného pořádku a bezpečnosti a další úkoly v rozsahu jak stanoví zákony.

Na ochranu areálů má zpracovanou dokumentaci bezpečnostní ochrany areálů v souladu s interními předpisy, kde je řešena v rámci přehledu opatření ochrana areálů, osob, předmětů chráněného zájmu před ohrožením na základě vyhodnocených rizik.

Doporučení: zhodnotit současný stav bezpečnostní ochrany areálů technickými prostředky. Modernizovat technické prostředky, např. kamerové systémy, elektronické zabezpečovací systémy apod. Zvážit pořízení bezpečnostních rámů, rentgenového zařízení pro prohlídku zavazadel u hlavního vstupu do areálu včetně zřízení místa pro uložení zbraní odložených návštěvou areálu, včetně bezpečného prostoru pro jejich vybití. Přezkoumat uložení předmětů chráněného zájmu v prostorách, které jsou ohroženy mimořádnou událostí. Tyto prostory zřizovat ve vyšších podlažích, pokud to umožní statika podlaží a budovy. Pravidelně aktualizovat dokumentaci bezpečnosti areálů a režimových prostorů a školit osoby pracující v areálech z těchto dokumentací.

13. Závěr

Tématem diplomové práce byla kritická infrastruktura a její ochrana. Diplomovou práci jsem rozdělil do kapitol, ve kterých se zabývám historickým vývojem kritické infrastruktury ve světě a v České republice, funkcí státu a odpovědností za jednotlivé oblasti kritické infrastruktury. První návrh těchto oblastí je uveden v příloze č. 1. Ke konci této kapitoly poukazuji na spojitost kritické infrastruktury a Evropské unie. Na ní navazuje kapitola, ve které vysvětluji termín infrastruktura, její vznik a z toho vymezené pojmenování veřejná infrastruktura a kritická infrastruktura. V rámci řešení problematiky kritické infrastruktury v České republice se v podkapitolách zmiňuji o dvou dokumentech, a to Komplexní strategii České republiky v řešení problematiky kritické infrastruktury a Národním programu ochrany kritické infrastruktury. Uvádím zde pak kritéria pro začleňování subjektů kritické infrastruktury kategorií, které jsou čtyři. Ty jsou pak dále zpracované pro přehlednost v tabulkách, které uvádím v příloze č. 2 – 5 podle jednotlivé kategorie s vymezením opatření k zachování potřebných činností a služeb v případě narušení jejich fungování.

V následující kapitole se zabývám možnostmi, které můžou způsobit ohrožení, poškození nebo zničení kritické infrastruktury v podobě mimořádných událostí a rizik. Základní rozdělení mimořádných událostí uvádím v příloze č. 6. Na závěr kapitoly je vypsáno 13 vybraných rizik, která mohou nejvíce ohrožovat kritickou infrastrukturu. Na to navazuji kapitolou analýza rizik a metody k jejímu provedení a kapitolou ochrana kritické infrastruktury. V kapitolách uvedených v předchozím a tomto odstavci jsem se snažil popsat v obecné rovině kritickou infrastrukturu a její ochranu s použitím literatury a internetu.

V dalších kapitolách diplomové práce se zabývám vlastním cílem diplomové práce. Tím je navrhnout možné způsoby ochrany subjektů a objektů kritické infrastruktury. Vzhledem k tomu, že ze stanoveného cíle vyznívá potřeba zabývat se ochranou všech subjektů a objektů kritické infrastruktury ve vazbě na stanovené oblasti kritické infrastruktury, jsme se domluvily s vedoucí práce zabývat se po upřesnění si tohoto výkladu pouze jedním subjektem kritické infrastruktury. Tímto subjektem je Policie České republiky, která patří do oblasti Nouzových služeb. V dalších kapitolách, napřed seznamuji ve stručnosti o složení a úkolech Policie České republiky. Zabývám se vysvětlením termínu veřejný pořádek, vnitřní pořádek a bezpečnost. Důvodem je, že jedním z úkolů policie je zajistit veřejný pořádek a bezpečnost.

Pro naplnění cíle diplomové práce jsem v dalších kapitolách učinil volbu metody pro provedení analýzy rizik. Pro analýzu rizik jsem zvolil metodu Check list (kontrolní seznam). Musel jsem si napřed ujasnit hlavní otázku a na ni pak vytvořit soubor otázek, které vycházely z rizik ohrožujících kritickou infrastrukturu. Navržený kontrolní seznam jsem pak konzultoval s kolegy odborníky. Poté jsem provedl vyplnění a vyhodnocení kontrolního seznamu. Na základě vyhodnocení jsem navrhl při záporných odpovědích doporučení pro zlepšení ochrany. Domnívám se, že do budoucna není vyloučena možnost praktického využití vytvořeného kontrolního seznamu k provedení analýzy rizik u Policie České republiky jako subjektu kritické infrastruktury. Samozřejmě, že mnou navržený soubor otázek by si jednotlivá pracoviště krizového řízení upřesnila nebo doplnila o další otázky (kontrolní seznam je variabilní) podle místních podmínek, kde by tuto metodu chtěli použít. Je pouze na rozhodnutí managementu Policie České republiky ve spolupráci s pracovišti oddělení krizového řízení na Policejním prezídiu a krajských ředitelstvích, pro kterou metodu analýzy rizik se rozhodnou a zda použijí metodu kontrolního seznamu nebo metodu jinou.

Závěrem chci ještě upozornit na skutečnost, že Policie České republiky jako subjekt kritické infrastruktury se nezabývá pouze ochranou vlastní, ale protože je závislá na dodávkách služeb z jiných oblastí kritické infrastruktury a subjektů této infrastruktury, požaduje se, aby byla nápomocna v zabezpečení ochrany v případě ohrožení těchto subjektů. Vzhledem k tomu, že v současné době není vytvořena legislativa na ochranu kritické infrastruktury, ale na základě směrnice Rady Evropy se v současnosti tato legislativa připravuje, není tak doposud stanoven způsob jak tento požadavek s policií řešit. Někteří vlastníci subjektů a objektů kritické infrastruktury na základě současné platné legislativy se toto snaží řešit uzavřením písemné dohody mezi nimi a Policií České republiky o vzájemné spolupráci na zajištění ochrany kritické infrastruktury. Jaké ale bude řešení popsané problematiky v budoucnosti, si musíme počkat na vydání připravované právní normy, která vyjde buď jako samostatný zákon na ochranu kritické infrastruktury nebo bude zakomponována do novely některého ze stávajících zákonů, např. krizového zákona s účinností od 12. ledna 2011.

Literatura

[1] ŠENOVSKÝ, M., ADAMEC, V., ŠENOVSKÝ, P., *Ochrana kritické infrastruktury*, 1. vydání Ostrava: Edice SPBI Spektrum, 2007, 141 s., ISBN: 978-80-7385-025-8

[2] Komise Evropských společenství, *Zelená kniha o Evropském programu na ochranu kritické infrastruktury*, KOM (2005) 576 v konečném znění, 26 s. Dostupný z WWW: http://eur-lex.europa.eu/LexUriServ/site/cs/com/2005/com2005_0576cs01.pdf, [cit. 2010-02-23]

[3] MARTÍNEK, B., *Východiska a principy zajištění ochrany kritické infrastruktury v České republice*, Časopis 112, ročník VII, číslo 4/2008, s. 22 – 24. Dostupný z WWW: www.hzscr.cz/clanek/archiv-2004-az-2008-503464.aspx, [cit. 2010-03-06]

[4] VEVERKA, I., *Vybrané kapitoly krizového řízení pro záchranářství*, 1. vydání Praha, 2003, 175 s., ISBN: 80-7251-126-2

[5] VALÁŠEK, J., KOVAŘÍK, F. a kolektiv, *Krizové řízení při nevojenských krizových situacích*, modul C, účelová publikace pro krizové řízení, vydání Praha: Ministerstvo vnitra, GŘ HZS ČR, 2008, 159 s., ISBN: 978-80-86640-93-8. Dostupný z WWW: http://www.hzscr.cz/clanek/moduly.aspx, [cit. 2010-03-19]

[6] Zákon č. 239/2000 Sb., o integrovaném záchranném systému a o změně některých zákonů, ve znění zákona č. 320/2002 Sb., 20/2004 Sb., 186/2006 Sb. a 267/2006 Sb.

[7] Zákon č. 240/2000 Sb., o krizovém řízení a změně některých zákonů (krizový zákon), ve znění zákona č. 320/2002 Sb., 127/2005 Sb., 112/2006 Sb., 267/2006 Sb. a 110/2007 Sb.

[8] Zákon č. 241/2000 Sb., o hospodářských opatřeních pro krizové stavy a o změně některých souvisejících zákonů, ve znění zákona č. 320/2002 Sb., 354/2003 Sb., 237/2004 Sb., 413/2005 Sb. a 444/2005 Sb.

[9] Zákon č. 133/1985 Sb., o požární ochraně, ve znění zákona č. 425/1990 Sb., 40/1994 Sb., 203/1994 Sb., 163/1998 Sb., 71/2000 Sb., 237/2000 Sb., 320/2002 Sb., 413/2005 Sb., 186/2006 Sb. a 267/2006 Sb.

[10] Směrnice rady 2008/114/ES, ze dne 8. prosince 2008, o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu

[11] Zákon č. 183/2006 Sb., o územním plánování a stavebním řádu (stavební zákon), ve znění zákona č. 68/2007 Sb., 191/2008 Sb., 223/2009 Sb. a 227/2009 Sb.

[12] Zpráva o řešení problematiky kritické infrastruktury v České republice, *Usnesení bezpečnostní rady státu č. 30 ze dne 3. července 2007*. Dostupný z WWW: http://www.evropskyrok.vlada.cz/cz/pracovni-a-poradni-organy-vlady/brs/cinnost/zaznamy-z-jednani/zaznamy-2007/zaznam-ze-schuze-brs-konane-dne-3--7--2007-23929/, [cit. 2010-03-19]

[13] Zpráva o řešení problematiky kritické infrastruktury v České republice, *uvedena v části III materiál čj. 09588/07-OOB, vydání: červenec 2007*

[14] *Internetová encyklopedie Wikipedie, česká verze*, http://cs.wikipedia.org/wiki/Infrastruktura, [cit. 2010-02-23]

[15] *Internetový ABZ.cz slovník cizích slov, česká verze*, http://slovnik-cizich slov.abz.cz/web.php/hledat?typ_hledani=prefix&cizi_slovo=strategie, [cit. 2010-03-19]

[16] KOVAŘÍK, J., *Kritická infrastruktura a ochrana obyvatelstva*, In: Ochrana obyvatel, 2007, Ochrana kritické infrastruktury, s. 145-153, ISBN: 80-86634-51-5

[17] *Internetové stránky Ministerstva vnitra*, http://www.mvcr.cz/clanek/hrozba.aspx, [cit. 2010-03-20]

[18] *Internetové stránky Ministerstva vnitra*, http://www.mvcr.cz/clanek/riziko.aspx, [cit. 2010-03-20]

[19] *Kritická infrastruktura – návrh tezí Komplexní strategie ČR k řešení problematiky kritické infrastruktury ČR*, MV GŘ HZS ČR, č.j. PO-762-90/CNP-2007 ze dne 3. srpna 2007.

[20] Harmonogram dalšího postupu zpracování dokumentů Komplexní strategie České republiky k řešení problematiky kritické infrastruktury a Národního programu ochrany kritické infrastruktury, *Usnesení bezpečnostní rady státu č. 4 ze dne 17. ledna 2008*.

[21] Harmonogram dalšího postupu zpracování dokumentů Komplexní strategie České republiky k řešení problematiky kritické infrastruktury a Národního programu ochrany kritické infrastruktury, *Usnesení Vlády České republiky č. 170 ze dne 25. února 2008*.

[22] STUCHLÁ, K., *Analýza rizik v havarijním plánování*, Časopis 112, ročník IV, číslo 4/2005, s. 26 – 27. Dostupný z WWW: http://www.hzscr.cz/clanek/archiv-2004-az-2008-503464.aspx, [cit. 2010-03-24]

[23] PROCHÁZKOVÁ, D., *Metodiky hodnocení rizik*, Časopis 112, ročník III, číslo 3/2004, s. 22 – 23. Dostupné z WWW: http://www.hzscr.cz/clanek/archiv-2004-az-2008-503464.aspx, [cit. 2010-03-29]

[24] ADAMEC, V., *Současnost a budoucnost typových plánů*, Časopis 112, ročník III, číslo 5/2004, s. 24 – 25. Dostupný z WWW: http://www.hzscr.cz/clanek/archiv-2004-az-2008-503464.aspx, [cit. 2010-04-12]

[25] SMEJKAL, V., RAIS, K., *Řízení rizik ve firmách a jiných organizací*, 3. vydání Praha: Grada Publishing, 2010, 354 s. ISBN: 978-80-247-3051-6

[26] SOUČEK, V., STAŇOVÁ, E., MACHOVÁ, N., VANGELI, B. a kolektiv, *Vnitřní bezpečnost a veřejný pořádek a vybrané kapitoly krizového řízení*, Odbor bezpečnostní politiky MV ČR, vydání Praha, 2009, 69 s. Dostupný z WWW: http://www.hzscr.cz/clanek/moduly.aspx, [cit. 2010-04-09]

[27] *Internetová encyklopedie o právu Eiuridictum, česká verze,* http://iuridictum.pecina.cz/w/Veřejný_pořádek, [cit. 2010-04-16]

[28] ŠKODA, J., VAVERA, F., ŠMERDA, R., *Zákon o policii s komentářem*, vydání Plzeň: Aleš Čeněk, 2009, 397 s., ISBN: 978-80-7380-160-1

[29] Zákon č. 273/2008 Sb., o Policii České republiky, ve znění zákona č. 274/2008 Sb.

[30] KOVÁRNÍK, L., TÓTH, J., *Policejní akce*, 1. vydání Praha: Policejní akademie České republiky v Praze, 2009, 222 s., ISBN: 978-80-7251-311-6

[31] ADAMEC, V., *Kritické infrastruktury I*, elektronický studijní materiál ve formátu pdf.

[32] Věstník Ministerstva vnitra, Nařízení Ministerstva vnitra číslo 20 ze dne 24. února 2009, kterým se upravuje bezpečnostní ochrana areálů, částka 28, Praha, ročník 2009.

Přílohy

Příloha č. 1: Seznam oblastí národní kritické infrastruktury navrhovaných v roce 2004.

Příloha č. 2: Podrobnosti k zařazení subjektů kritické infrastruktury do kategorie III.

Příloha č. 3: Podrobnosti k zařazení subjektů KI do kategorie II.

Příloha č. 4: Podrobnosti k zařazení subjektů KI do kategorie I.

Příloha č. 5: Podrobnosti k zařazení subjektů KI do zvláštní kategorie (Evropská kritická infrastruktura).

Příloha č. 6: Základní dělení mimořádných událostí.

Příloha č. 7: Přehled typových krizových situací.

Příloha č. 1

Seznam oblastí národní kritické infrastruktury navrhovaných v roce 2004 [16]

P.č.	*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 z 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.	Zdravotnická péče	4.1. přednemocniční neodkladná péče, 4.2. nemocniční péče, 4.3. ochrana veřejného zdraví, 4.4. distribuce léčiv.
5.	Doprava	5.1. silniční, 5.2. železniční, 5.3. letecká, 5.4. vnitrozemská vodní.
6.	Komunikační a informační systémy	6.1. služby pevných komunikačních sítí, 6.2. služby mobilních komunikačních sítí, 6.3. radiová komunikace a navigace, 6.4. satelitní komunikace, 6.5. televizní a radiové vysílání, 6.6. přístup k internetu a datovým službám, 6.7. poštovní a kurýrní služby.
7.	Bankovní a finanční systém	7.1. správa veřejných financí, 7.2. bankovnictví, 7.3. pojišťovnictví, 7.4. kapitálový trh.
8.	Nouzové služby	8.1. Policie ČR, 8.2. Hasičský záchranný sbor ČR, 8.3. Zdravotnická záchranná služba, 8.4. Letecká zdravotnická záchranná služba, 8.5. Armáda ČR, 8.6. radiační a chemické monitorování, 8.7. předpovědní, varovná a hlásná služba.
9.	Veřejná správa	9.1. výkon justice a vězeňství, 9.2. sociální ochrana a zaměstnanost, 9.3. diplomacie, 9.4. veřejná správa.
10.	Odpadové hospodářství	10.1. nakládání s odpady, 10.2. radioaktivní odpady.

Příloha č. 2

Podrobnosti k zařazení subjektů kritické infrastruktury do kategorie III [1]

Subjekt kritické infrastruktury	***Kategorie III – obec***
Narušení/vyřazení má dopad na obyvatelstvo	– obce či části obce.
Schopnost eliminovat narušení/vyřazení	– obec schopna odstranit, nahradit jiným subjektem nebo provizorním způsobem, – vlastní subjekt samostatně, – vlastní subjekt společně s obcí na základě vzájemné smlouvy.
Opatření	– stanovení postupu odstranění závad vedoucí k nefunkčnosti objekt kritické infrastruktury-III, popřípadě způsob náhrady jiným subjektem nebo dočasné provizorní řešení, – stanovení postupu řešení následků mimořádné události vedoucí k nefunkčnosti objektů kritické infrastruktury, – uzavření smluv (dohod) mezi obcí, subjekty kritické infrastruktury-III a dalšími právnickými a fyzickými osobami obsahující řešení závad, náhradu nebo provizorium, – zpracování přijatých opatření do havarijního plánu kraje a dalších dokumentů v oblasti bezpečnosti.
Právní opora	– K zabezpečení plnění úkolů těmito subjekty lze v současné době využít §§ 23 a 24 zákona č. 239/2000 Sb. (zákon o IZS) za podmínky, že jsou zahrnuty do havarijního plánu kraje nebo vnějšího havarijního plánu. – Zvláštní význam vůči uvedeným subjektům má obec, která v souladu s § 15 zákona č. 239/2000 Sb. zabezpečuje úkoly v oblasti přípravy na řešení mimořádných událostí, podílu na záchranných a likvidačních pracích a na ochraně obyvatelstva.

Příloha č. 3

Podrobnosti k zařazení subjektů KI do kategorie II [1]

Subjekt kritické infrastruktury	***Kategorie II – kraj***
Narušení/vyřazení má dopad na obyvatelstvo	– více obcí, části kraje nebo celý kraj.
Schopnost eliminovat narušení/vyřazení	– kraj je schopen odstranit, nahradit jiným subjektem nebo provizorním způsobem nebo, – územní správní úřady s krajskou působností, – oblastní organizace v jednotlivých odvětvích, – subjekt/y na základě smlouvy (dohody) s krajem.
Opatření	– stanovení postupu odstranění závad (technologická havárie, přerušení dodávek médií, selhání lidského činitele atd.) vedoucí k nefunkčnosti objekt kritické infrastruktury-II, případě způsob náhrady jiným subjektem nebo dočasné provizorní řešení, – stanovení postupu řešení následků mimořádné události (požár, povodeň, teroristický útok, kriminální čin atd.), – uzavření smluv (dohod) mezi krajem, subjekty kritické infrastruktury-II a dalšími právnickými a fyzickými osobami obsahující řešení závad, náhradu nebo provizorium, – zpracování přijatých opatření do krizového plánu kraje a dalších dokumentů v oblasti bezpečnosti, – zpracování opatření do plánu krizové připravenosti příslušného subjektu kritické infrastruktury-II.
Právní opora	– K zabezpečení plnění úkolů těmito subjekty lze v současné době využít § 29 zákona č. 240/2000 Sb. (krizový zákon) za podmínky, že plní úkoly vyplývající z krizového plánu kraje. – Zvláštní význam vůči uvedeným subjektům má kraj, který v souladu s § 14 zákona č. 240/2000 Sb. zabezpečuje úkoly v oblasti připravenosti kraje na řešení krizových situací.

Příloha č. 4

Podrobnosti k zařazení subjektů KI do kategorie I [1]

Subjekt kritické infrastruktury	*Kategorie I – stát*
Narušení/vyřazení má dopad na obyvatelstvo	– území dvou a více krajů nebo celého státu.
Schopnost eliminovat narušení/vyřazení	– ministerstvo, ústřední správní úřad, – právnické a podnikající fyzické osoby působící na území celého státu nebo na území více krajů. – Při narušení nebo zničení jsou nutné opravy, rekonstrukce nebo výstavba části zařízení (systému), které nelze obvykle zabezpečit v krátké době. – Subjekty kritické infrastruktury kategorie I jsou prakticky nenahraditelné. – Činnost po jejich vyřazení je možné řešit pouze provizorně nebo s využitím předem připravených zdrojů např. zásob PHM, plynu, apod.
Opatření	– speciální řešení v územním plánování, – stanovení postupů k zajištění realizace plánů kontinuity, – stanovení postupu odstranění závad vedoucí k nefunkčnosti kritické infrastruktury-I, – stanovení způsobu dočasného provizorního řešení s využitím např. zahraniční pomoci, – stanovení postupu řešení následků mimořádné události, – uzavření smluv (dohod) mezi ministerstvy, Ústředním správním úřadem, subjekty kritické infrastruktury-I a dalšími právnickými a fyzickými osobami, – zpracování přijatých opatření do krizového plánu příslušného Ústředního správního úřadu/České národní banky a dalších dokumentů v oblasti bezpečnosti, – zapracování opatření do plánu krizové připravenosti příslušného subjektu kritické infrastruktury-I, – zajištění fyzické ochrany, – zajištění kybernetické ochrany.
Právní opora	– K zabezpečení plnění úkolů těmito subjekty lze v současné době využít § 29 zákona č. 240/2000 Sb. (krizový zákon) nebo zvláštní zákony (např. zákon č. 458/2000 Sb. (energetický zákon)). Subjekty plní úkoly vyplývající z krizových plánů příslušných ministerstev, Ústředního správního úřadu, České národní banky. – Zvláštní význam vůči uvedeným subjektům mají ministerstva a Ústřední správní úřad, které v souladu s § 9 odst. 2, písm. c) zákona č. 240/2000 Sb. zabezpečují okamžité opravy nezbytných veřejných zařízení pro přežití obyvatelstva a k zajištění funkčnosti veřejné správy.

Příloha č. 5

Podrobnosti k zařazení subjektů KI do zvláštní kategorie (Evropská kritická infrastruktura) [1]

Subjekt kritické infrastruktury	*Kategorie „zvláštní“ – Evropská unie*
Narušení/vyřazení má dopad na obyvatelstvo	– Území dvou a více zemí Evropské unie včetně přeshraničního účinku na jiný druh infrastruktury (domino-efekt).
Schopnost eliminovat narušení/vyřazení	– V současné době jsou na základě analýz Komise a generálního ředitelství dopravy a energetiky Evropské unie zpracována kritéria pro dopravu a energetiku.
Opatření	– Stanovení vzájemných vazeb a dopadů mezi jednotlivými sektory a účastníky procesu je velice náročné i s ohledem na měnící se subjekty a podmínky jejich fungování a existenci. – Kriteria by měla být v souladu se současným směrem vývoje a stanovena na základě určení jednotlivých členských států Evropské unie a v rámci jednání na úrovni Evropské unie.
Právní opora	– Připravuje se zákon na ochranu kritické infrastruktury v České republice na základě Směrnice rady 2008/114/ES.

Základní dělení mimořádných událostí [4]

1. **Přírodní (naturogenní) mimořádné události**, které vznikají za pomocí přírodních sil. Jsou reprezentovány seismickou aktivitou, vulkanickou činností, extrémními meteorologickými jevy, apod., které mohou být ještě umocněny doprovodnými ději. Přírodní mimořádné události dále pak rozdělujeme:

   a) **Abiotické** jsou způsobené neživou přírodou:
   - požáry způsobené přírodními vlivy,
   - kosmické záření,
   - radioaktivita přírodního prostředí,
   - únik radonu,
   - zvýšené radioaktivní pozadí,
   - povodně a záplavy,
   - dlouhodobá sucha,
   - dlouhodobé inverzní situace,
   - propad zemských dutin,
   - zemětřesení,
   - sopečná činnost,
   - posun říčního koryta,
   - půdní eroze,
   - silné mrazy a vzniky námraz,
   - sněhové kalamity,
   - zemské sesuvy,
   - krupobití,
   - vichřice,
   - větrné poryvy,
   - větrné víry – tornáda,
   - mlhy,
   - atmosférické výboje,
   - geomagnetické anomálie,
   - narušování ozónové vrstvy,
   - narušování krajinných celků a celkové ekologické rovnováhy,
   - přepólování zemských pólů,

- globální změna klimatu,
- pád kosmických těles.

b) **Biotické** jsou způsobené živou přírodou:

- epifylie – rozsáhlá nákaza rostlin,
- epizootie – rozsáhlá nákaza zvířat,
- epidemie – velká nákaza lidí,
- přemnožení přírodních škůdců,
- parazité,
- živočišní a rostlinní vetřelci,
- přemnožení plevelů,
- rychlé vymírání druhů,
- genové a biologické manipulace.

2. **Antropogenní mimořádné události** způsobené činností člověka přímo nebo zprostředkovaně. Tyto mimořádné události může člověk způsobit záměrně nebo svou neopatrností. Antropogenní mimořádné události dále rozdělujeme:

a) **Technogenní** jsou to provozní havárie a havárie spojené s infrastrukturou, jako:

- radiační havárie velkého rozsahu,
- technologické havárie spojené s výronem nebo únikem nebezpečných látek,
- havárie v dopravě s výronem toxických látek,
- rozsáhlé ropné havárie,
- požáry,
- rozsáhlé dopravní havárie v silniční, železniční letecké, městské a vnitrozemské lodní dopravě a na lanovkách,
- důlní neštěstí,
- mechanické a statické poruchy staveb a zařízení,
- technické a technologické havárie – požáry, exploze, destrukce,
- narušení hrází vodohospodářských děl,
- havárie v dopravě – požáry, exploze, destrukce,
- nepříznivé působení člověka na životní prostředí.

b) **Sociogenní mimořádné události interní** – vnitrostátní společenské, sociální a ekonomické krize, mezi které patří:

- narušení finančního a devizového hospodářství státu,
- narušení dodávek ropy a ropných produktů,
- narušení dodávek elektrické energie, plynu a tepla,
- narušení dodávek potravin a pitné vody,
- narušení dodávek léčiv a zdravotnického materiálu,
- narušení funkčnosti dopravních systémů,
- narušení funkčnosti informačních systémů a komunikačních vazeb,
- narušení funkčnosti systémů pro varování a vyrozumění obyvatelstva,
- totální zhroucení ekonomiky státu,
- migrační vlny a rozsáhlá migrace ze státu,
- rozvoj rasové, národnostní a náboženské nesnášenlivosti,
- hromadné postižení osob mimo epidemii,
- hrozba teroristických akcí, aktivity vnitřního mezinárodního zločinu a terorismu militantních nebo extrémních politických skupin mezi sebou,
- ohrožení zdraví a života občanů jiných zemí takového rozsahu, kdy je vyžadovaná humanitární pomoc nebo nasazení záchranných sil v rámci zahraniční pomoci,
- ohrožení demokratických základů státu extrémistickými politickými skupinami,
- psychosociální negativní jevy,
- záměrné šíření poplašných a nepravdivých zpráv, vyvolávání stavu paniky,
- záměrné šíření drogových závislostí,
- působení toxických odpadů na okolí,
- použití zbraní hromadného ničení jaderných, chemických a biologických,
- decimování a vyhlazování obyvatelstva,
- vliv přelidnění.

c) **Sociogenní mimořádné události externí** – vojenské krizové situace:

- násilné akce subjektů cizí moci spojené s použitím vojenských sil a prostředků na území, ke kterému jsou plněny spojenecké závazky nebo poskytována mezinárodní humanitární pomoc,
- vnější vojenské napadení státu nebo jeho spojenců,

- ohrožení základních demokratických hodnot v takovém rozsahu, že je požadováno nasazení ozbrojených sil pro provedení mezinárodní mírové nebo humanitární operace,
- hospodářská sankce a hospodářský nátlak,
- rozsáhlé ekologické havárie, přesahující hranice států,
- politický nátlak,
- přenos hospodářských krizí z důvodu propojení ekonomik.

d) **Agrogenní** – spojené se zemědělstvím a půdou:

- eroze půdy,
- degradace kvality půdy,
- splavování půd do vodních toků,
- zhutňování půd z důvodu používání těžké mechanizace,
- nevhodné používání hnojiv a agrochemikálií,
- vysychání a znehodnocování vodních zdrojů,
- monokulturní zemědělská výroba,
- zhoršení kvality zemědělské produkce vlivem velkoprodukce.

Příloha č. 7

Přehled typových krizových situací [24]

P.č.	*Typ krizové situace (druh ohrožení)*
1.	Dlouhodobá inverzní situace
2.	Povodně velkého rozsahu
3.	Jiné živelné pohromy velkého rozsahu, mimo typu krizové situace č. 1 a 2, jako např. rozsáhlé lesní požáry, sněhové kalamity, vichřice, sesuvy půdy, zemětřesení, apod.
4.	Epidemie – hromadné nákazy osob (včetně hygienických a dalších režimů)
5.	Epifytie – hromadné nákazy polních kultur (včetně hygienických a dalších režimů)
6.	Epizootie – hromadné nákazy zvířat (včetně hygienických a dalších režimů)
7.	Radiační havárie
8.	Havárie velkého rozsahu způsobená vybranými nebezpečnými chemickými látkami a chemickými přípravky
9.	Jiné technické a technologické havárie velkého rozsahu – požáry, exploze, destrukce nadzemní a podzemní části staveb
10.	Narušení hrází významných vodohospodářských děl se vznikem zvláštní povodně
11.	Znečištění vody, ovzduší a přírodního prostředí haváriemi velkého rozsahu
12.	Narušení finančního a devizového hospodářství státu velkého rozsahu
13.	Narušení dodávek ropy a ropných produktů velkého rozsahu
14.	Narušení dodávek elektrické energie, plynu nebo tepelné energie velkého rozsahu
15.	Narušení dodávek potravin velkého rozsahu
16.	Narušení dodávek pitné vody velkého rozsahu
17.	Narušení dodávek léčiv a zdravotnického materiálu velkého rozsahu
18.	Narušení funkčnosti dopravní soustavy velkého rozsahu
19.	Narušení funkčnosti veřejných telekomunikačních vazeb velkého rozsahu
20.	Narušení funkčnosti veřejných informačních vazeb velkého rozsahu
21.	Migrační vlny velkého rozsahu
22.	Hromadné postižení osob mimo epidemií – řešení následků včetně hygienických a dalších režimů
23.	Narušení zákonnosti velkého rozsahu