Zranitelná místa kritické infrastruktury ve vybraném regionu

Pavel Havlík

Bakalářská práce
2015

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav ochrany obyvatelstva
akademický rok: 2014/2015

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Pavel Havlík**
Osobní číslo:	**L12137**
Studijní program:	**B2825 Ochrana obyvatelstva**
Studijní obor:	**Ochrana obyvatelstva**
Forma studia:	**prezenční**
Téma práce:	**Zranitelná místa kritické infrastruktury ve vybraném regionu**

Zásady pro vypracování:

1. **Vypracujte literární rešerši na téma kritická infrastruktura a její ochrana.**
2. **Vymezte základní pojmy a legislativu.**
3. **Charakterizujte oblasti kritické infrastruktury a její vývoj.**
4. **Analyzujte kritické infrastruktury vybraného regionu a její zranitelná místa.**
5. **Na základě získaných poznatků navrhněte možná řešení nebo inovace ochrany kritické infrastruktury v daném regionu.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

[1] ŠENOVSKÝ, Michail, Vilém ADAMEC a Pavel ŠENOVSKÝ. Ochrana kritické infrastruktury. 1. vyd. V Ostravě: Sdružení požárního a bezpečnostního inženýrství, 2007, 141 s. ISBN 978-80-7385-025-8.

[2] HROMADA, Martin. Systém a způsob hodnocení odolnosti kritické infrastruktury. 1. vyd. V Ostravě: Sdružení požárního a bezpečnostního inženýrství, 2013, 177 s. ISBN 978-80-7385-140-8.

[3] MOZGA, Jaroslav, Miloš VÍTEK a František KOVÁŘÍK. Kritická infrastruktura společnosti. Vyd. 1. Hradec Králové: Gaudeamus, 2008, 156 s. ISBN 978-80-7041-299-2.

Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce:	**doc. Ing. Otakar Jiří Mika, CSc.** Ústav krizového řízení
Datum zadání bakalářské práce:	**6. února 2015**
Termín odevzdání bakalářské práce:	**16. května 2015**

V Uherském Hradišti dne 20. února 2015

doc. RNDr. Jiří Dostál, CSc.
děkan

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta logistiky a krizového řízení

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

ABSTRAKT

Tato bakalářská práce pojednává o kritické infrastruktuře ve vybraném regionu. V teoretické části jsou rozebrány základní pojmy a platná legislativa České republiky pro lepší orientaci v oblasti kritické infrastruktury, jejího určování a její ochrany. Dále je zde ve stručnosti rozebrán vývoj kritické infrastruktury a základní teoretická fakta z oblasti kritické infrastruktury. V praktické části se nachází charakteristika vybraného regionu a vybraných odvětví kritické infrastruktury tohoto regionu. Jsou zde také rozebrány hrozby ohrožující kritickou infrastrukturu a jejich možné dopady. Cílem práce je shrnout poznatky o kritické infrastruktuře a zanalyzovat její stav ve vybraném regionu.

Klíčová slova: kritická infrastruktura, ochrana kritické infrastruktury, prvky kritické infrastruktury, zranitelná místa

ABSTRACT

This bachelor thesis concerns about the critical infrastructure in the selected region. The theoretical part deals with the basic concepts and the valid legislation of the Czech Republic for a better orientation in the area of critical infrastructure, its determination and its protection. In next step there is briefly analyzed the development of critical infrastructure and basic theoretical facts in the field of critical infrastructure. In the practical part there is characteristic of the selected region and the selected critical infrastructure sectors in the region. There are also discussed threats which may affect critical infrastructure and their possible impacts. The purpose of this thesis is to summarize the findings of critical infrastructure and analyze its status in the selected region.

Keywords: critical infrastructure, critical infrastructure protection, critical infrastructure elements, vulnerabilities

Poděkování:

Na tomto místě bych chtěl poděkovat panu doc. Ing. Otakaru Jiřímu Mikovi, CSc., vedoucímu mé bakalářské práce za jeho odborné vedení, a také cenné rady a připomínky ke zpracování této práce. Dále bych chtěl poděkovat Mgr. Liboru Kirschovi, Odboru ochrany obyvatelstva a krizového řízení Hasičského záchranného sboru Pardubického kraje a Oddělení krizového řízení Krajského úřadu Pardubického kraje, zejména panu Bc. Martinu Holovskému, za cenné materiály a čas, který mi věnovali při odborných konzultacích. V neposlední řadě samozřejmě děkuji mé rodině za zázemí a podporu během celé doby mého studia.

Motto:

„Co je dobro? Znalost věci. Co je zlo? Neznalost věci.“

Lucius Annaeus Seneca

Prohlašuji, že

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

Prohlašuji,

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

V Uherském Hradišti

12. 5. 2015

Havlík

podpis studenta

OBSAH

ÚVOD **9**

I TEORETICKÁ ČÁST **10**

1 ZÁKLADNÍ POJMY **11**

1.1 INFRASTRUKTURA 11

1.2 KRITICKÁ INFRASTRUKTURA 11

1.2.1 Evropská kritická infrastruktura 11

1.3 PRVEK KRITICKÉ INFRASTRUKTURY 11

1.4 SUBJEKT KRITICKÉ INFRASTRUKTURY 11

1.5 OCHRANA KRITICKÉ INFRASTRUKTURY 11

2 LEGISLATIVA **12**

2.1 KRIZOVÝ ZÁKON 12

2.1.1 Novela krizového zákona 12

2.1.2 Nařízení vlády upravující problematiku kritické infrastruktury 12

2.2 SMĚRNICE RADY EVROPSKÉ UNIE O EVROPSKÉ KRITICKÉ INFRASTRUKTUŘE 13

3 VÝVOJ OCHRANY KRITICKÉ INFRASTRUKTURY **14**

4 OCHRANA KRITICKÉ INFRASTRUKTURY **16**

4.1 BEZPEČNOSTNÍ PROSTŘEDÍ Z HLEDISKA KRITICKÉ INFRASTRUKTURY 17

4.2 SUBJEKT KRITICKÉ INFRASTRUKTURY 18

4.3 OBJEKTY KRITICKÉ INFRASTRUKTURY 19

4.3.1 Plán krizové připravenosti subjektu kritické infrastruktury 19

4.4 NÁSTROJE EVROPSKÉ UNIE K OCHRANĚ KRITICKÉ INFRASTRUKTURY 20

4.4.1 Zelená kniha o evropském programu na ochranu kritické infrastruktury 20

4.4.2 Výstražná informační síť kritické infrastruktury 22

5 URČENÍ PRVKŮ KRITICKÉ INFRASTRUKTURY **23**

5.1 SYSTÉM URČOVÁNÍ PRVKŮ KRITICKÉ INFRASTRUKTURY 23

5.2 PRŮŘEZOVÁ KRITÉRIA 24

5.3 ODVĚTVOVÁ KRITÉRIA 24

5.3.1 Oblasti kritické infrastruktury 24

5.4 KRITICKÁ INFRASTRUKTURA NA ÚZEMNÍ ÚROVNI 27

II PRAKTICKÁ ČÁST **28**

6 CHARAKTERISTIKA VYBRANÉHO REGIONU **29**

6.1 SPRÁVNÍ ČLENĚNÍ REGIONU 30

6.2 MOŽNÁ RIZIKA V REGIONU 31

7 PRVKY KRITICKÉ INFRASTRUKTURY V REGIONU **32**

7.1 PRVKY KRITICKÉ INFRASTRUKTURY URČENÉ MINISTERSTVEM PRŮMYSLU A OBCHODU 32
7.2 PRVKY KRITICKÉ INFRASTRUKTURY URČENÉ OSTATNÍMI SPRÁVNÍMI ÚŘADY 33
8 VYBRANÉ OBLASTI KRITICKÉ INFRASTRUKTURY V REGIONU 34
8.1 ZDRAVOTNICTVÍ 34
8.2 ENERGETIKA – ELEKTŘINA 34
8.2.1 Odvětvová kritéria pro elektřinu 35
8.2.2 Elektřina v regionu 36
8.2.2.1 Transformační stanice Krasíkov 37
8.2.2.2 Transformační stanice Opočínek 37
8.2.2.3 Zdroje elektrické energie 38
9 BEZPEČNOSTNÍ HROZBY PRO ENERGETIKU VYBRANÉHO REGIONU 39
9.1 MOŽNÉ DOPADY 40
9.2 FYZICKÁ OCHRANA KRITICKÉ INFRASTRUKTURY 41
9.2.1 Režimová opatření 42
9.2.2 Technická opatření 42
9.2.3 Ostraha 42
10 POZNATKY O OCHRANĚ KRITICKÉ INFRASTRUKTURY VE VYBRANÉM REGIONU 43
10.1 OBLAST ZDRAVOTNICTVÍ 43
10.2 OBLAST ENERGETIKY – ELEKTŘINA 43
ZÁVĚR 46
SEZNAM POUŽITÉ LITERATURY 47
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK 51
SEZNAM OBRÁZKŮ 52
SEZNAM TABULEK 53

ÚVOD

Státy mezinárodního společenství se musely začít zabývat mírou zranitelnosti důležitých subjektů v různých odvětvích hospodářství, situací zajištění základních úkolů státu zvláště v krizových situacích a zajištěním základních životních potřeb obyvatelstva za situací a okolností, jež vybočují z běžných podmínek. Ochrana těchto životně významných zdrojů, infrastruktur a služeb je součástí problematiky, které se nazývá kritická infrastruktura (KI).

KI je komplexní systém klíčových prvků v oblastech důležitých pro bezpečnost a zajištění základních potřeb moderní společnosti. Proto je ochrana KI jeden z hlavních úkolů a cílů každého vyspělého státu. Jelikož se KI prolíná různými odvětvími lidské činnosti, je ochrana KI mnoha-oborovou problematikou s technickými, organizačními, právními, finančními, manažerskými a jinými aspekty. Spojuje vědecké disciplíny, jako je krizové řízení, řízení a analýza rizik, krizové plánování a mnoho dalších.

Vzhledem k tendencím v době posledních několika let, je snahou ochránit KI především proti hrozbám, které mají charakter teroristického útoku. Nicméně ochrana KI je komplexní záležitostí, která se pojí se zvládáním živelních pohrom a jejich následků, nebo i haváriemi uvnitř prvku. Hrozby, které ohrožují KI, mohou v případě ničivých následků způsobit narušení infrastruktury velkého rozsahu a nefunkčnost některých jejích prvků v řádu hodin až dní. A právě takovýmto situacím je potřeba předcházet a být na ně připraven.

I. TEORETICKÁ ČÁST

1 ZÁKLADNÍ POJMY

1.1 Infrastruktura

Infrastruktura je v obecné rovině uměle vytvořený systém vzájemně propojených prvků, který slouží pro rámcovou podporu v různých oblastech moderní společnosti.

1.2 Kritická infrastruktura

KI se označuje ta část infrastruktury, která je životně důležitá pro bezproblémové fungování společnosti. V České republice (ČR) se pojmem KI rozumí: "*Prvek kritické infrastruktury nebo systém prvků kritické infrastruktury, narušení jehož funkce by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu“*. [1, 2]

1.2.1 Evropská kritická infrastruktura

Evropskou kritickou infrastrukturou (EKI) se rozumí: *„Kritická infrastruktura, která se nachází na území jednoho členského státu Evropské unie a jejíž narušení by mělo závažný dopad i na další členský stát Evropské unie.“* [1, 4]

1.3 Prvek kritické infrastruktury

Prvkem KI se rozumí: *„Zejména stavba, zařízení, prostředek nebo veřejná infrastruktura, určené podle průřezových a odvětvových kritérií; je-li prvek KI součástí evropské kritické infrastruktury, považuje se za prvek evropské kritické infrastruktury.“* [1]

1.4 Subjekt kritické infrastruktury

Subjektem KI se rozumí: *„Provozovatel prvku KI; jde-li o provozovatele prvku evropské kritické infrastruktury, považuje se za subjekt evropské kritické infrastruktury.“* [1]

1.5 Ochrana kritické infrastruktury

Ochranou KI se rozumí: *„Opatření zaměřená na snížení rizika narušení funkce prvku kritické infrastruktury.“* [1]

2 LEGISLATIVA

Právní ukotvení problematiky KI je dáno především *zákonem č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon*), *ve znění pozdějších předpisů.* [1] Do 31. prosince 2010 nebyla problematika KI v právním řádu ČR přímo zakotvena. To se však změnilo přijetím novely krizového zákona. V širších souvislostech se zajištěním fungování a ochrany KI dotýká i *ústavní zákon č. 110/1998 Sb. o bezpečnosti České republiky* [30] nebo *zákon č. 239/2000 Sb. o integrovaném záchranném systému* [31] a *zákon č. 241/2000 Sb. o hospodářských opatřeních pro krizové stavy* [32].

2.1 Krizový zákon

Zákon č. 240/2000 Sb., o krizovém řízení vytváří právní rámec pro působnosti a pravomoci státních orgánů a orgánů územních samosprávných celků a práva a povinnosti právnických a fyzických osob při přípravě na krizové situace, které nesouvisejí se zajišťováním obrany ČR před vnějším napadením, a při jejich řešení. [6]

2.1.1 Novela krizového zákona

Klíčovou příčinnou pro přijetí *zákona č. 430/2010 Sb., kterým se mění zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů* [33] byla nutnost zapracovat do právního řádu ČR povinnosti vyplývající *Směrnice Rady Evropské unie č. 2008/114/ES* [9] *ze dne 8. prosince 2008 o určování a označování evropských kritických infrastruktur a posuzování potřeby zvýšit jejich ochranu.*

Pro zapracování této směrnice Rady Evropské unie do právního řádu ČR bylo potřeba právní úpravy pro řešení problematiky KI na národní úrovni, jakožto výchozího předpokladu pro vymezení EKI, a tedy i pro splnění požadavků vyplývajících ze směrnice. [6]

2.1.2 Nařízení vlády upravující problematiku kritické infrastruktury

- Nařízení vlády č. **462/2000 Sb.** k provedení § 27 odst. 8 a § 28 odst. 5 zákona č. **240/2000 Sb.**, o krizovém řízení a o změně některých zákonu (krizový zákon)

- Nařízení vlády č. **431/2010 Sb.**, kterým se mění nařízení vlády č. **462/2000 Sb.**, k provedení § 27 odst. 8 a § 28 odst. 5 zákona č. **240/2000 Sb.**, o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění nařízení vlády č. **36/2003 Sb.**

  Tyto nařízení vlády řeší náležitosti plánu krizové připravenosti subjektu KI.

- Nařízení vlády č. **432/2010 Sb.** o kritériích pro určení prvku kritické infrastruktury. [34]

Toto nařízení definuje průřezová a odvětvová kritéria pro určování KI. Avšak 1. ledna 2015 nabylo účinnosti nařízení vlády č. **315/2014 Sb.** ze dne 8. prosince 2014, kterým se mění nařízení vlády č. **432/2010 Sb.**, o kritériích pro určení prvku kritické infrastruktury. Nezbytnost novelizace tohoto nařízení vzešla jak z aplikační praxe a nutnosti terminologických úprav textu, tak i z požadavku na zapracování problematiky kybernetické bezpečnosti, v důsledku přijetí zákona č. 181/2014 Sb., o kybernetické bezpečnosti a změně souvisejících zákonů (zákon o kybernetické bezpečnosti). [15]

2.2 Směrnice Rady Evropské unie o evropské kritické infrastruktuře

Směrnice Rady Evropské unie č. 2008/114/ES definuje KI jako složku, systém nebo jejich část nacházející se v členských státech, jejichž narušení nebo zničení by mělo vážné přeshraniční dopady na základní funkce společnosti z hlediska bezpečnosti, kvality života z ekonomického a sociálního hlediska a schopnost státu tyto základní funkce zachovat. [9]

Hlavním cílem této směrnice je vytvoření rámce pro určování a rozlišování EKI a národní KI. Jako odvětví EKI směrnice určuje pouze energetiku (elektřina, ropa, zemní plyn) a dopravu (silniční, železniční, letecká, vnitrozemská vodní doprava, zámořská, pobřežní vodní doprava a přístavy). O možném dalším odvětví pro EKI se uvažovalo o oblasti informačních a komunikačních systému, ale pro chybějící kritéria výběru tato oblast prozatím mezi ostatní zařazena nebyla. [10]

3 VÝVOJ OCHRANY KRITICKÉ INFRASTRUKTURY

V dnešní době jsou lidská sídla mnohem zranitelnější, než tomu bývalo minulosti. V minulosti bývala sídla obehnána hradbami a do značné míry samostatná v rámci surovin a zdrojů, byla tedy schopna odolávat i několikaměsíčnímu obléhání nepřátel. Města současnosti jsou naprosto závislá na fungující infrastruktuře, a tak narušení kontinuity její funkce může mít za následek rychle se rozvíjející krizové situace. V dnešním světě svobodného pohybu a otevřených metropolí je tato infrastruktura vystavena možnému působení nepřátelského charakteru. Proniknutí do současné metropole ve svobodném světě nevyžaduje překonání žádných překážek. K narušení, či dokonce zhroucení, běžného života a způsobení velkých finančních škod ve městě postačí narušit či přerušit funkci městské KI. To je navíc možné i bez proniknutí na území města, tedy napadením rozvodné soustavy různých systémů (elektrická vedení, potrubí, zdroje vody, důležité dopravní stavby). Bez fungující infrastruktury se život ve větším městě zhroutí v průběhu několika málo hodin. [11]

Triviální závada nebo nízkonákladový útok se tak mohou rozvinout v rozsáhlou krizovou situaci. Vzájemná závislost systémů KI vede k tzv. domino efektu, kdy se krizová situace začne šířit kaskádově i vějířovitě a zasahuje další prvky a systémy zajišťující normální život v daném regionu. V řadě případů narušení KI mohou být tyto sekundární následky mnohem závažnější, nežli přímý dopad iniciační poruchy. [11]

Mezi prvními státy, které se začaly zabývat problematikou ochrany KI, byly Spojené státy americké (USA) a Austrálie. Prvním uceleným dokumentem, řešícím otázky ochrany KI, byla tzv. Bílá kniha (White Paper). Jednalo se o Směrnici 63, vydanou v květnu 1998 [28]. Vydal ji prezident USA Bill Clinton jako prezidentské rozhodnutí (Presidential Decision Directive 63). Bílá kniha pojímá KI jako základní systémy, které mají hmotnou a kybernetickou podstatu a mají vliv na funkce ekonomiky a státu. Hlavním záměrem Bílé knihy bylo přijetí nezbytných opatření ke snížení zranitelnosti KI, zejména z hlediska fyzických a kybernetických útoků. [2]

Po vzoru USA se ochranou konkrétních skupin potencionálních cílů KI začaly zabývat i státní administrativy evropských zemí. Týkalo se to především Velké Británie, kde bylo v roce 1999 ustanoveno Koordinační centrum pro bezpečnost národní infrastruktury (National Infrastructure Security Coordination Centre), toto instituce v dnešní době funguje jako Centrum pro ochranu národní infrastruktury (Centre for the Protection of National In-

frastructure) [29]. Dalšími evropskými zeměmi, které tuto problematiku řešili, byli také například Německo a Nizozemí. O jednotném a komplexním přístup řešení problematiky ochrany KI v evropských zemích se zasadila především Evropská unie (EU). [10]

Jestliže v rámci EU je zažitý pojem KI, pak je nutné uvést, že v USA se pro oblast této problematiky používá jiné, v podstatě synonymní označení. Jedná se o pojem *základní funkce státu*. Rozdílné označení vzešlo ze snahy EU, která se snažila o vytvoření silného, perspektivního a uznávaného mezinárodního společenství, jakožto protiváhu americkému systému. Rozdílné pojmenování mělo být prvním krokem k vytvoření vlastního systému a přístupu v oblasti ochrany KI. [10]

Ochrana KI eskaluje po událostech 11. září 2001, nabývá nového obsahu a rozměru. V USA se bezprostředně formují první sofistikovaná opatření. Terorismus, ať již za použití konvenčních nebo nekonvenčních zbraní, se stal aktuální ústřední hrozbou pro celosvětové společenství. [18]

Historie problematiky ochrany KI v ČR je vcelku rozsáhlá, i když ve svém vývoji v různých obdobích měla různé priority a nebyla to nijak ukotvená a komplexní problematika. V 70. a 80. letech minulého století to byla například priorita potřeby zvýšení odolnosti objektů národního hospodářství proti účinkům zbraní hromadného ničení. Avšak v příslušných pokynech bylo uvedeno, že při hodnocení zranitelnosti objektu se bere v úvahu i vliv živelních pohrom a provozních havárií.

Na přelomu 20. a 21. století, kdy ČR tuto problematiku začala rozvíjet, převládaly tendence přidat se k americkému systému, což pramenilo zejména z členství ČR v Severoatlantické alianci (od 12. března 1999). Zlom nastal v období mezi roky 2002 – 2003, kdy byla ČR jako možný kandidát na vstup do EU pravidelně zvána na zasedání o tzv. Zelené knize. Nakonec byl tedy americký přístup k řešení problematiky ochrany KI zavržen a ČR tedy tuto oblast rozvíjela v součinnosti s EU. [2, 10]

4 OCHRANA KRITICKÉ INFRASTRUKTURY

Ochrana KI je jedním z úkolů moderní společnosti. Je potřeba KI chránit tak, aby v ideálním případě fungovala za jakékoliv situace, tj. za běžných, mimořádných i kritických podmínek. Ochranou KI můžeme nazvat proces, který při zohlednění všech rizik a hrozeb vytváří podmínky k fungování subjektů KI a vazeb mezi nimi. Primárním cílem ochrana KI je snížení zranitelnosti systému, resp. zvýšení jeho odolnosti vůči následkům mimořádných událostí a krizových situací. [2, 3]

Narušení či přerušení funkce KI může být zapříčiněno přírodními, technologickými a asymetrickými hrozbami. Ochrana KI vychází ze sloučení velkého počtu existujících strategií, plánů a procedur zabývajících se prevencí, připraveností, odezvou a obnovou. Jedná se o syntézu dosavadních disciplín, jako jsou např. krizové řízení, řízení rizik, řízení bezpečnosti, ochrana obyvatelstva, plánování kontinuity podnikání a strategie udržitelného rozvoje. Velmi zranitelnou oblastí KI je zejména energetika, která může podléhat politickým tlakům, ale i hrozbám s kriminální podstatou. Příkladem mohou být politicky motivované manipulace s dodávkami strategických surovin, vstup nejasného kapitálu do KI ČR, sabotáže, či hospodářská kriminalita. [2, 3, 10]

Konkrétní zájmy při ochraně KI:

- snížit zranitelnost KI,
- ochránit obyvatelstvo, kritické zdroje a systémy, které jsou zásadní pro fungování společnosti,
- vytvořit podmínky pro prevenci a zajištění připravenosti na zvládání narušení prvku KI,
- zabezpečit práva obyvatelstva na odpovídající pomoc v situaci, kdy je narušena funkce KI, zajistit jejich informovanost o opatřeních ke zvládnutí této situace a o tom, jak mají na nastalou situaci reagovat. [3]

Problémem ochrany KI je především její rozsáhlost, z čehož vyplývá, že je velmi obtížné ji ochránit v celé její šíři. Strukturu prvku KI je možné si představit, jako soubor několika následujících částí:

1) kritické liniové stavby

2) kritické objekty
3) kritické stroje a zařízení
4) kritické materiály
5) kritický personál

Nejtěžším úkolem je ochránit právě kritické stavby liniového charakteru, typickým příkladem mohou být energetické přenosové sítě. Z tohoto důvodu se v ochraně KI přistupuje především k ochraně vybraných prvků, uzlových bodů, jejichž poškozením nebo vyřazením z činnosti by mohlo dojít k největší újmě. [2]

Mezi nástroje ochrany prvku KI patří:

- prevence,
- snížení rizika,
- odvrácení útoku,
- odstranění následků útoku.

Na ochraně KI se podílí zástupci státního a soukromého sektoru, tedy vláda a ústřední správní úřady (ÚSÚ) v jednotlivých oblastech KI a především konkrétní subjekty kritické infrastruktury, kterým je zákonem dána hlavní úloha v odpovědnosti za provedení opatření k ochraně KI. Při tvorbě ucelené strategie řešící ochranu KI je nutné vzít v potaz, že podstatná část subjektů KI je právě v soukromých rukou, proto je v této problematice nutná úzká spolupráce státního a soukromého sektoru. [2, 7]

4.1 Bezpečnostní prostředí z hlediska kritické infrastruktury

Ochrana KI je jeden z mnoha zájmů státu v rámci bezpečnostního prostředí. Bezpečnostní prostředí ovlivňující bezpečnost státu je prostředím velmi dynamickým. Vzhledem k provázanosti bezpečnostních trendů je bezpečnostní prostředí komplexní a velmi těžko předvídatelnou problematikou. Zdroje možných hrozeb a jejich nositelé mohou být jak státního, tak i stále více nestátního a nadnárodního charakteru. Mezi vnitřními a vnějšími bezpečnostními hrozbami dochází ke stírání rozdílů. Tyto charakteristiky mají tedy podstatný vliv na pojetí zajištění obrany a bezpečnosti státu. Pro účinné řešení této problematiky je tedy nezbytný komplexní přístup, který kombinuje civilní i vojenské nástroje, včetně eko-

nomických a diplomatických prostředků k předcházení hrozeb a ke zmírnění jejich nežádoucích vlivů. S tím souvisí stupňující se požadavky na připravenost a včasné účinné reagování na nečekané hrozby. [10, 19]

V rámci ochrany KI ČR monitoruje možné investice a vstup kapitálu ze zahraničí do odvětví KI a také strategických národních podniků, aby bylo předcházeno možným hrozbám z hlediska jejich zneužití při prosazování politických a ekonomických zájmů na úkor ČR. Z toho vyplývá potřeba státu na zachování kontroly nad KI, která dosud patří státu a nesnižování vlivu a kontroly státu ve strategických společnostech, které působí v jednotlivých odvětvích KI. [10, 19]

4.2 Subjekt kritické infrastruktury

Subjektem KI může být určen kterýkoliv provozovatel, jestliže provozuje prvek KI, který je uveden v usnesení vlády, je určen ÚSÚ nebo výzvou kompetentního orgánu krizového řízení. Povinností subjektu KI je zabezpečit ochranu prvku KI a posilovat jeho odolnost. K zvýšení odolnosti prvku KI slouží technické systémy ochrany, fyzická ochrana, kybernetická ochrana, organizační a režimová opatření a jejich případná kombinace. [7]

Povinností subjektu KI je také umožnit kontrolu opatření zajišťujících ochranu prvku KI, umožnit přístup na pozemek a prostor, kde se prvek nachází a bez zbytečného odkladu oznámit skutečnosti, jež se týkají výrobních, organizačních či jiných změn. [1]

Subjekty KI jsou navzájem propojené a jsou na sobě vzájemně závislé. V důsledku tohoto uspořádání tvoří systém navzájem závislých infrastruktur, ve kterém může docházet k řetězovému hromadění problémů, jež mohou způsobovat neočekávané a stále vážnější selhávání nezbytných služeb. [16]

Subjekty KI můžeme dle územního významu rozdělit do čtyř kategorií:

- subjekty KI kategorie III – subjekty místní úrovně
- subjekty KI kategorie II – subjekty krajské úrovně
- subjekty KI kategorie I – subjekty národní úrovně
- subjekty KI zvláštní kategorie – subjekty nadnárodní úrovně [2]

Pro součinnost subjektu KI při vykonávání úkolů podle zákona č. 240/2000 Sb. o krizovém řízení a o změně některých zákonů (krizový zákon), je povinen subjekt KI určit styčného bezpečnostního zaměstnance, o kterém je povinen informovat příslušné ministerstvo nebo jiný ÚSÚ. [1]

4.3 Objekty kritické infrastruktury

Objekty KI můžeme rozlišovat podle různých hledisek:

- Geometrické definice objektů:
  - bodové (budova, vysílač) – bod
  - liniové (železnice, produktovody) – spojnice bodů
  - areálové (letiště, železniční uzel) – spojnice bodů a plocha
  - prostorové (přeprava osob, materiálu) – suma bodových, liniových a areálových objektů umístěných v prostoru
  - síťové (mobilní, internetové sítě) – vzájemně propojené body liniovými prvky do sítě s různou prostorovou geometrickou polohou
- Lokalizace charakterizovaná umístěním objektu:
  - v zastavěném prostoru (v sídelním útvaru – ústřední správní úřad)
  - v nezastavěném prostoru (mimo sídlo – muniční sklad)
  - ve smíšeném prostoru (elektrická přenosová síť)
- Typy objektů určené k ochraně:
  - stacionární
  - mobilní [10]

4.3.1 Plán krizové připravenosti subjektu kritické infrastruktury

Plán krizové připravenosti (PKP) je nástrojem subjektů KI k zajištění jejich činnosti během krizových situací a k zajištění uskutečňování úkolů, které vyplývají z krizového plánu kraje, popřípadě obce s rozšířenou působností (ORP). Povinnost zpracovat PKP subjektu

KI zpracovávají subjekty, které jsou určeny dopisem Hasičského záchranného sboru kraje, Krajského úřadu nebo příslušného úřadu ORP. [8]

Patřičnosti PKP subjektu KI jsou stanoveny nařízením vlády č. 462/2000 Sb., ve znění pozdějších předpisů.

Účelem vypracování PKP subjektu KI je především:

- identifikování možných zdrojů rizik,
- analyzování možných ohrožení a jejich možný dopad na funkci prvku KI,
- popis a zhodnocení stávajících bezpečnostních opatření na ochranu KI s návrhem na jejich doplnění
- stanovení scénáře a postupů k zvládání mimořádných událostí a krizových situací. [10]

Povinnost subjektu KI zpracovat PKP subjektu KI je *„do jednoho roku od rozhodnutí vlády nebo ode dne nabytí právní moci opatření obecné povahy, kterým byl prvek KI určen“*. Aby měl takovýto dokument smysl, je potřeba ho pravidelně aktualizovat a přizpůsobovat aktuálním hrozbám. [10]

Kromě povinnosti zpracovat PKP subjektu KI, jsou tu i další dokumenty, které umožní subjektu KI být připraven na různé druhy mimořádných událostí a krizových situací, například plán kontinuity a plán obnovy.

4.4 Nástroje Evropské unie k ochraně kritické infrastruktury

Z praktické činnosti vyvíjené EU je zřejmé, že si je vědoma důležitosti a zároveň velké zranitelnosti KI a možných následků při jejím narušení či zničení. Jde především o ***Evropský program pro ochranu kritické infrastruktury*** (EPCIP), který by měl sloužit k tomu, aby v rámci EU existovala odpovídající a stejná úroveň bezpečnosti ochrany KI, co nejméně možností selhání a rychlá, osvědčená nápravná opatření. Úroveň ochrany by měla být přiměřená možnému dopadu, jenž by mohl způsobit jejich možné selhání. [11]

4.4.1 Zelená kniha o evropském programu na ochranu kritické infrastruktury

Zelená kniha o evropském programu na ochranu kritické infrastruktury je dokument EU, který řeší problematiku KI, byl vydán dne 17. listopadu 2005 v Bruselu.

Účelem Zelené knihy je vyvinutí úsilí o spolupráci se subjekty KI, které by navrhovaly konkrétní postupy a možná řešení vhodná pro EPCIP. Uvádí, že: *„Účinná ochrana kritické infrastruktury vyžaduje komunikaci, koordinaci a spolupráci jak na národní, tak na evropské úrovni, a to mezi všemi zainteresovanými subjekty – vlastníky a provozovateli infrastruktur, regulačními orgány, profesními organizacemi a odvětvovými sdruženími, stejně jako všech úrovní státní a veřejné správy a také veřejnosti.“* [11]

Jak bylo řečeno, účinná ochrana KI v EU je možná pouze za spolupráce, jak na evropské úrovni, tak na národní úrovni, za účasti na všech úrovních státní správy, samosprávy, mezi profesními organizacemi, vlastníky a provozovateli KI a také veřejnosti. [10]

Jednotlivé kapitoly Zelené knihy popisují účel a rozsah působnosti EPCIP. Cílem EPCIP je zajištění odpovídající a stejné úrovně ochrany KI v členských státech Evropské unie. EPCIP je charakteristický zaměřením prioritně proti hrozbám teroristických útoků. Mezi klíčové zásady EPCIP, které jsou uvedené v Zelené knize, patří: [10, 12]

- **Subsidiarita** – „*úsilí Evropské komise v oblasti ochrany KI se bude zaměřovat na infrastrukturu, která je kritická spíše z evropského než vnitrostátního či regionálního pohledu. Ačkoli se Komise zaměří na EKI, může v případě potřeby a s přihlédnutím ke stávajícím pravomocem Společenství a dostupným zdrojům poskytnout podporu členským státům v souvislosti s vnitrostátními KI.“* [12]
- **Doplňkovost** – „*jedná se vyvarování se zdvojování stávajícího úsilí, na úrovni EU i vnitrostátní či regionální úrovni, pokud je toto úsilí při ochraně KI prokazatelně efektivní. EPCIP bude tedy navazovat na existující odvětvová opatření a doplňovat je.“* [12]
- **Důvěrnost** – „*jak na úrovni EU, tak na úrovni členských států budou informace o ochraně kritické infrastruktury utajovány a přístup k nim bude povolen jen v případech potřeby. Sdílení informací o kritické infrastruktuře bude probíhat v prostředí důvěry a bezpečnosti.“* [12]
- **Spolupráce zainteresovaných subjektů** – „*všechny příslušné zainteresované subjekty se v rámci svých možností zapojí do rozvoje a provádění EPCIP. To bude zahrnovat vlastníky/provozovatele kritických infrastruktur označených jako evropské KI a také státní či další příslušné orgány.“* [12]

- **Proporcionalita** – „*opatření budou navržena pouze tam, kde byla na základě analýzy stávajících nedostatků v oblasti bezpečnosti zjištěna jejich potřebnost, a tato opatření budou úměrná úrovni a druhu daného ohrožení.“* [12]
- **Odvětvový přístup** – „*jelikož různá odvětví mají odlišné zkušenosti, odborné znalosti a požadavky týkající se ochrany KI, bude EPCIP rozvíjen podle odvětví a prováděn podle dohodnutého seznamu odvětví ochrany KI.*“ [12]

4.4.2 Výstražná informační síť kritické infrastruktury

Výstražná informační síť kritické infrastruktury (Critical Infrastructure Warning Information Network – CIWIN), je chráněný bezpečnostní a informační systém na internetové bázi, určený pro diskusi a výměnu informací vztahující se k ochraně KI v rámci členských státu EU. CIWIN byl vytvořen na základě Sdělení EPCIP z roku 2006. CIWIN se v prosinci 2012 posunul do provozní fáze a funkční je od ledna 2013. V prvních měsících jeho existence byl zaznamenán pozitivní vývoj, a to včetně nárůstu využívání statistik a vyhrazeného prostoru CIWIN pro národní účely. [13]

Očekává se, že se bude CIWIN dále rozvíjet a že bude sloužit jako důležitý interaktivní nástroj pro vývoj zde popisovaného přístupu EU. Tato role může být naplněna prostřednictvím několika důležitých funkcí CIWIN: [13]

- Síť je využívána pro ukázku vývoje vybraných případů EKI a k získání zpětné vazby od uživatelů CIWIN.
- Cílem CIWIN je nabídnout soubor nástrojů obsahující metodiky posouzení rizik a nástroje pro analýzu rizik (např. šablony).
- CIWIN se může stát hostitelskou platformou pro několik národních oblastí ochrany KI v členských státech EU.
- Tato síť bude obsahovat všechny důležité informace týkající se spolupráce s vybranými třetími zeměmi, jako jsou Spojené státy americké, Kanada a země EFTA (Evropské sdružení volného obchodu). [13]

5 URČENÍ PRVKŮ KRITICKÉ INFRASTRUKTURY

V souvislosti s přijetím definice KI bylo přijato také definování samotného prvku KI (dříve objekt), které konkretizuje samotný prvek KI (dříve objekt) a kritéria, která jsou určena k jeho určení. Určení prvku KI je podmíněno splněním dvou podmínek, za prvé naplnění definice KI a prvku KI, za druhé aplikování průřezových a odvětvových kritérií.

5.1 Systém určování prvků kritické infrastruktury

Znaky KI se odvíjejí z přijatých definic, získaných zkušeností a z teoretických poznatků problematiky ochrany KI. Pro rozeznání znaků KI existují různá teoretická východiska. Administrativně byrokratický systém přistoupil v první etapě řízené ochrany k tvorbě prostých seznamů KI. Podle praxe lze rozlišit na: [18]

- Seznam sektorů, objektů a služeb s kvalitativní charakteristikou – např. „jaderná elektrárna, vodní dílo, energovod“,
- Seznam sektorů, objektů a služeb s kvantitativní charakteristikou – např. „výrobna s celkovým instalovaným elektrickým výkonem nejméně 500 MW“,
- Seznam kritických (životně důležitých) společenských funkcí, jako indikačních kritérií pro výběr a označení KI – např. „vyřazený objekt vyvolá dopad mimořádné události s postihem více než 1000 osob“. [18]

V systému určování prvků KI je třeba rozlišovat postup při určování prvků KI, které provozuje organizační složka státu, a prvků, které neprovozuje žádná organizační složka státu.

V případě prvků, jejichž provozovatelem je stát, ministerstva a jiné ÚSÚ a Česká národní banka zašlou návrhy prvků Ministerstvu vnitra (resp. Ministerstvu vnitra-generálnímu ředitelství Hasičského záchranného sboru ČR), které z takto zaslaných podkladů vypracuje seznam. Ministerstvo vnitra jej následně předkládá vládě, která usnesením rozhodne o prvcích KI, které provozuje organizační složka státu. [14]

V případě, že provozovatelem prvků KI není organizační složka státu, realizují rozhodující činnost příslušná ministerstva a jiné ÚSÚ a Česká národní banka. Ty určí prvky opatřením obecné povahy v souladu se zákonem č. 500/2004 Sb., správní řád, ve znění

pozdějších předpisů. Následně o tomto určení bez zbytečného odkladu informují Ministerstvo vnitra. [14]

5.2 Průřezová kritéria

Průřezová kritéria jsou vymezena jako: *„Souhrn hledisek pro posuzování závažnosti vlivu narušení funkce prvku KI s mezními hodnotami, které obsahují rozsah ztrát na životě, dopad na zdraví osob, mimořádně vážný ekonomický dopad nebo dopad na veřejnost v důsledku rozsáhlého omezení poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života.“* [10]

Průřezovým kritériem pro určení prvku KI je hledisko:

a) *„obětí s mezní hodnotou více než 250 mrtvých nebo více než 2 500 osob s následnou hospitalizací po dobu delší než 24 hodin,“*

b) *„ekonomický dopad s mezní hodnotou ztráty státu vyšší než 0,5 % hrubého domácího produktu, nebo“*

c) *„dopad na veřejnost s mezní hodnotou rozsáhlého omezení poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života postihující více než 125 000 osob.“* [17]

5.3 Odvětvová kritéria

„Odvětvová kritéria jsou technické nebo provozní hodnoty pro určování prvku KI v odvětvích energetika, vodní hospodářství, potravinářství a zemědělství, zdravotnictví, doprava, komunikační a informační systémy, finanční trh a měna, nouzové služby a veřejná správa.“ Tyto oblasti a jejich členění jsou vyobrazeny v tabulce č. 1 Oblasti národní kritické infrastruktury na straně č. 25. [10]

5.3.1 Oblasti kritické infrastruktury

Při ochraně KI, zejména při přístupu z hlediska jednotlivých oblastí KI, nemůžeme uvažovat pouze nad jednou konkrétní oblastí. Všechny oblasti vykazují vysoký stupeň závislosti na ostatních, jednotlivých oblastech. Jako klíčové oblasti KI je možno označit především informační a komunikační systémy, energetiku a dopravu. To je možné vypozorovat

i z programu Evropské unie k ochraně KI, která právě tyto tři oblasti KI považuje za klíčové a věnuje jejich ochraně maximální úsilí.

Při neustále rostoucí závislosti na informačních a komunikačních technologiích je fenoménem posledních let především ohrožení právě informačních a komunikačních systémů kybernetickými útoky, ať už ohrožují občany nebo přímo stát. Tyto útoky mohou být novým prostředkem k vedení války, nebo mohou mít kriminální či teroristický charakter a jejich motivací může být destabilizace společnosti. Mohou způsobit selhání zejména komunikačních, energetických a dopravních sítí či procesů, průmyslových nebo finančních systémů, jež by měly za následek významné hmotné škody. Závislost ozbrojených sil státu na informačních a komunikačních systémech může mít vliv na obranyschopnost státu. S úniky strategicky důležitých informací ze státních a soukromých institucí souvisí problematika politické a ekonomické špionáže. [10, 19]

Tab. 1 Oblasti národní kritické infrastruktury [17]

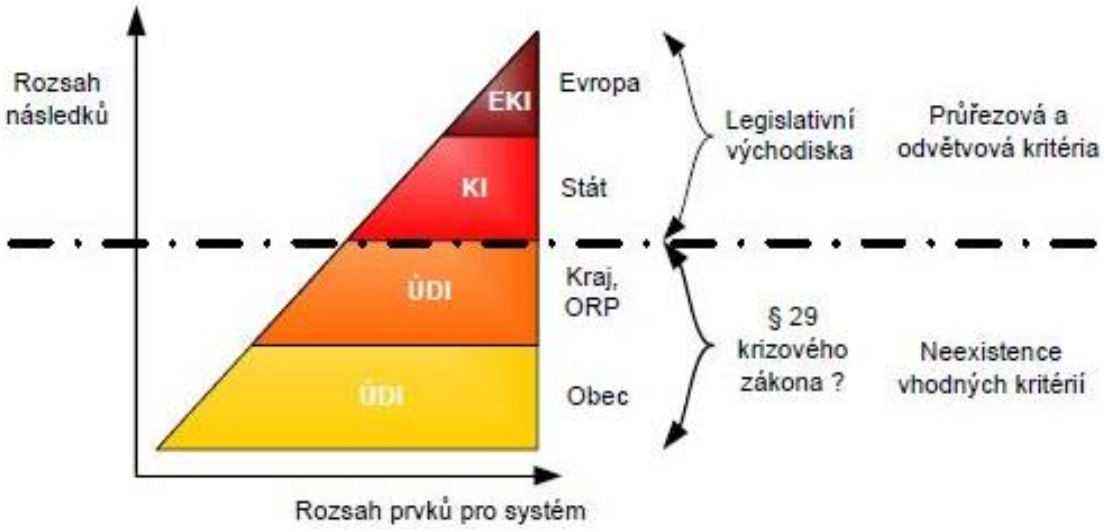
Pořadové číslo	Oblast KI	Podoblast
1.	Energetika	1.1. Elektřina
		1.2. Zemní plyn
		1.3. Ropa a ropné produkty
		1.4. Centrální zásobování teplem
2.	Vodní hospodářství	
3.	Potravinářství a zemědělství	3.1. Rostlinná výroba
		3.2. Živočišná výroba
		3.3. Potravinářská výroba
4.	Zdravotnictví	
5.	Doprava	5.1. Silniční doprava
		5.2. Železniční doprava
		5.3. Letecká doprava
		5.4. Vnitrozemská vodní doprava
6.	Komunikační a informační systémy	6.1. Technologické prvky pevné sítě elektronických komunikací
		6.2. Technologické prvky mobilní sítě elektronických komunikací
		6.3. Technologické prvky sítí pro rozhlasové a televizní vysílání
		6.4. Technologické prvky pro satelitní komunikaci
		6.5. Technologické prvky pro poštovní služby
		6.6. Technologické prvky informačních systémů
		6.7. Oblast kybernetické bezpečnosti
7.	Finanční trh a měna	
8.	Nouzové služby	8.1. Integrovaný záchranný systém
		8.2. Radiační monitorování
		8.3. Předpovědní, varovná a hlásná služba
9.	Veřejná správa	9.1. Veřejné finance
		9.2. Sociální ochrana a zaměstnanost
		9.3. Ostatní státní správa
		9.4. Zpravodajské služby

5.4 Kritická infrastruktura na územní úrovni

Z uvedených definic a kritérií pro určování prvků KI je zřejmé, že vymezují závažné následky nefunkčnosti prvku KI především na národní úrovni. Systém určování prvků je určen zejména s ohledem na bezpečnost státu a jeho ekonomikou, zajištění základních životních potřeb obyvatelstva z hlediska státu. [20]

Cílem i povinností státu je chránit a rozvíjet jeho klíčové zájmy. Klíčovým zájmem je bezpochyby i KI, jež je v rámci obecné infrastruktury ochraňována prioritně. Povinnosti k ochraně KI, jsou nařízeny zejména ÚSÚ a subjektům KI. [20]

Avšak i v rámci regionální úrovně mohou vzniknout okolnosti, za kterých mohou nastat rozsáhlá narušení územní infrastruktury územních celků. Je otázkou, jak řešit problematiku KI na územní úrovni. [20]



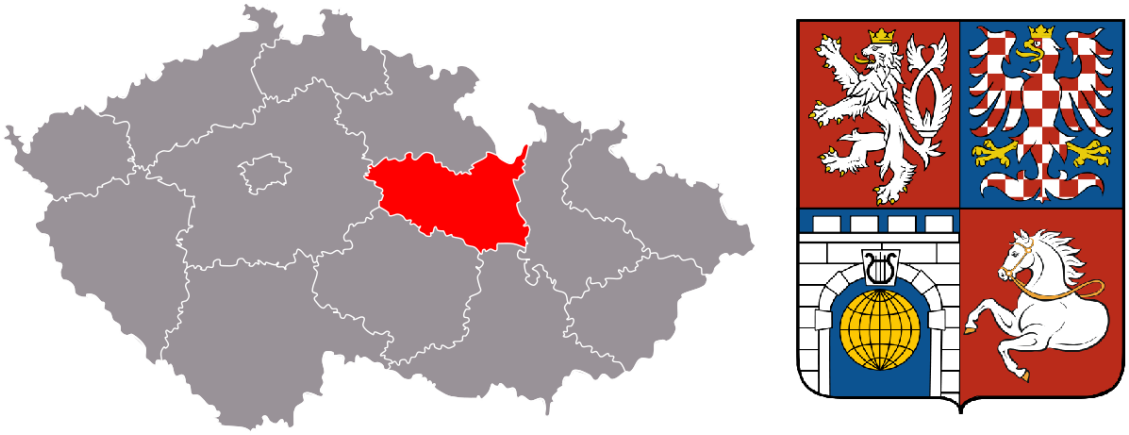
Obr. 1 Územně důležitá infrastruktura [20]

Legenda:
EKI - Evropská kritická infrastruktura
KI - Kritická infrastruktura
ÚDI - Územně důležitá infrastruktura

II. PRAKTICKÁ ČÁST

6 CHARAKTERISTIKA VYBRANÉHO REGIONU

Pro zpracování praktické části této bakalářské práce byl vybrán region Pardubického kraje.

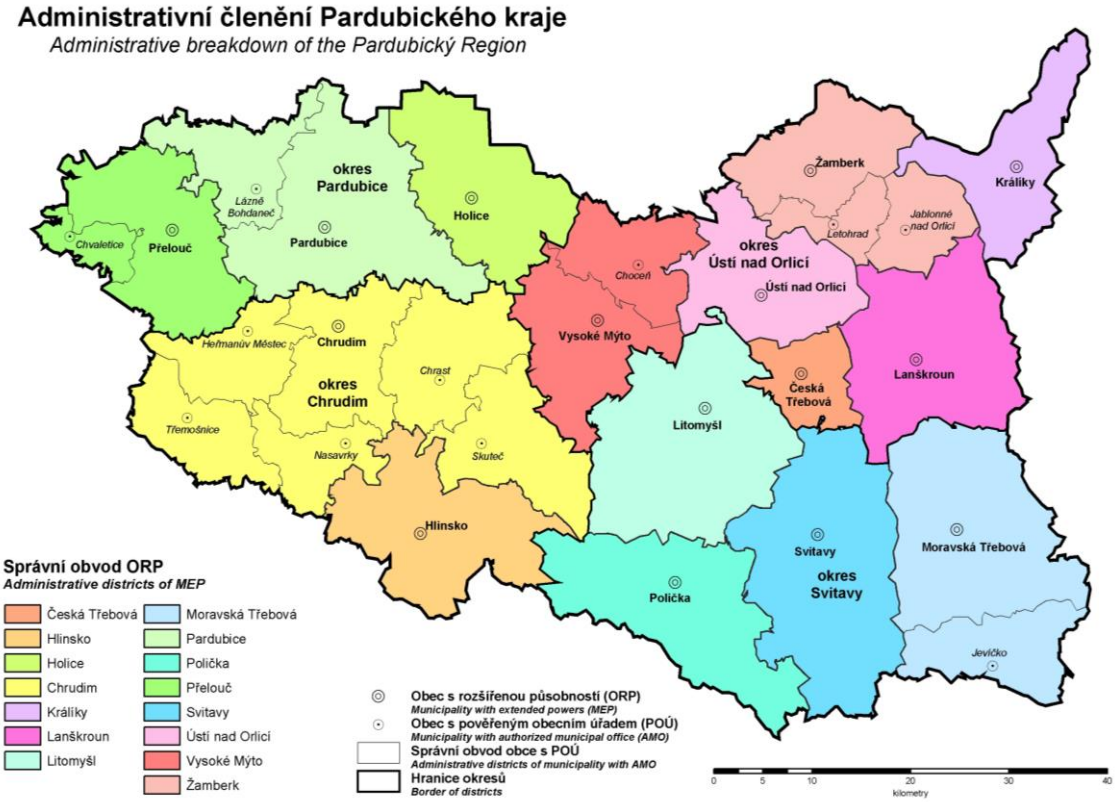


Obr. 2 Poloha Pardubického kraje v rámci ČR a znak Pardubického kraje

Pardubický kraj se rozkládá ve východní části Čech a jeho část leží také na historickém území Moravy. Pardubický kraj sousedí s kraji – Středočeským, Královéhradeckým, Olomouckým, Jihomoravským a Vysočinou. Spolu s Libereckým a Královéhradeckým krajem tvoří *„oblast soudržnosti Severovýchod“* (tzv. NUTS 2). Část severovýchodní hranice kraje vytváří současně i státní hranici s Polskem, odtud je kraj lemován jižní částí Orlických hor a nejzápadnějšími svahy Hrubého Jeseníku. Jih a jihovýchod kraje je ohraničen vrchovinnými oblastmi Žďárských vrchů a Železných hor, střed a západ kraje je tvořen Polabskou nížinou. Orlické hory, Žďárské vrchy a Železné hory patří k chráněným krajinným oblastem kraje. [21]

Rozloha Pardubického kraje je 4 519 km^2 (5,7 % rozlohy ČR), což znamená, že je pátým nejmenším krajem ČR. Z rozlohy kraje tvoří 60,0 % zemědělská půda. Zalesněné pozemky tvoří 29,7 % rozlohy kraje. [21]

6.1 Správní členění regionu



Obr. 3 Administrační členění Pardubického kraje [21]

Pardubický kraj se skládá ze čtyř okresů (Český statistický úřad s pojmem „okres“ pracuje, přestože byly okresy a okresní úřady v roce 2002 legislativně zrušeny) – Chrudim, Pardubice, Svitavy a Ústí nad Orlicí. Počet obyvatel v kraji k 31. prosinci 2013 byl 515 985 obyvatel, tedy 4,9 % z celkového počtu obyvatel ČR. Okres s nejvyšším počtem obyvatel je okres Pardubice, následují okresy Ústí nad Orlicí, Svitavy a Chrudim. [21]

V Pardubickém kraji se nachází celkem 451 obcí z toho 15 obcí s rozšířenou působností:

- Česká Třebová, Hlinsko, Holice, Chrudim, Králíky, Lanškroun, Litomyšl, Moravská Třebová, Pardubice, Polička, Přelouč, Svitavy, Ústí nad Orlicí, Vysoké Mýto a Žamberk

V krajském městě Pardubice žije 17,3 % obyvatel kraje. V kraji je celkem 38 měst, ve kterých žije 62,0 % obyvatel kraje. Třemi největšími městy Pardubického kraje jsou Pardubice, Chrudim a Svitavy. [21]

6.2 Možná rizika v regionu

Na následujícím obrázku je výčet možných hrozeb tak, jak jsou zpracovány v Krizovém plánu Pardubického kraje [23], a u kterých lze předpokládat vyhlášení krizového stavu.

P.č.	Druh hrozby/ORP	PR	PA	HO	CR	HL	UO	KR	ZA	LA	VM	CT	MT	SY	PO	LT
1	Dlouhodobá inverze															
2	Povodně	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO
	Bleskové povodně															
3	Lesní požáry															
	Vichřice	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO
	Sněhové kalamity															
	Sesuvy půdy															
	Zemětřesení															
4	Epidemie a nákazy (pandemie)	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO
5	Epifytie															
6	Epizootie	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO
7	Radiační havárie															
8	Technologické havárie v daném provozu															
9	Únik chemických látek, výbuch, požár															
10	Zvláštní povodeň		ANO		ANO	ANO	ANO		ANO		ANO	ANO		ANO		
11	Znečištění haváriemi velkého rozsahu															
12	Narušení finančního a devizového hospodářství	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO
13	Narušení dodávek ropy a ropných produktů	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO
14	Narušení dodávek elektrické energie	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO
	Narušení dodávek plynu	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO
	Narušení dodávek tepla		ANO		ANO											
15	Narušení dodávek potravin	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO
16	Narušení dodávek pitné vody velkého rozsahu	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO
17	Narušení dodávek léčiv	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO
18	Narušení funkčnosti dopravy	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO
19	Narušení služeb elektronických komunikací	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO
20	Narušení informačních vazeb	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO
20a	Narušení poštovních služeb	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO
21	Migrační vlny	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO
22	Hromadné postižení osob mimo epidemií															
23	Narušení zákonnosti velkého rozsahu	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO
24	Hrozba teroristického útoku	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO

Obr. 4 Seznam možných rizik na území Pardubického kraje [23]

Legenda:

ANO – identifikované riziko, PR – ORP Přelouč, PA – ORP Pardubice, HO – ORP Holice, CR – ORP Chrudim, HL – ORP Hlinsko, UO – ORP Ústí nad Orlicí, KR – ORP Králíky, ZA – ORP Žamberk, LA – ORP Lanškroun, VM – ORP Vysoké mýto, SY – ORP Svitavy, ZA – ORP Žamberk, CT – ORP Česká Třebová, PO – ORP Polička, UO – ORP Ústí nad Orlicí, LA – ORP Lanškroun, MT – ORP Moravská Třebová, LT – ORP Litomyšl

7 PRVKY KRITICKÉ INFRASTRUKTURY V REGIONU

V Krizovém plánu Pardubického kraje v části „Přehled prvků kritické infrastruktury a evropské kritické infrastruktury“ se nachází přehled prvků KI, které určuje Ministerstvo průmyslu a obchodu, a dále přehled prvků KI, které určují ostatní správní úřady. Z toho přehledu dále vyplývá, že se na území Pardubického kraje nenachází žádný prvek EKI.

7.1 Prvky kritické infrastruktury určené Ministerstvem průmyslu a obchodu

Přehled prvků KI určených Ministerstvem průmyslu a obchodu je rozdělen na:

- Prvky kritické infrastruktury v poštovních službách
- Prvky kritické infrastruktury v odvětví výroby, přenosu a distribuce elektřiny
- Prvky kritické infrastruktury v elektronických komunikacích

Přehled těchto prvků KI je zpracován jako označení prvku a jeho provozovatele. Příklad provozovatelů prvků KI ze seznamu:

- Česká pošta, s.p.
- ČEPS, a.s.
- ČEZ Distribuce, a. s.
- ČEZ, a.s.
- ČEZ ICT Services, a. s.
- Elektrárna Chvaletice, a.s.
- Elektrárny Opatovice, a.s.
- České Radiokomunikace, a.s.
- Telefónica Czech Republic, a.s.
- T-Mobile Czech Republic, a.s.

7.2 Prvky kritické infrastruktury určené ostatními správními úřady

V přehledu prvků KI na území Pardubického kraje se nachází celkem 19 prvků KI.

Tab. 2 Prvky KI určené ostatními správními úřady [23]

P. č.	Označení prvku KI	Subjekt KI	Odvětví	Určující ÚSÚ	Kraj
1	010	Správa železniční dopravní cesty, státní organizace	doprava	MD	Pk
2	36 Produktovod	Čepro, a. s.	ropa a ropné produkty	SSHR	SČk - Pk - KHk
3	72 Vnitrostátní ropovod	MERO, a. s.	ropa a ropné produkty	SSHR	SČk - Pk
4	81 Koncové zařízení pro předávání ropy	MERO, a. s.	ropa a ropné produkty	SSHR	Pk
5	88 Komplex zásobníků ropy a PHM	Paramo, a. s.	ropa a ropné produkty	SSHR	Pk
6	89 Technický dispečink	Paramo, a. s.	ropa a ropné produkty	SSHR	Pk
7	90 Rafinérie	Paramo, a. s.	ropa a ropné produkty	SSHR	Pk
8	91 Komplex zásobníků PHM	Union Consulting, s. r. o.	ropa a ropné produkty	SSHR	Pk
9	92 Technický dispečink	Union Consulting, s. r. o.	ropa a ropné produkty	SSHR	Pk
10	93 Produktovod	Union Consulting, s. r. o.	ropa a ropné produkty	SSHR	Pk
11	Krajské zdravotnické operační středisko	Zdravotnická záchranná služba Pardubického kraje	nouzové služby	MV	Pk
12	Objekt	Česká spořitelna, a.s.	finanční trh a měna	ČNB	Pk
13	Objekt 45	Komerční banka, a.s.	finanční trh a měna	ČNB	Pk
14	Objekt 65	ČSOB, a.s.	finanční trh a měna	ČNB	Pk
15	Datová infrastruktura	Okresní správa sociálního zabezpečení Pardubice	veřejná správa	MPSV	Pk
16	Integrované operační středisko operačního odboru Krajského ředitelství policie Pardubického kraje	Krajské ředitelství policie Pardubického kraje	nouzové služby	MV	Pk
17	Školící a záložní operační středisko	Vyšší policejní škola Ministerstva vnitra v Pardubicích	nouzové služby	MV	Pk
18	Operační středisko HZS Pardubického kraje	HZS Pardubického kraje	nouzové služby	MV	Pk
19	Radiační monitorování, stálá měřící a odběrová místa	Státní úřad pro jadernou bezpečnost	nouzové služby	SÚJB	Pk

8 VYBRANÉ OBLASTI KRITICKÉ INFRASTRUKTURY V REGIONU

Pro účel této práce jsem se zaměřil v rámci KI na dvě její oblasti. Oblast zdravotnictví a z oblasti energetiky na jednu z jejích podoblastí – elektřinu.

8.1 Zdravotnictví

Na území Pardubického kraje v roce 2013 v oblasti zdravotnictví působilo 9 nemocnic s 2 500 lůžky, 7 odborných léčebných ústavů s 1 295 lůžky, z toho 2 léčebny pro dlouhodobě nemocné s 205 lůžky a 152 lékáren včetně odloučených oddělení výdeje léčiv. Kromě těchto zdravotnických zařízení je v Pardubickém kraji 961 samostatných ordinací lékařů (praktických i odborných) a řada dalších zdravotnických zařízení (pracoviště vedená nelékařem, samostatné laboratoře atd.). [21]

Klíčovým subjektem v oblasti zdravotnictví v Pardubickém kraji je „Nemocnice Pardubického kraje, a.s.“ Tento subjekt vznikl k 31. prosinci 2014 sloučením pěti nemocnic akutní lůžkové péče, jejichž vlastníkem byl Pardubický kraj. Vznikem nové společnosti vyvrcholil dlouhodobý proces naplánovaný na základě „Scénáře efektivní transformace akutní lůžkové nemocniční péče v Pardubickém kraji“, který schválili krajští zastupitelé.

Subjekt „Nemocnice Pardubického kraje, a.s.“ tedy v současnosti disponuje pěti nemocnicemi poskytující péči na akutních lůžkách. Jsou to:

1) Svitavská nemocnice
2) Litomyšlská nemocnice
3) Orlickoústecká nemocnice
4) Chrudimská nemocnice
5) Pardubická nemocnice

8.2 Energetika – Elektřina

Elektrizační soustava je celostátně plošný systém s vysokou mírou vazeb na elektroenergetické soustavy okolních států. Tento systém se skládá z: [26]

- výrobní části produkující elektřinu v různých zdrojích

- přenosové soustavy vedení a zařízení (rozvoden – transformoven) 400 kV, 220 kV a vybraných vedení a zařízení 110 kV
- distribučních soustav vysokého napětí 3 kV, 6 kV, 10 kV, 22 kV, 35 kV a 110 kV
- distribučních soustav nízkého napětí 0,4/0,23 kV
- technických dispečinků hierarchicky uspořádaných k řízení celé soustavy. [26]

Jde o systém, který je velmi citlivý na správnou funkci a požadovanou interakci jeho jednotlivých prvků, které jsou úzce propojené a vzájemně se ovlivňují.

Útoky nebo havárie velkého rozsahu na klíčových prvcích elektrizační soustavy mohou přesáhnout reálné možnosti provozovatelů daného prvku zajistit okamžité obnovení provozu nebo si mohou vyžádat odstavení systému, a způsobí tak krizovou situaci v zásobování odběratelů elektrickou energií. Jelikož je elektřina oblast s vysokou provázaností do dalších odvětví, vznik sekundárních krizových situací je v takovém případě velice pravděpodobný. [25]

8.2.1 Odvětvová kritéria pro elektřinu

Odvětvová kritéria pro podoblast elektřina dle Nařízení vlády č. 432/2010 Sb. o kritériích pro určení prvku KI:

1. Výrobna elektřiny:

a) *„výrobna s celkovým instalovaným elektrickým výkonem nejméně 500 MW,*

b) *výrobna poskytující podpůrné služby s celkovým instalovaným elektrickým výkonem nejméně 100 MW,*

c) *vedení pro vyvedení výkonu a zabezpečení vlastní spotřeby výrobny elektřiny,*

d) *dispečink výrobce elektřiny.“* [17]

2. Přenosová soustava:

a) *„vedení přenosové soustavy o napětí nejméně 110 kV,*

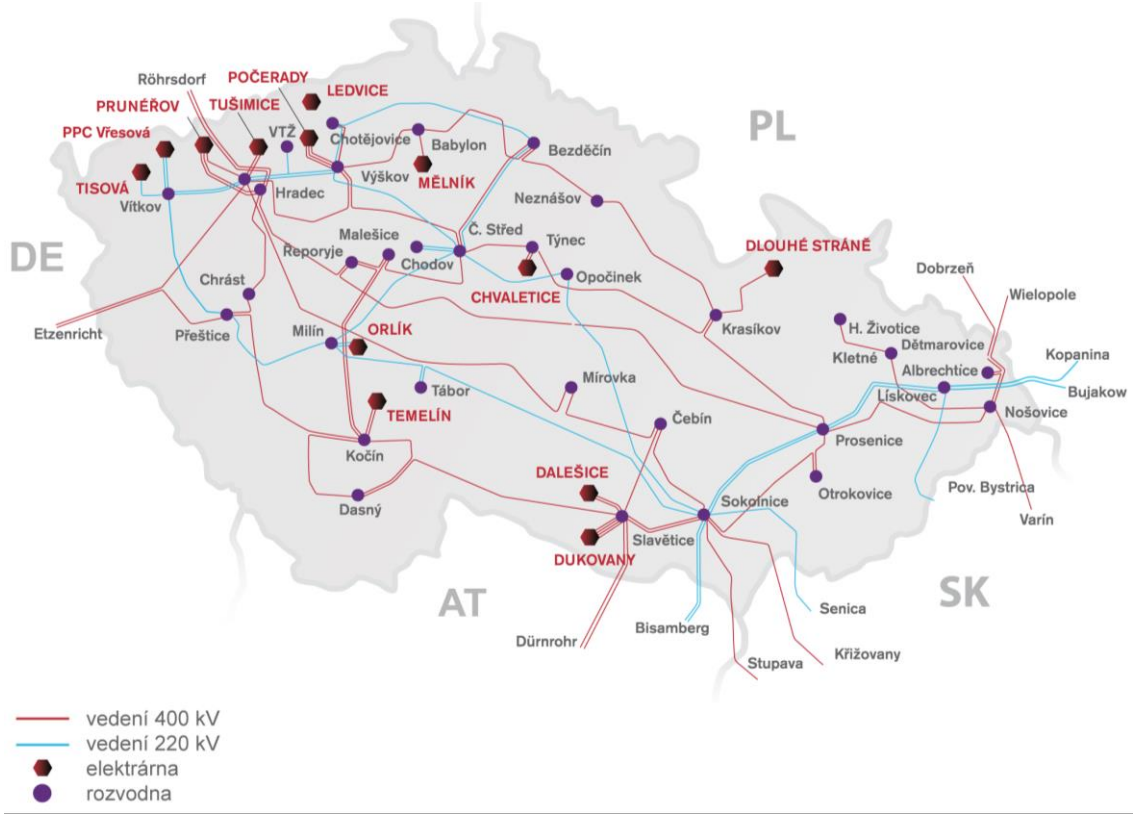
b) *elektrická stanice přenosové soustavy o napětí nejméně 110 kV,*

c) *technický dispečink provozovatele přenosové soustavy.“* [17]

3. Distribuční soustava:

a) *„elektrická stanice distribuční soustavy a vedení o napětí 110 kV (stanice typu 110/10 kV, 110/22 kV a 110/35 kV a k nim patřící vedení se posuzují podle jejich strategického významu v distribuční soustavě),*

b) *technický dispečink provozovatele distribuční soustavy*.“ [17]



Obr. 5 Schéma rozvodné sítě ČR [22]

8.2.2 Elektřina v regionu

Elektřina je na území Pardubického kraje distribuována vedením sítí velmi vysokého napětí (VVN) 110 kV, sítí vysokého napětí (VN) 35; 22; 10 a 6 kV a sítí nízkého napětí (NN) 400/220 V. Přenosové trasy tvoří nadzemní stožárová vedení s VVN hladiny 400 kV a 220 kV. Pro lepší představu soustavy elektrizačního vedení v Pardubickém kraji, je v příloze P I Mapa liniových tras elektrického vedení Pardubického kraje.

Místem napájení distribuční sítě 110 kV jsou transformovny 400/110 kV a 220/110 kV. Zařízení jsou v kombinovaném vlastnictví – část transformoven s hladinou napětí 400 kV a 220 kV včetně transformace VVN/VVN patří ČEPS, a. s.. Část těchto 110 kV objek-

tů je v majetku ČEZ, a. s. Dále je elektřina s napěťovou hladinou 110 kV dodávána z elektráren zapojených do sítě 110 kV Pardubického kraje. Dodávka z přenosové soustavy je realizována ze dvou transformačních stanic, které patří do celostátní přenosové soustavy provozované ČEPS a.s.: [24]

- **Krasíkov** (ORP Lanškroun) – 400/110 kV,
- **Opočínek** (ORP Pardubice) – 220/110 kV.

8.2.2.1 Transformační stanice Krasíkov

Transformační stanice Krasíkov má největší podíl na pokrytí spotřeby Pardubického kraje. Nachází se zde tři transformátory s napětím 400/110 kV o výkonu 2 x 250 MVA a 1 x 350 MVA. Velikost dodávky z této transformační stanice do Pardubického kraje je závislá na rozsahu sítě a tím na počtu transformátorů 110 kV/VN zapojených na vedení 110 kV vycházející z transformační stanice Krasíkov. Zapojení je možné měnit podle provozní situace a hospodárnosti distribuce. [24]

V rozvodně 110 kV Krasíkov je na směru do Pardubického kraje zapojen nejméně jeden transformátor 400/110 kV. Z tohoto transformátoru je zpravidla napájeno 8 distribučních transformačních stanic 110 kV/VN se souhrnným výkonem cca 200 MVA a dále ještě čtyři velkoodběratelé. Tři z těchto velkoodběratelů (České dráhy a. s.) představují poměrně malé odběry. Čtvrtým, významnějším velkoodběratelem, je VERTEX Litomyšl. [24]

8.2.2.2 Transformační stanice Opočínek

Transformační stanice v Opočínku má dva transformátory 220/110 kV po 200 MVA. Na tuto transformační stanici je zapojeno 6 transformoven 110 kV/VN. Do této oblasti dodává elektrickou energii také zdroj Opatovice.

Propojení mezi Týncem nad Labem a Opočínkem je jedním dvojitým vedením 110 kV přes rozvodnu elektrárny Chvaletice, které zajišťuje vlastní spotřebu elektrárny. Může však sloužit pro dodávku v nouzových stavech, při určitém druhu poruch nebo revizích zařízení distribuční sítě. V dalších sousedních transformačních stanicích za hranicemi kraje (Mírovka a Neznášov) jsou vždy dva transformátory 400/110 kV s výkonem 250 MVA (každý stroj). [24]

8.2.2.3 Zdroje elektrické energie

Mimo zmíněné transformovny nadřazeného systému se nacházejí v řešeném území dva výrazné zdroje elektrické energie, parní elektrárny spalující hnědé uhlí. Jsou to elektrárny:

- **Opatovice nad Labem** s instalovaným elektrickým výkonem 363 MW,
- **Chvaletice** s instalovaným výkonem 820 MW.

Místní výrobní zdroje jsou zapojeny prakticky do všech napěťových úrovní, podle velikosti instalovaného výkonu. Do nižších hladin napětí jsou zapojeny výkonově menší zdroje.

Elektrárna Chvaletice je vyvedena do přenosové soustavy, a proto při jejím výpadku není tento velký výkon pro nouzové zásobování využitelný.

Pokud by propojení 400 kV a 220 kV Opočínek – Čechy střed – Krasíkov nezůstala provozuschopná, vytvořilo by se při rozpadu přenosové soustavy na území kraje několik „ostrovů“ napájených místními zdroji. Reálně je možné uvažovat s dodávkami elektřiny v západní části kraje, i za cenu přísných dispečerských omezení odběru. Nepříznivé důsledky krizové situace by byly výraznější ve východní části kraje, kde je místních zdrojů tak málo, že by nebyly schopné pokrýt potřebu. [24]

9 BEZPEČNOSTNÍ HROZBY PRO ENERGETIKU VYBRANÉHO REGIONU

Pojem bezpečnostní hrozby elektroenergetiky je možno chápat jako hrozby, které působí na zařízení pro výrobu, přenos a distribuci elektrické energie. K tomu, aby mohla hrozba působit, je nutná její aktivace, která vyžaduje zdroje (vytvoření podmínek pro její působení) lidské, materiální, časové a procesní. Hrozby poté využívají slabých míst v realizovaných protiopatřeních, překonávají je v čase a způsobují narušení, či vyřazení prvku KI. [25]

Energetická bezpečnost státu/regionu v oblasti elektroenergetiky může být ovlivněna ve třech základních rovinách:

1) bezpečnost zajištění energetických zdrojů,
2) bezpečnost energetických transformací a dopravy elektřiny (výroba a přenos elektřiny),
3) energetická bezpečnost konečných uživatelů elektřiny (distribuce elektřiny).

Hrozby, které ovlivňují energetickou bezpečnost v oblasti elektroenergetiky, můžeme rozdělit podle jejich charakteru na přírodní (naturogenní) a společenské (antropogenní). Přírodní hrozby, jsou velmi obtížně ovlivnitelné, jelikož jejich vznik a průběh jsou založeny převážně na přírodních a meteorologických podmínkách. Avšak některé z těchto přírodních hrozeb, jako jsou například povodně lze s určitým časovým předstihem předpovědět. Vzniká zde tedy prostor na realizování konkrétních opatření v době, než hrozba udeří. Oproti tomu společenské hrozby jsou plně závislé na lidském faktoru. Drtivá většina těchto hrozeb je nenadálých a jediným prostředkem na snížení jejich možného dopadu jsou preventivní opatření a vytváření možných scénářů průběhu pro jednotlivé hrozby. V průběhu posledních několika desítek let je možno pozorovat významný nárůst jejich počtu. Jde o spojení především z pohledu vědeckotechnického pokroku. Hrozby působící na elektroenergetiku můžeme tedy členit následovně: [25]

1. přírodní:

- meteorologické hrozby (přirozené povodně, větrné smršti, sněhové kalamity, lesní požáry),

- geologické hrozby (sesuvy půdy),

2. společenské:

- technologické hrozby (technologické havárie, zvláštní povodně, rozsáhlé poruchy inženýrských sítí, dopravní, železniční a letecké nehody),
- kriminální hrozby (terorismus, kriminalita),

Výrobny elektrické energie mohou být odstaveny vlivem:

- *přímého poškození určitého výrobního zařízení (z důvodu technické poruchy, vady materiálu, zanedbání údržby, živelní události, teroristického útoku, války),*
- *chybné funkce řídícího systému,*
- *nevhodného dispečerského zásahu nebo manipulace (selhání lidského činitele),*
- *rozpadu elektrické sítě výrobnou napájené,*
- *nedostatku paliva nebo jiných provozních hmot.* [26]

Přenosová a distribuční soustavy mohou být odstaveny vlivem:

- *přímého poškození určitého prvku vedení,*
- *chybné funkce řídícího systému nebo automaticky působících ochran,*
- *nevhodného dispečerského zásahu (chybného působení techniky, poškození, selhání lidského činitele),*
- *nerovnováhou mezi poptávkou a nabídkou v systému přesahující určitou mez.* [26]

9.1 Možné dopady

Události, které mohou způsobit narušení nebo ztrátu funkce jednoho, nebo i několika prvků KI, jsou závislé na své závažnosti, četnosti výskytu a velikosti území, na němž působí. Dopady těchto událostí mohou být regionálního, nebo celostátního charakteru. Zde je výčet možných dopadů [25]:

- *narušení dodávek vody, tepla a plynu pro domácnosti i pro průmysl,*
- *narušení zásobování potravinami a zbožím ve všech oblastech,*

- *absolutní kolaps v informační a komunikační infrastruktuře – zastavení provozu mobilní telefonní sítě i pevných linek, nefunkční informační severy (internet a řídicí systémy), velmi obtížné informování veřejnosti o situaci (zastavení funkce hromadných sdělovacích prostředků), výrazné omezení provozuschopnosti zabezpečovacích systémů apod.,*
- *narušení bankovního systému – pokladny, bankomaty, platební a kreditní karty a veškerý platební pohyb,*
- *výraznému omezení základní i specializované lékařské péče,*
- *zastavila by se veškerá výroba, obchod a služby,*
- *absolutnímu ochromení dopravy – vyřazení letecké, železniční a městské dopravy, chaos v silniční dopravě (nefunkční signalizace, komplikace při čerpání pohonných hmot, dopravní zácpy, vysoký počet dopravních nehod apod.),*
- *přestaly by fungovat základní funkce domácností obyvatel,*
- *došlo by k výraznému omezení funkcí státní správy i samosprávy.*

9.2 Fyzická ochrana kritické infrastruktury

Fyzická ochrana prvků elektrizační soustavy je nedílným prvkem komplexního zajištění bezpečnosti. Tvoří ji systém technických, organizačních a režimových opatření, jejichž účelem je zabránit neoprávněnému nakládání s majetkem a zajištění bezpečnosti osob. Efektivní a funkční fyzická ochrana je základním předpokladem pro dosažení požadované úrovně ochrany prvků KI v oblasti energetiky před vnějšími vlivy způsobenými lidským faktorem. [25]

Atomový zákon (zákon č. 18/1997 Sb.) [35] definuje fyzickou ochranu jako *„systém technických a organizačních opatření zabraňujících neoprávněným činnostem s jadernými zařízeními, jadernými materiály a vybranými položkami.“*

Fyzická ochrana je tedy právními předpisy definována pouze pro oblast jaderné energetiky. Pro zařízení výroby, přenosu a distribuce elektrické energie, především prvků KI se opatření fyzické ochrany realizují v rozsahu určeném provozovateli daného prvku. Jako celek není fyzická ochrana v České republice upravena žádným zvláštním právním předpisem, který by stanovil, jaká opatření fyzické ochrany jsou pro rozhodující a nezbytná

pro to, aby míra rizika ohrožení prvků KI byla snížena na akceptovatelnou úroveň s ohledem na reálné hrozby a ekonomické možnosti subjektů KI. [25]

Fyzická ochrana prvku KI by se měla skládat z režimových a technických opatření doplněných ostrahou objektu, za účelem:

- detekce možných hrozeb a narušení perimetrů,
- odrazení útočníků od svých záměrů zviditelněním připravenosti prvku,
- zamezení nekontrolovatelnému přístupu nepovolaných osob do příslušné bezpečnostní zóny a zajištění okamžité a adekvátní reakci na signály narušení.

9.2.1 Režimová opatření

„Režimová opatření fyzické ochrany jsou součástí interní bezpečnostní dokumentace vlastníka/provozovatele zařízení. Zahrnují opatření organizačního, personálního a provozního charakteru, která jsou východiskem pro účinný systém fyzické ochrany a mají přímou vazbu na další technická opatření fyzické ochrany a ostrahu.“ [25]

9.2.2 Technická opatření

„Systémy technické ochrany slouží ke snížení rizika poškození nebo zničení majetku na akceptovatelnou míru a vytváří podmínky pro včasnou reakci na rizikovou situaci s cílem eliminace útočníků nebo pachatelů.“ [25]

9.2.3 Ostraha

„Ostraha je bezpečnostní služba vykonávaná bezpečnostními pracovníky. Osoby pověřené výkonem ostrahy musí být pro tuto činnost svědomitě vybrány, náležitě proškoleny a také vycvičeny. Ostraha může být zajišťována vlastními zaměstnanci vlastníka/provozovatele objektu (profesionálními nebo neformálními bezpečnostními pracovníky) nebo smluvní bezpečnostní agenturou s profesionálními bezpečnostními pracovníky.“ [25]

10 POZNATKY O OCHRANĚ KRITICKÉ INFRASTRUKTURY VE VYBRANÉM REGIONU

10.1 Oblast zdravotnictví

Jak je možné si všimnout z přehledu KI v Pardubickém kraji, v regionu se nenachází žádný prvek KI z oblasti zdravotnictví. Základním problémem ochrany KI v oblasti zdravotnictví je totiž odvětvové kritérium pro určení prvků KI v oblasti zdravotnictví. Toto kritérium udává, že aby zdravotnické zařízení splňovalo status prvku KI, je nutné, aby celkový počet jeho akutních lůžek byl nejméně 2500. V Pardubickém kraji proběhlo sloučení původních 5 nemocnic do nového subjektu „Nemocnice Pardubického kraje, a. s.“. Avšak před tímto sloučením ani jedno zdravotnické zařízení v Pardubickém kraji kritérium 2500 akutních lůžek nesplňovalo, ostatně nesplňuje ho žádné zdravotnické zařízení v ČR. Tento problém tedy není krajského charakteru, ale jeví se jako celostátní a ukazuje na špatně nastavené parametry pro určování prvků KI v oblasti zdravotnictví. Přestože v reakci na vydaný „kybernetický zákon“ od 1. ledna 2015 nabylo účinnosti nařízení vlády č. 315/2014 Sb., kterým se mění nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, zůstalo toto nesmyslně nastavené kritérium bez povšimnutí. Gestorem KI v oblasti zdravotnictví je samozřejmě Ministerstvo zdravotnictví, to by tedy mělo vyvinout snahu směrem k upravení tohoto odvětvového kritéria. Jako nápravné opatření by mělo být toto kritérium jednoznačně upraveno, a to snížením hranice počtu akutních lůžek pro určení prvků KI v oblasti zdravotnictví. Upravení tohoto kritéria budu impulzem k důslednější ochraně vybraných zdravotnických zařízení, jakožto prvků KI.

Vytvoření subjektu „Nemocnice Pardubického kraje, a. s.“ Pardubickým krajem, by mělo umožnit kraji strategicky a komplexně rozvíjet systém zdravotnictví, zlepšit hospodaření s financemi, a také zjednodušit a zefektivnit řízení toho systému.

10.2 Oblast energetiky – elektřina

Elektrizační soustavu Pardubického kraje, stejně jako každou jinou, není možné z bezpečnostního hlediska v celém jejím rozsahu ochránit. Proto je tu systém určování prvků KI pomocí odvětvových a průřezových kritérií, který umožňuje identifikovat klíčové prvky elektroenergetického systému. Otázkou je, zda jsou tato kritéria nastavena správně.

Nejzranitelnější částí elektrizační soustavy je přenosová soustava, zejména její vedení a transformační stanice. Klíčovými prvky KI v elektrizační soustavě Pardubického kraje jsou především transformační stanice Krasíkov 400/110 kV a Opočínek 220/110 kV. Z hlediska fyzického útoku a možných škod, které by tento útok mohl způsobit, jsou tyto dva prvky KI nejatraktivnějším cílem v oblasti elektroenergetiky v Pardubickém kraji. Bez ohledu na příčiny může při současném vícenásobném narušení těchto aktiv dojít k rozpadu provozu přenosové soustavy regionu. Následkem může být rozsáhlý blackout, jelikož veřejné distribuční soustavy nejsou schopny samostatně, bez propojení s přenosovou soustavou, zabezpečit dodávky elektrické energie od výroben elektřiny ke spotřebitelům. Jestliže dojde k výpadku jedné rozvodny, dochází automaticky k jejímu odpojení a přesměrování na jinou (jiné). Pokud ovšem pracují ostatní rozvodny na hranici svého maxima, nejsou schopné zvýšenou zátěž unést, a také zkolabují. To může mít za následek dominový efekt, který vyřadí z provozu celou síť.

Pro zajištění přiměřené soběstačnosti je třeba zajistit schopnost distribuční soustavy pracovat nouzově, oddělené od přenosové soustavy. V tomto režimu by se měla opírat o místní zdroje elektřiny vyvedené do napěťových hladin distribuční soustavy (110 kV, 35 kV, 22 kV). S tím souvisí potřeba podpory výstavby náhradních zdrojů elektrické energie.

Největší příležitostí k zvýšení ochrany prvků KI v oblasti energetiky je především zvýšení snahy o prevenci násilného vniknutí do bezpečnostních zón prvků KI a snížení rizika možného zničení či poškození technologických zařízení a dalšího majetku. Tomu by mohlo napomoci zpracování předpisu, který by stanovil požadavky na fyzickou ochranu KI pro jednotlivé oblasti KI, v souladu s nařízením vlády o kritériích pro určení prvků KI. Toto úsilí musí být vyvinuto na národní úrovni, orgány regionální úrovně k tomuto nemají kompetence. Pro fyzickou ochranu prvku KI existuje v současné době norma ČSN 73 4450-1 Fyzická ochrana prvku kritické infrastruktury, která stanovuje obecné principy a požadavky využitelné pro všechna odvětví kritické infrastruktury. ČSN normy nejsou podle zákona obecně závazné. Normy jsou dobrovolné nástroje, které však zaručují uživateli postup v souladu s tím, který byl na národní úrovni schválen.

Pro zlepšení stavu fyzické ochrany KI a posuzování její adekvátní ochrany, bych doporučoval aplikování podobných kritérií, jako obsahuje *vyhláška č. 250/2006 Sb., kterou se*

stanoví rozsah a obsah bezpečnostních opatření fyzické ochrany objektu nebo zařízení zařazených do skupiny A nebo do skupiny. [36]

Podle zákona č. 59/2006 Sb., o prevenci závažných havárií způsobených vybranými nebezpečnými chemickými látkami nebo chemickými přípravky [37], se určují objekty a zařízení, kde jsou umístěny a využívány vybrané nebezpečné chemické látky. Tato vyhláška stanovuje konkrétní režimová opatření, technické prostředky a požadavky na fyzickou ostrahu takovýchto objektů. Dle mého názoru, by kritéria této vyhlášky č. 250/2006 Sb., byla aplikovatelná na oblast energetiky a její podoblasti, tj. pro elektřinu, zemní plyn, ropu a ropné produkty, a také centrální zásobování teplem.

Navrhované řešení by pomohlo zefektivnit fyzickou ochranu prvků KI v oblasti energetiky a stanovilo by jejich provozovatelům konkrétní kritéria pro ochranu prvku KI. Dále by zjednodušila posuzování fyzické ochrany prvků KI, z hlediska jejich adekvátnosti.

ZÁVĚR

V teoretické části jsou shrnuty poznatky o KI, které vycházejí z platné legislativy, z materiálů, které jsou uvedeny v seznamu literatury a z poznatků získaných během odborných konzultací. Tyto zdroje slouží také jako základ praktické části této práce.

Praktická část práce je zaměřena na 2 oblasti národní KI ve vybraném regionu. První z nich je oblast zdravotnictví, která je v současné době velmi opomíjenou oblastí z hlediska určování prvků KI a jejich ochrany. Druhou rozebíranou oblastí je energetika, konkrétně její podoblast – elektřina. Elektroenergetika patří naopak mezi oblasti, které jsou prioritní jak v rámci národní, tak i v rámci nadnárodní KI. Význam, který je elektroenergetice přisuzován, vyplývá jednak z faktu, že je to systém, který je úzce propojen s ostatními oblastmi KI, a jehož selhání se projeví značnými dopady v těchto oblastech, a také z faktu, že jde o nejzranitelnější oblast KI. Z tohoto důvodu je potřeba klíčové prvky této KI správně identifikovat a posoudit potencionální rizika ohrožení a v návaznosti na tento krok, přijmout adekvátní bezpečnostní opatření, zajišťující dostatečnou ochranu těchto prvků. Realizováním těchto kroků dochází nejen k ochraně samotných prvků, ale i ke zvýšení zabezpečení základních životních potřeb obyvatelstva, výrobní sféry a dalších oblastí, které jsou na dodávkách elektrické energie závislé.

SEZNAM POUŽITÉ LITERATURY

[1] ČESKO. Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů. Dostupné z: http://www.zakonyprolidi.cz/cs/2000-240

[2] ŠENOVSKÝ, Michail, Vilém ADAMEC a Pavel ŠENOVSKÝ. Ochrana kritické infrastruktury. 1. vyd. V Ostravě: Sdružení požárního a bezpečnostního inženýrství, 2007, 141 s. ISBN 978-80-7385-025-8.

[3] MOZGA, Jaroslav, Miloš VÍTEK a František KOVÁŘÍK. Kritická infrastruktura společnosti. Vyd. 1. Hradec Králové: Gaudeamus, 2008, 156 s. ISBN 978-80-7041-299-2.

[4] KOMISE EVROPSKÝCH SPOLEČENSTVÍ. *ZELENÁ KNIHA O EVROPSKÉM PROGRAMU NA OCHRANU KRITICKÉ INFRASTRUKTURY*. Brusel, 2005. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:52005DC0576&rid=1

[5] MINISTERSTVO VNITRA-GENERÁLNÍ ŘEDITELSTVÍ HASIČSKÉHO ZÁCHRANNÉHO SBORU ČR. *Krizové řízení při nevojenských krizových situacích: modul C* [online]. Praha, 2008 [cit. 2015-03-01]. ISBN 978-80-86640-93-8. Dostupné z: http://www.hzscr.cz/soubor/vzdelavani-v-krizovem-rizeni-moduly-modul-c-pdf.aspx

[6] KOLEŇÁK, Ivan, Daniel MIKLÓS a Marika ROSINOVÁ. NOVELIZACE KRIZOVÉHO ZÁKONA. In: KRIZOVÝ MANAGEMENT 2011: 10 let krizového řízení - teorie pro praxi [online]. 2011 [cit. 2015-03-01]. ISBN 978-80-7395-411-6. Dostupné z: http://www.upce.cz/fes/veda-vyzkum/konference/krizovy-management/sbornik-km-11.pdf

[7] PECINA, M. Komplexní strategie České republiky k řešení problematiky kritické infrastruktury a Národní program ochrany kritické infrastruktury [online]. 2009. [cit. 2015-03-01] Dostupný z: http://krizport.firebrno.cz/file/132

[8] Plán krizové připravenosti. HZS JMK. Portál krizového řízení JmK [online]. [cit. 2015-03-07]. Dostupné z: http://krizport.firebrno.cz/dokumenty/plan-krizove-pripravenosti

[9] Evropská unie. SMĚRNICE RADY 2008/114/ES: o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu. In: 2008. Dostupné z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:CS:PDF

[10] VILÁŠEK, Josef a Jan FUS. Krizové řízení v ČR na počátku 21. století. Vyd. 1. Praha: Karolinum, 2012, 264 s. ISBN 978-80-246-2170-8.

[11] Ochrana obyvatel 2007: Ochrana kritické infrastruktury [online]. Ostrava: Sdružení požárního a bezpečnostního inženýrství, 2007[cit. 2015-03-12]. ISBN 80-86634-51-5. Dostupné z: http://www.spbi.cz/download.php?param=L3Zhci93d3cvdmhvc3RzL3NwYmkuY3ovaHR0cGRvY3MvcmVzL2R3ZS1maWxlcy85NTg4O09PYiAyMDA3LnBkZg==

[12] SDĚLENÍ KOMISE: o Evropském programu na ochranu kritické infrastruktury. In: KOM(2006) 786. Brusel, 2006. Dostupné z: http://www.hzscr.cz/soubor/sdeleni-komise-o-epcip-2006-pdf.aspx

[13] Evropská unie. PRACOVNÍ DOKUMENT KOMISE: o novém přístupu k Evropskému programu na ochranu kritické infrastruktury. In: SWD(2013) 318 v konečném znění. 2013. Dostupné z: http://www.hzscr.cz/soubor/pracovni-preklad-dok-ek-novy-pristup-k-epcip-pdf.aspx

[14] ROSINOVÁ, Marika. AKTUÁLNÍ STAV URČENÍ PRVKŮ KRITICKÉ INFRASTRUKTURY V ČESKÉ REPUBLICE. Časopis 112 [online]. 2012, ČÍSLO 10 [cit. 2015-03-15]. Dostupné z: http://www.hzscr.cz/clanek/informacni-servis-casopis-112-2012-casopis-112-rocnik-xi-cislo-10-2012.aspx?q=Y2hudW09NQ%3D%3D

[15] ŠINDLEROVÁ, Barbora a Marika ROSINOVÁ. NOVELIZACE KRITÉRIÍ PRO URČENÍ PRVKU KRITICKÉ INFRASTRUKTURY. Časopis 112 [online]. 2015, ČÍSLO 2 [cit. 2015-03-017]. Dostupné z: http://www.hzscr.cz/clanek/casopis-112-rocnik-xiv-cislo-2-2015.aspx?q=Y2hudW09NA%3D%3D

[16] PROCHÁZKOVÁ, Dana. KRITICKÁ INFRASTRUKTURA A JEJÍ PROBLÉMY.

[17] ČESKO. Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury

[18] ŘÍHA, Josef. TYPOLOGICKÉ ZNAKY KRITICKÉ INFRASTRUKTURY. In: THE SCIENCE FOR POPULATION PROTECTION [online]. 2009 [cit. 2015-03-25]. Dostupné z: http://www.population-protection.eu/prilohy/casopis/6/43.pdf

[19] MINISTERSTVO ZAHRANIČNÍCH VĚCÍ ČESKÉ REPUBLIKY. Bezpečnostní strategie České republiky [online]. Praha, 2015 [cit. 2015-03-25]. ISBN 978-80-7441-005-

5. Dostupné z: http://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf

[20] ROSTEK, Petr a Vilém ADAMEC. KRITICKÁ INFRASTRUKTURA NA ÚROVNI ÚZEMNÍCH SYSTÉMŮ. In: THE SCIENCE FOR POPULATION PROTECTION [online]. 2012 [cit. 2015-03-30]. 2. Dostupné z: http://www.population-protection.eu/prilohy/casopis/13/101.pdf

[21] ČESKÝ STATISTICKÝ ÚŘAD. Český statistický úřad [online]. [cit. 2015-04-07]. Dostupné z: https://www.czso.cz/

[22] ČEPS, A.S. 2015. ČEPS, a.s., [online]. [cit. 2015-04-07]. Dostupné z: http://www.ceps.cz/CZE/Stranky/default.aspx

[23] HASIČSKÝ ZÁCHRANNÝ SBOR PARDUBICKÉHO KRAJE. 2013. Krizový plán Pardubického kraje.

[24] PARDUBICKÝ KRAJ KRAJSKÝ ÚŘAD, ODDĚLENÍ KRIZOVÉHO ŘÍZENÍ. 2008. INFRASTRUKTURA NA TERITORIU PARDUBICKÉHO KRAJE: LINIOVÉ STAVBY ZÁSOBENÍ ELEKTRICKOU ENERGIÍ, PLYNEM A TEPLEM.

[25] Kritická infrastruktura elektroenergetiky: určování, posuzování a ochrana. 2013. 1. vyd. V Ostravě: Sdružení požárního a bezpečnostního inženýrství, 79 s. Spektrum (Sdružení požárního a bezpečnostního inženýrství). ISBN 978-80-7385-126-2.

[26] Typový plán pro řešení krizové situace narušení dodávek elektrické energie velkého

rozsahu [online]. Ministerstvo průmyslu a obchodu, 2011 [cit. 2015-04-12].

Dostupné z: http://download.mpo.cz/get/26093/48806/574890/priloha007.doc.

[27] ČESKO. Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky

[28] UNITED STATES OF AMERICA. PRESIDENTIAL DECISION DIRECTIVE/NSC-63. 1998. In: . THE WHITE HOUSE. Dostupné také z: http://fas.org/irp/offdocs/pdd/pdd-63.htm

[29] Centre for the Protection of National Infrastructure [online]. [cit. 2015-04-12]. Dostupné z: http://www.cpni.gov.uk/

[30] ČESKO. Ústavní zákon č. 110/1998 Sb. o bezpečnosti České republiky. Dostupné z: http://www.zakonyprolidi.cz/cs/1998-110

[31] ČESKO. Zákon č. 239/2000 Sb. o integrovaném záchranném systému. Dostupné z: http://www.zakonyprolidi.cz/cs/2000-239

[32] ČESKO. Zákon č. 241/2000 Sb. o hospodářských opatřeních pro krizové stavy. Dostupné z: http://www.zakonyprolidi.cz/cs/2000-241

[33] ČESKO. Zákon č. 430/2010 Sb., kterým se mění zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů. Dostupné z: http://www.zakonyprolidi.cz/cs/2010-430

[34] ČESKO. Nařízení vlády č. 432/2010 Sb. o kritériích pro určení prvku kritické infrastruktury. Dostupné z: http://www.zakonyprolidi.cz/cs/2010-432

[35] ČESKO. Zákon č. 18/1997, o mírovém využívání jaderné energie a ionizujícího záření (atomový zákon) a o změně a doplnění některých zákonů. Dostupné z: http://www.zakonyprolidi.cz/cs/1997-18

[36] ČESKO. Vyhláška č. 250/2006 Sb., kterou se stanoví rozsah a obsah bezpečnostních opatření fyzické ochrany objektu nebo zařízení zařazených do skupiny A nebo do skupiny B. Dostupné z: http://www.zakonyprolidi.cz/cs/2006-250

[37] ČESKO. Zákon č. 59/2006 Sb., o prevenci závažných havárií způsobených vybranými nebezpečnými chemickými látkami nebo chemickými přípravky. Dostupné z: http://www.zakonyprolidi.cz/cs/2006-59

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

KI	kritická infrastruktura
ČR	Česká republika
EKI	evropská kritická infrastruktura
EU	Evropská unie
USA	Spojené státy americké
ÚSÚ	ústřední správní úřad
ORP	obec s rozšířenou působností
PKP	plán krizové připravenosti
EPCIP	Evropský program pro ochranu kritické infrastruktury
CIWIN	Výstražná informační síť kritické infrastruktury

SEZNAM OBRÁZKŮ

Obr. 1 Územně důležitá infrastruktura [20] 27
Obr. 2 Poloha Pardubického kraje v rámci ČR a znak Pardubického kraje 29
Obr. 3 Administrační členění Pardubického kraje [21] 30
Obr. 4 Seznam možných rizik na území Pardubického kraje [23] 31
Obr. 5 Schéma rozvodné sítě ČR [22] 36

SEZNAM TABULEK

Tab. 1 Oblasti národní kritické infrastruktury [17] 26
Tab. 2 Prvky KI určené ostatními správními úřady [23] 33