



ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

FAKULTA BIOMEDICÍNSKÉHO INŽENÝRSTVÍ
Katedra zdravotnických oborů a ochrany obyvatelstva

Ochrana kritické infrastruktury ČR v odvětví zemní plyn, ropa a ropné produkty

Protection of Critical Infrastructure in the Czech Republic in Natural Gas, Oil and Petroleum Products Sector

Bakalářská práce

Studijní program: Ochrana obyvatelstva
Studijní obor: Plánování a řízení krizových situací
Autor bakalářské práce: Daniel Ondra
Vedoucí bakalářské práce: Mgr. Petr Houdek

Kladno 2020



ZADÁNÍ BAKALÁŘSKÉ PRÁCE

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení: **Ondra** Jméno: **Daniel** Osobní číslo: **473917**
Fakulta: **Fakulta biomedicínského inženýrství**
Garantující katedra: **Katedra zdravotnických oborů a ochrany obyvatelstva**
Studijní program: **Ochrana obyvatelstva**
Studijní obor: **Plánování a řízení krizových situací**

II. ÚDAJE K BAKALÁŘSKÉ PRÁCI

Název bakalářské práce:

Ochrana kritické infrastruktury ČR v odvětví zemní plyn, ropa a ropné produkty

Název bakalářské práce anglicky:

Protection of Czech Critical Infrastructure in the Sectors of Natural Gas, Oil and Petroleum Products

Pokyny pro vypracování:

Předmětem práce bude zhodnocení současného stavu ochrany kritické infrastruktury v ČR a navržení určitých opatření ke zlepšení. Teoretická část obsáhne vymezení pojmů, historický vývoj kritické infrastruktury, ohrožení kritické infrastruktury a strategie ochrany kritické infrastruktury. Dále bude popsána oblast národní energetické kritické infrastruktury. V praktické části budou prostřednictvím analýz AKIS identifikován současný stav. Bude provedena analýza dopadů rizik poškození, ohrožení, celkové zranitelnosti v oblastech zemní plyn, ropa a ropné produkty. V závěru budou navrženy možnosti, které by vedly ke zlepšení v oblasti ochrany kritické infrastruktury v ČR.

Seznam doporučené literatury:

- [1] ŠENOVSÝ, Michail, ADAMEC, Vilém, ŠENOVSÝ, Pavel, Ochrana kritické infrastruktury, Ostrava: Sdružení požárního a bezpečnostního inženýrství, 2007, ISBN 978-80-7385-025-8
- [2] BLAŽKOVÁ, Kateřina a kol., Ochrana obyvatelstva a krizové řízení, Praha: MV – generální ředitelství Hasičského záchranného sboru ČR, 2015, 323 s., ISBN 978-80-86466-62-0
- [3] Kolektiv autorů pod vedením Ministerstva zahraničních věcí ČR, Bezpečnostní strategie ČR 2015, Praha: Ministerstvo zahraničních věcí České republiky, 2015, 23 s., ISBN 978-80-7441-005-5
- [4] Kolektiv autorů, Ochrana kritické infrastruktury, Praha: Česká asociace bezpečnostních manažerů, 2011, 189 s., ISBN 978-80-260-1215-3

Jméno a příjmení vedoucí(ho) bakalářské práce:

Mgr. Petr Houdek

Jméno a příjmení konzultanta(ky) bakalářské práce:

Datum zadání bakalářské práce: **17.02.2020**

Platnost zadání bakalářské práce: **19.09.2021**


prof. MUDr. Leoš Navrátil, CSc., MBA, dr.h.c.
podpis vedoucí(ho) katedry

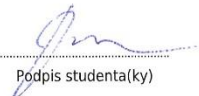

prof. MUDr. Ivan Dylevský, DrSc.
podpis děkana(ky)

III. PŘEVZETÍ ZADÁNÍ

Student(ka) bere na vědomí, že je povinnen(a) vypracovat bakalářskou práci samostatně, bez cizí pomoci, s výjimkou poskytnutých konzultací. Seznam použité literatury, jiných pramenů a jmen konzultantů je třeba uvést v bakalářské práci.

30.6.2020

Datum převzetí zadání



Podpis studenta(ky)

PROHLÁŠENÍ

Prohlašuji, že jsem bakalářskou práci s názvem „Ochrana kritické infrastruktury ČR v odvětví zemní plyn, ropa a ropné produkty“ vypracoval samostatně pouze s použitím pramenů, které uvádím v seznamu bibliografických odkazů.

Nemám závažný důvod proti užití tohoto školního díla ve smyslu § 60 zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.

V Roudnici nad Labem dne 06.08.2020

.....
Daniel Ondra

PODĚKOVÁNÍ

Na tomto místě bych chtěl poděkovat Mgr. Petr Houdkovi, vedoucímu mé bakalářské práce, za cenné připomínky, odborné vedení a podnětné rady, kterými velkou měrou přispěl k vypracování této diplomové práce.

Rád bych také poděkoval své ženě za trpělivost a její podporu při studiu, bez které bych se jistě k napsání této bakalářské práce nedostal.

ABSTRAKT

Tématem této bakalářské práce je ochrana kritické infrastruktury České republiky v odvětví zemní plyn, ropa a ropné produkty.

Teoretická část vysvětluje problematiku kritické infrastruktury, přístupu České republiky k její ochraně a legislativnímu procesu určování prvků kritické infrastruktury. Současně je vysvětlena implementace evropského práva do oblasti ochrany kritické infrastruktury České republiky. V dalších částech práce jsou popsány hrozby ohrožující kritickou infrastrukturu a bezpečnostní opatření, která mají za cíl, úroveň stávajícího rizika snížit. Dále jsou popsány a vysvětleny jednotlivé vybrané oblasti kritické infrastruktury.

Závěrečná část práce se zabývá bezpečnostní analýzou AKIS současného stavu kritické infrastruktury v oblastech zemního plynu, ropy a ropných produktů.

Klíčová slova

kritická infrastruktura; ochrana kritické infrastruktury; zemní plyn; ropa; ropné produkty

ABSTRACT

This bachelor thesis deals with a protection of critical infrastructure in the Czech Republic in Natural Gas, Oil and Petroleum Products sectors.

The theoretical part explains the problematics of critical infrastructure, the Czech Republic's approach to its protection and the legislative process of determining critical infrastructure elements. The implementation of European law in the Czech Republic's critical infrastructure protection is also explained in the theoretical part. The next of the thesis describes the threats of critical infrastructure and security measures helping to reduce the level of existing risk. Additionally, the individual selected sectors of critical infrastructure are described and explained.

The final part of the thesis deals with current state AKIS safety analysis of critical infrastructure in Natural Gas, Oil and Petroleum Products sectors.

Keywords

critical infrastructure; critical infrastructure protection; natural gas; oil; petroleum products

Obsah

1	ÚVOD	10
2	CÍLE PRÁCE	11
3	PŘEHLED SOUČASNÉHO STAVU	12
3.1	Infrastruktura	13
3.2	Kritická infrastruktura	14
3.2.1	Historický vývoj ochrany kritické infrastruktury ve světě	16
3.2.2	Vývoj ochrany kritické infrastruktury v ČR.....	18
3.2.3	Evropská kritická infrastruktura.....	24
3.3	Hrozby kritické infrastruktury	27
3.4	Bezpečnostní opatření k ochraně kritické infrastruktury	31
3.4.1	Fyzická ochrana	32
3.4.2	Bezpečnost informačních systémů.....	33
3.4.3	Komunikační bezpečnost	34
3.4.4	Kybernetická bezpečnost	34
3.4.5	Administrativní bezpečnost	34
3.4.6	Personální bezpečnost	34
3.4.7	Management ochrany kritické infrastruktury.....	35
3.5	Určení prvku kritické infrastruktury ČR	35
3.6	Energetická oblast KI ČR.....	38
3.7	Zemní plyn	40
3.7.1	Plynárenská soustava ČR.....	42
3.7.2	Přepravní soustava zemního plynu.....	43
3.7.3	Skladování plynu	43

3.7.4	Distribuční soustava	45
3.8	Ropa a ropné produkty	45
3.8.1	Ropovodná síť ČR	48
3.8.2	Skladování ropy	49
3.8.3	Ropné produkty	50
3.8.4	Výroba pohonných hmot	52
4	METODIKA	55
4.1	Analýza AKIS	56
5	VÝSLEDKY	59
5.1	Analýza AKIS odvětví zemního plynu	60
5.2	Analýza AKIS ropy a ropných produktů	69
6	DISKUZE	78
7	ZÁVĚR	85
8	SEZNAM POUŽITÝCH ZKRATEK	86
9	SEZNAM POUŽITÉ LITERATURY	87
10	SEZNAM POUŽITÝCH OBRÁZKŮ	94
11	SEZNAM POUŽITÝCH TABULEK	95
12	SEZNAM PŘÍLOH	97

1 ÚVOD

Lidstvo je vystaveno různým rizikům odjakživa. Tyto hrozby se postupem času a rozvojem lidské společnosti měnily, některé z nich přestaly člověka ohrožovat a jiné nové se naopak objevily. S rostoucí lidskou populací na této planetě a rychle se rozvíjející, materialisticky založenou společností, člověk se rozhodl některé z hrozeb, se kterými přicházel do styku každodenně, jednoduše přehlížet. Mnohdy ho začaly znovu zajímat až ve chvíli, kdy tato ohrožení způsobila již trvalé dopady (například na životní prostředí) nebo došlo k mimořádné události (havárii, katastrofě apod.) takových rozměrů, že již jednoduše nebylo možné dopustit v budoucnu něco podobného.

Každá takováto událost ve své podstatě zapříčinila následné zvýšení úrovně bezpečnosti daného odvětví, systému. Mnoho bezpečnostních dokumentů nese jméno právě po havárii s katastrofálními následky z hlediska počtu obětí, způsobených škod na majetku nebo dlouhodobého poškození životního prostředí. Mezinárodní společnosti, jako například Organizace spojených národů nebo později Evropská unie (dále také „EU“), postupem času donutily členské země, začít řešit problematiku bezpečnosti zmíněných infrastruktur a identifikovaná rizika zapracovávat do jejich bezpečnostních plánů.

Stále pokračující technologický rozvoj znamenal a znamená pro lidskou společnost obrovský přínos, v mnohém člověku život usnadnil. Získané životní pohodlí ovšem na druhou stranu přináší také jistá rizika. Lidé jsou dnes zcela závislí na dodávkách pitné vody, celé oblasti ekonomiky nemohou fungovat bez dodávek elektřiny, pohonných hmot, zemního plynu nebo ropy. Zajištění funkčnosti takovýchto infrastruktur se tedy stalo životně (kriticky) důležité a bezpečnostní hrozby kritické infrastruktury jsou tedy ve své podstatě hrozbami, ohrožujícími kteréhokoliv z nás.

2 CÍLE PRÁCE

Cílem této bakalářské práce je čtenáři přiblížit problematiku ochrany kritické infrastruktury České republiky v odvětvích zemního plynu, ropy a ropných produktů. Práce nastíní vývoj, jakým si tato bezpečnostní oblast prošla, dále vysvětlí hrozby, které tuto kritickou infrastrukturu ohrožují. Práce také zmíní bezpečnostní opatření k její ochraně. Dále bude vysvětlen legislativní rámec, který ochranu kritické infrastruktury vymezuje, zmíní implementaci požadované legislativy ze strany mezinárodních organizací.

Výstupem této práce bude zpracování analýzy vybraných odvětví metodou AKIS. Analýza rozdělí posuzovaná odvětví zemního plynu, ropy a ropných produktů na dílčí sektory.

3 PŘEHLED SOUČASNÉHO STAVU

Lidská společnost si za poslední staletí prošla dynamickým vývojem. Věci, které byly pro obyčejného člověka před sto lety nepředstavitelné, se dnes mnohdy stávají skutečností. Vývoj, jež započal průmyslovou revolucí a elektrifikací, v současnosti opět pokračuje například díky „chytrým“ technologiím. Všechny tyto výtěžky moderní doby člověku život usnadnily. Na druhou stranu je třeba říci, že jsme na mnohých z nich značně závislí a díky této závislosti i zranitelnější.

Ve dávných dobách se lidé jistě také obávali jistých hrozeb a snažili se ochránit své jmění, majetek a další cennosti. Hrozby se vesměs daly eliminovat jednoduchým řešením. Byla-li lidem zima, stačil oheň a ten je ochránil také před divokými zvířaty. Později, když jim hrozil nepřítel, postavily se okolo města nedobytné hradby. Bylo-li potřeba více vody či jídla, vykopala se studna nebo se jednoduše navýšilo množství uskladněných zásob potravin. V dnešním světě to již tak jednoduše neplatí. Města, dnes dokonce i celé státy (Schengenský prostor v rámci Evropské unie) umožňují v podstatě zcela volný pohyb osob a není potřeba je tedy dobývat. Člověk se díky všem vymoženostem stal životně závislý na úplně jiných věcech. K ochromení velkého počtu osob je dnes stačí připravit o elektrickou energii, tekoucí vodu nebo útočník může paralyzovat kupříkladu dopravní systém velkého města. Právě zmíněná elektřina je pro člověka nesmírně důležitá, protože bez ní často nefungují ani další životně důležité infrastruktury. To jsou některé z hodnot, které současná společnost kriticky potřebuje pro svůj život a je na státu, aby tyto služby v nezbytně nutné míře pro své občany dokázal zabezpečit.

Tato potřeba nutí daný stát k tomu, aby jasně definoval základní zájmy a hodnoty, které se snaží chránit. Stejně tak musí stát definovat nástroje, přístupy a v neposlední řadě i cíle v oblasti zajišťování své ochrany a bezpečnosti.

Z hlediska bezpečnosti České republiky je takovýmto stěžejním a definujícím dokumentem „Bezpečnostní strategie České republiky“. Tato strategie ve svém textu objasňuje principy, na kterých bezpečnostní politika ČR stojí, popisuje bezpečnostní zájmy ČR. Dokument analyzuje z bezpečnostního hlediska prostředí, ve kterém Česká republika jako stát funguje, zmiňuje konkrétní hrozby a jejich vývojové trendy [1].

Jedním ze základních úkolů vlády, jakožto i všech územních samosprávních celků, je zajistit příslušnou míru bezpečnosti obyvatel, bránit územní celistvost a svrchovanost státu, stejně tak jako se podílet na udržení demokratických principů právního státu. K zajištění takto důležitých cílů musí mít zodpovědné instituce logicky také odpovídající nástroje. Takovýmto nástrojem je dostatečně připravený a funkční bezpečnostní systém ČR. Připravenost systému tkví v tom, že je tento systém připraven pružně a rychle reagovat na měnící se hrozby a bezpečnostní situaci uvnitř České republiky, stejně jako ve světě [1].

Za jeden z nejdůležitějších bezpečnostních úkolů státu tedy můžeme považovat ochranu a rozvoj lidské společnosti, to za všech okolností – ať se jedná o běžné podmínky nebo při krizových situacích, či válečných stavech.

3.1 Infrastruktura

Pojem Infrastruktura není pojmem nikterak novým. Poprvé se objevil ve Francii v 19. století. Původně označoval vojenská zařízení, především během první a druhé světové války. Poté se tento pojem znovu objevil v průběhu Kubánské krize v roce 1962. Zmíněná krize poukázala na potřebu lepšího zajištění komunikačních sítí. Postupem času se naštěstí podařilo napětí mezi hlavními světovými mocnostmi urovnat a od konce dvacátého století začínají infrastrukturu ohrožovat hrozby převážně nevojenského charakteru. Termín infrastruktura byl stále častěji využíván ve spojitosti s ochranou obyvatel

a společnosti jako takové, zajištění kontinuity dodávek strategických surovin apod [2].

Výsledek snahy definovat infrastrukturu, může mít mnoho odlišných podob. Záležet bude převážně na tom, v jakém kontextu a odvětví se o to pokusíme. Obecnou definicí můžeme říci, že infrastruktura jsou uměle vytvořené sítě či objekty, které tvoří jakousi množinu vzájemně propojených prvků. Může se týkat mnoha rozličných oblastí jako například dopravy (dopravní stavby, silnice nebo letiště), zásobování vodou nebo třeba přenosu elektrické energie. Infrastruktura může být ve vlastnictví či užívání státu, stejně jako soukromého sektoru [3].

3.2 Kritická infrastruktura

Státy v současnosti poskytují svým obyvatelům mnoho služeb. S rozvojem moderních technologií se systémy, které tyto služby poskytují, stávají technologicky složitějšími a ruku v ruce s tím také zranitelnějšími. Pokud je tedy stát zodpovědný za zajištění základních životních potřeb svých obyvatel, musí zajistit svou funkčnost společně se všemi potřebnými službami. Takovéto služby je pak logicky nucen chránit a udržovat ve funkčním stavu.

Existují pak tedy systémy (infrastruktura), které jsou pro stát velmi (kriticky) důležité. Takovýto systém je pro fungování státu nezbytný a můžeme ho tedy nazvat kritickou infrastrukturou (dále také „KI“). Infrastruktura má uspořádání podobné síti, kdy se sítě skládají z jednotlivých prvků a spojnic. Místa, ve kterých se propojuje více prvků, se nazývají „uzly“. Jednotlivé uzly mají z hlediska bezpečnosti KI různou důležitost. Pokud by došlo k poškození či zničení některého z důležitých uzlů, mohlo by to mít za následek vyřazení celé této kritické infrastruktury. Z tohoto důvodu by mělo být prvořadým zájmem

každého vyspělého státu se ochranou své kritické infrastruktury, důsledně zabývat [4].

Kritickou infrastrukturu lze definovat jako: Prvek kritické infrastruktury, systém prvků kritické infrastruktury, narušení jehož funkce by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu. [5].

Za prvek kritické infrastruktury lze obecně označit objekt, zařízení, stavbu nebo prostředek, určený dle odvětvových a průřezových kritérií. Tyto kritéria stanovila vláda ČR svým nařízením č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.

V případě, že by narušení činnosti prvku KI mělo závažný dopad i na jiný členský stát Evropské unie (narušení by mělo přeshraniční dopad), jedná se o prvek evropské kritické infrastruktury (dále také „EKI“) [5].

Subjektem KI rozumíme samotného provozovatele prvku KI. Může jím být některá ze státních institucí nebo také soukromý subjekt. Jedná-li se o provozovatele prvku evropské KI, považuje se za subjekt evropské kritické infrastruktury [6].

Mezi kompetence Ministerstva Vnitra České republiky (dále také „MV ČR“), resp. Generálního ředitelství Hasičského záchranného sboru České republiky, patří vést evidenci prvků KI. Současný seznam čítá okolo 1300 prvků. [7].

Smyslem ochrany KI je snížit její zranitelnost či zvýšit její odolnost. Preventivními opatřeními se snažíme dosáhnout toho, aby případný dopad výpadku služeb a činností dané KI byl, pokud možno krátkodobý, nepřilíš častý,

snadno provizorně odstranitelný, územně omezený a zasáhl co nejmenší počet obyvatel. Hrozbu pro kritickou infrastrukturu mohou představovat přírodní živly nebo samotná činnost člověka (úmyslná nebo neúmyslná). Rozličnost těchto hrozeb poukazuje bezesporu na potřebu velkého množství bezpečnostních opatření, ale možnosti státu bývají bohužel i v této oblasti omezeny jeho finančními možnostmi. V tomto ohledu má ekonomika na KI nemalý vliv [8].

Zcela ideální by tedy jistě bylo to, kdyby stát KI nepřetržitě hlídal a tím zajistil její bezpečnost. Díky své členitosti by náklady na takovouto bezpečnost KI byly pro stát zcela neúnosné. Cílem tedy zůstává, vynaloženými investicemi do bezpečnosti snížit míru rizika ohrožení KI na přijatelnou míru, která již bude pro daný stát akceptovatelná [3].

Kritická infrastruktura je velmi rozsáhlá, ať už plošně nebo také co se týče počtu prvků. Zmínili jsme, že všechny prvky KI nejsou ve vlastnictví státu. Soukromý sektor má jako prvořadý úkol tvorbu zisku. To je pro něj prioritou, na rozdíl od investice do bezpečnosti a ochrany KI. Stát samozřejmě nemůže investovat finance do soukromého majetku (KI v soukromém vlastnictví) a stejně tak má omezené možnosti k tomu, aby donutil soukromý subjekt investovat vlastní kapitál do preventivních bezpečnostních opatření [4, 9].

3.2.1 Historický vývoj ochrany kritické infrastruktury ve světě

Historicky prvními státy, které se začaly zajímat o problematiku ochrany své životně důležité infrastruktury (v té době se ještě označení „kritická infrastruktura“ nepoužívalo), byly Spojené státy americké, Kanada nebo také Austrálie. V těchto státech docházelo k nejprudšímu rozvoji IT technologií a kybernetických systémů. Současně s tímto rozvojem začaly být také řešeny bezpečnostní otázky takovýchto propojených sítí a systémů. Týkaly se jejich dlouhodobé bezpečnosti, stejně jako třeba rizika spojeného

s přechodem počítačových sítí do nového milénia (tzv. „Y2K problém“). Tyto i jiné další obavy byly důvodem vzniku tzv. „Bílé knihy“. Tato směrnice amerického prezidenta Billa Clintona, vydaná v roce 1998, byla ve své podstatě prvním uceleným materiálem řešícím problematiku možných útoků (fyzických nebo kybernetických) na KI. Směrnice převážně řešila útoky na komunikační a informační systémy, zajišťující zejména oblasti energetiky, bankovníctví, telekomunikací, dopravy nebo také zásobování vodou a záchranné služby [10, 11].

Teroristické útoky na Světové obchodní centrum v New Yorku dne 11. září 2001 měly za následek obrovský posun v chápání KI. V plné síle ukázaly hrozbu, která bude KI ohrožovat v následujících letech nejvíce, a to terorismus. Americká administrativa v roce 2003 vydala „Národní strategii vnitřní bezpečnosti“, která již reflektovala potřebu změn po zmíněných útocích. Obsahovala také definici KI: „Systémy a zařízení, jak hmotné, tak i virtuální, které jsou životně důležité pro USA a jejich zneschopnění nebo zničení by mělo vliv na snížení bezpečnosti, národní ekonomické bezpečnosti, národního veřejného zdraví, bezpečí nebo na jakoukoliv jejich kombinaci.“ Toto může být považováno za základní stavební kámen současné ochrany KI. Byla jasně definována potřeba ochrany KI a jejich zařízení a tuto potřebu lze považovat za jádro vnitřní bezpečnosti státu. Vytvořená strategie ochrany KI vycházela z politiky aktivního přístupu státní administrativy, soukromého sektoru, stejně jako běžného občana USA [12, 13].

Za evropské průkopníky na poli ochrany KI lze označit Německo společně s Velkou Británií. Velká Británie již v roce 1999 zřídila Koordinační centrum pro bezpečnost národní infrastruktury. Cílem tohoto centra byla koordinace a rozvoj činností směřujících k obraně – ochraně kritické národní infrastruktury. V rámci této národní KI byly jasně definovány systémy, které mají zásadní vliv

na zabezpečení funkce státu, jejichž poškození nebo vyřazení by zcela jistě znamenalo ohrožení lidských životů a stejně tak vedlo k závažným hospodářským a sociálním dopadům na společnost. Německo řešilo problematiku KI taktéž již v roce 1999. Přijalo materiál nazvaný „Informačně technické ohrožení klíčových infrastruktur v Německu“, který se následně stal základním dokumentem ochrany KI v Německu [2, 14].

3.2.2 Vývoj ochrany kritické infrastruktury v ČR

Na území dnešní České republiky docházelo k činnostem srovnatelným s ochranou kritické infrastruktury mnohem dříve, než se samotný pojem „kritická infrastruktura“ vůbec objevil. Nejedná se tedy o nic nového a během let docházelo k vývoji těchto ochranných snah. Podíváme-li se podrobněji na druhou polovinu minulého století, kdy probíhala tzv. „studená válka“, můžeme v této době za největší hrozbu zcela jistě považovat jaderný útok nepříteli. V tehdejší Československé socialistické republice se tyto hrozby také řešily. Nejvyšší prioritu tehdy mělo zvýšení odolnosti důležitých prvků národního hospodářství, obecně řečeno proti zbraním hromadného ničení. Nebezpečí jaderného útoku naštěstí pomalu sláblo, díky zlepšujícím se vztahům dvou největších jaderných velmocí Spojených států amerických a Sovětského svazu a v neposlední řadě taky díky konci komunismu ve státech tzv. východního bloku [15].

Po pádu železné opony, již nebylo zapotřebí připravovat hospodářství a obyvatelstvo na válku. To mělo za následek postupný úpadek vybudovaného systému civilní ochrany, postupnou likvidaci jejich jednotek a také například ukončení branné výchovy obyvatelstva. Hlavním problémem (rizikem) se tak postupně stávaly přírodní živly a katastrofy [15].

Prvotní pokusy o ochranu kritické infrastruktury, jak již bylo výše zmíněno, směřovaly po vzoru západních států převážně na kybernetickou bezpečnost

a ochranu počítačových sítí. Takto úzké chápání KI brzy narušily povodně (zejména v letech 1997 a 1998). Po povodních docházelo k analýze toho, jak se na povodně dokázalo včas reagovat, jaká byla na ně připravenost. V zahraničí se prováděly rešerše za účelem vylepšení našeho stávajícího systému [11].

Jedním z důležitých momentů, týkajících se ochrany tak zásadních hodnot jako jsou životy, zdraví a majetek, se stalo přijetí tzv. krizových zákonů v roce 2000 a s tím spojený vznik integrovaného záchranného systému v České republice. Jedním z těchto zákonů byl i zákon č. 238/2000 Sb., o Hasičském záchranném sboru České republiky. Tímto zákonem došlo k zásadním změnám ve struktuře dosavadního hasičského sboru a ten byl tímto zákonem reorganizován do současné podoby. Základním posláním Hasičského záchranného sboru ČR (dále také „HZS ČR“) se stala ochrana životů, zdraví obyvatel a majetku před požáry, stejně jako poskytování účinné pomoci při mimořádných událostech. HZS ČR se kromě svého primárního poslání také podílí na organizaci a provádění úkolů požární ochrany, ochraně obyvatelstva, civilního a nouzového plánování, integrovaného záchranného systému, krizového řízení a dalších úkolech [16, 17].

Z pohledu ochrany kritické infrastruktury je to podstatné z toho důvodu, že společně s novým členěním HZS ČR dle jednotlivých krajů, platným od 1. ledna 2001, vzniklo také Generální ředitelství Hasičského záchranného sboru České republiky [17].

Pro stát je bezpečnost kritické infrastruktury úkolem značné důležitosti. Problematika ochrany KI byla přidělena Bezpečnostní radě státu (dále také „BRS“). BRS je stálým poradním orgánem vlády pro koordinaci problematiky bezpečnosti České republiky a přípravu návrhů opatření k jejímu zajišťování.

Pracovním výborem BRS, kterému problematika KI přísluší, je Výbor pro civilní a nouzové plánování (dále také „Výbor CNP“) [11, 16].

Na základě rozhodnutí BRS, začalo Ministerstvo Vnitra ČR (resp. Generální ředitelství Hasičského záchranného sboru ČR) v roce 2003 připravovat materiál, který měl jako první definovat rozsah základních funkcí státu během krizových situací. Následným krokem bylo přijetí usnesení č. 173 Výboru pro civilní a nouzové plánování ze dne 24. června 2003, které se stalo prvním komplexním materiálem v oblasti kritické infrastruktury. Toto usnesení se detailně věnovalo analýze jednotlivých odvětví KI a její legislativě, přineslo první ucelené definice základních funkcí státu za krizových situací. Na definování těchto základních hodnot se podílely také další ústřední správní úřady. V dokumentu se podařilo pojmenovat bezpečnostní priority státu při krizových situacích, důležité pro ochranu životů a zdraví obyvatel, majetku, životního prostředí a také státu samotného [18].

Za prvořadý úkol státu, při krizových stavech, tedy můžeme považovat [2]:

- ochranu života a zdraví obyvatel,
- obranu České republiky, její svrchovanosti a celistvosti,
- zajištění základních životních potřeb obyvatelstva,
- koordinovaný postup státní správy a územní samosprávy při řešení krizových situací,
- udržení bezpečnosti a vnitřního pořádku,
- zajištění dostatečných zdrojů (finančních, materiálních, energetických) pro řešení krizové situace,
- funkčnost orgánů krizového řízení, záchranných sborů, ozbrojených sil a ozbrojených bezpečnostních sborů, havarijních služeb za krizových stavů,

- dopravní obslužnost
- udržení funkčnosti systémů, jejichž zničení nebo poškození by mělo závažný dopad na obranyschopnost, ekonomickou a společenskou stabilitu a bezpečnost státu.

Rozsah základních funkcí státu tedy můžeme chápat, jako souhrn všech nezbytných infrastruktur (systémů či technologií), společně s množstvím organizačních, legislativních a technických opatření, prováděných státními nebo soukromými subjekty ve vybraných oblastech. Všechna takováto opatření musejí zabezpečit základní životní potřeby obyvatel státu a současně umožnit adekvátní reakci na nastalou krizovou situaci, směřující k jejímu vyřešení.

Výborem CNP bylo dne 23. září 2003 schváleno usnesení č. 179. Tento dokument obsahoval přehled vybraných subjektů KI, které bylo v případě ohrožení nutno ochránit. Kritická infrastruktura ČR byla ve zmíněných seznamech rozdělena na KI národní, regionální a místní úrovni. Seznamy nebyly konečné a v následujícím období postupně docházelo k jejich dalšímu upravování. Národní kritickou infrastrukturou se dle tohoto usnesení rozuměl systém, skládající se ze dvou úrovní. Úrovní sektorů (oblastí) a dále úrovně produktů (služeb). Usnesením Výboru CNP č. 190 ze dne 23. března 2004 došlo ke schválení návrhu základních oblastí kritické infrastruktury a jejich služeb nebo produktů. Vybraná ministerstva a ústřední správní úřady se, dle svých kompetencí, staly odpovědnými za příslušné oblasti KI, součástí usnesení byl také soupis 42 nejdůležitějších objektů KI s celostátním významem [14].

Prvním květnovým dnem roku 2004 se Česká republika stala součástí Evropského unie. Tento historický okamžik přinesl pro Českou republiku povinnost implementovat do svého právního rámce nezbytnou evropskou legislativu.

Tato povinnost se pochopitelně nevyhnula ani oblasti ochrany kritické infrastruktury. Kritická infrastruktura byla v obecné rovině rozdělena na národní kritickou infrastrukturu (dále také NKI) a evropskou kritickou infrastrukturu (EKI). Problematika NKI byla zcela ponechána v kompetenci jednotlivých členských států EU, jelikož narušení či zničení takovéto infrastruktury by případně postihlo pouze a jenom tento konkrétní stát. V případě České republiky tedy zůstala garantem bezpečnosti KI Bezpečnostní rada státu. Za jednotlivé oblasti (sektory) kritické infrastruktury zůstala nadále odpovědnost jednotlivým ministerstvům a vybraným ústředním správním úřadům, odpovídající jejich působnosti a kompetencím [19].

V následujících letech Výbor CNP pokračoval v řešení problematiky kritické infrastruktury, analyzoval a porovnával kroky České republiky s přístupy k ochraně KI v jiných členských zemích Evropské unie. V průběhu roku 2007 Výbor CNP finalizoval výslednou podobu pojmu „Kritická infrastruktura“ a navrhl oblasti kritické infrastruktury. Tyto oblasti KI byly schváleny v příloze usnesení BRS č. 30, v průběhu července 2007 (viz tabulka níže) [20].

Tabulka 1 – Oblasti a služby kritické infrastruktury ČR [20]

	Oblast KI	Služba nebo produkt
1.	Energetika	1.1. Elektřina
		1.2. Plyn
		1.3. Tepelná energie
		1.4. Ropa a ropné produkty
2.	Vodní hospodářství	2.1. Zásobování pitnou a užitkovou vodou
		2.2. Zabezpečení a správa povrchových vod a podzemních zdrojů vody
		2.3. Systém odpadních vod

3.	Potravinařství a zemědělství	3.1. Produkce potravin
		3.2. Péče o potraviny
		3.3. Zemědělská výroba
4.	Zdravotní péče	4.1. Přednemocniční zdravotní péče
		4.2. Nemocniční péče
		4.3. Ochrana veřejného zdraví
		4.4. Distribuce léčiv
5.	Doprava	5.1. Silniční
		5.2. Železniční
		5.3. Letecká
		5.4. Vnitrozemská vodní
6.	Komunikační a informační systémy	6.1. Služby pevných komunikačních sítí
		6.2. Služby mobilních komunikačních sítí
		6.3. Radiová komunikace a navigace
		6.4. Satelitní komunikace
		6.5. Televizní a rádiové vysílání
		6.6. Přístup k internetu a k datovým službám
		6.7. Poštovní a kurýrní služby
7.	Bankovní a finanční sektor	7.1. Správa veřejných financí
		7.2. Bankovníctví
		7.3. Pojišťovnictví
		7.4. Kapitálový trh
8.	Nouzové služby	8.1. Policie ČR a jednotky požární ochrany
		8.2. Hasičský záchranný sbor ČR
		8.3. Zdravotnické záchranné služby
		8.4. Letecká zdravotnická záchranná služba
		8.5. Armáda ČR
		8.6. Radiační monitorování
		8.7. Předpovědní, varovná a hlásná služba
9.	Veřejná správa	9.1. Sociální ochrana a zaměstnanost
		9.2. Diplomacie
		9.3. Výkon justice a vězeňství
		9.4. Státní správa a samospráva

Výborem CNP byla projednána a schválena Zpráva o řešení problematiky kritické infrastruktury v České republice. Tento dokument, se po jeho následném schválení Vládou ČR v únoru 2008, stal základním kamenem umožňujícím následný vznik Komplexní strategie ČR k řešení problematiky KI a také Národního programu ochrany kritické infrastruktury. Usnesení, kterým BRS Komplexní strategii a Národní program projednala, bylo přijato ještě před koncem roku 2009 a následně byla Komplexní strategie a Národní program přijat vládním usnesením č. 140 ze dne 22. února 2010 [11, 21].

Zákon č. 240/2000 Sb., o krizovém řízení a změně některých zákonů, se v roce 2010 dočkal novelizace (zákonem č. 430/2010 Sb.), díky čemuž se i evropská kritická infrastruktura konečně stala součástí českého právního řádu. Tímto zákonem (po jeho další novelizaci zákonem č. 118/2011 Sb.) je stanovena působnost státních orgánů a územních samosprávných celků, dále také práva a povinnosti právnických a fyzických osob při přípravě na krizové situace, které nesouvisejí se zajišťováním obrany České republiky před vnějším napadením a při jejich řešení a při ochraně kritické infrastruktury a odpovědnost za porušení těchto povinností [5].

3.2.3 Evropská kritická infrastruktura

Problematika kritické infrastruktury logicky začala být řešena také na evropské, nadnárodní úrovni. Potřeba těchto snah se ještě navýšila po zmíněných teroristických útocích z 11. září 2001 v New Yorku. Útoky odstartovaly období, kdy některé země pocítily hrozbu terorismu na vlastní kůži. Pro jejich připomenutí lze zmínit teroristické útoky na vlaky v Madridu (2004), či útoky na Londýnskou hromadnou dopravu (2005). Nesmíme zapomenout ani na výpadky elektrické přenosové soustavy v Itálii a Německu. Všechny tyto události přispěly k tomu, že značná část evropských států již začala definovat svou národní kritickou infrastrukturu [22].

V roce 2004 se Česká republika stala členským státem Evropské unie. Vstoupila do ní právě v době, kdy se EU začala intenzivně zabývat problematikou kritické infrastruktury. Právě prožívané teroristické útoky, společně se zkušenostmi z nedávných přírodních katastrof, zapříčinily nutnou reakci ze strany Evropské unie. Během téhož roku byl Evropskou Komisí vydán dokument pojmenovaný „Ochrana kritické infrastruktury v boji proti terorismu“, který obsahoval návrhy ke zlepšení bezpečnosti KI v Evropské unii, včetně opatření k zabezpečení lepší prevence a připravenosti na teroristické útoky zasahující kritické infrastruktury [22, 23].

Evropská Komise předložila po mnoha jednáních na podzim roku 2005 dokument nazvaný „Zelená kniha“, ta byla následně Evropskou Komisí schválena dne 17. listopadu 2005. Tuto Zelenou knihu lze bezesporu nazvat nejzásadnějším dokumentem evropské kritické infrastruktury. Ve svém obsahu definovala, co lze považovat za prvek evropské kritické infrastruktury. Za evropskou KI můžeme považovat prvky KI, které vykazují zásadní důležitost v rámci EU a současně by jejich poškození či úplné zničení postihlo alespoň dva členské státy. Podstata rizika vyplývá ze vzájemného propojení jednotlivých (národních) infrastruktur napříč odvětvími, kdy jejich ochromení by mělo přeshraniční dopad [24].

Cílem této knihy bylo zapojit do ochrany KI co nejvíce subjektům, majících zodpovědnost za ochranu jednotlivých prvků KI nebo i celých systémů. Snahou bylo také zapojit zainteresované spolky v daných odvětvích či profesní spolky, širokou veřejnost a v neposlední řadě také veřejnou správu. Součástí Zelené knihy byl také popis a návrh možností ke zřízení „Evropského programu na ochranu kritické infrastruktury“ (dále také „EPCIP“). Zpětná vazba jednotlivých členských států EU na navrhovaná opatření a postupy měla být zohledněna při samotném spuštění tohoto programu [24].

Evropský program na ochranu kritické infrastruktury byl schválen 12. prosince 2006. Cílem programu bylo zajistit ochranu kritické infrastruktury s důrazem na ochranu před terorismem (důsledek výše zmíněných teroristických útoků od roku 2001). EPCIP k tomu měl využít několika základních principů (zásad), kterými byly subsidiarita, důvěrnost, doplňkovost, spolupráce zainteresovaných subjektů, proporcionalita a odvětvový přístup (příloha č. 1). Snaha Evropské unie o ochranu kritické infrastruktury se zaměřila 3 klíčovými směry. Prvním cílem bylo jasně vymezit EPCIP na strategické úrovni tak, aby fungoval ve všech oblastech KI. Druhý cíl představovala nově vznikající oblast Evropské kritické infrastruktury a poslední bodem byla podpora národní kritické infrastruktury [25].

Dne 8. prosince 2008 byla schválena evropská Směrnice Rady č. 2008/114/ES o určování a označování evropských kritických infrastruktur a potřeby posouzení zvýšení jejich ochrany (dále také „Směrnice o EKI“). Tato směrnice znamenala jistý politický kompromis a musela být členskými státy Evropské unie implementována do jejich právního řádu. Hlavním cílem Směrnice o EKI bylo přispět svou měrou k ochraně obyvatelstva a zajistit komplexnost přístupu ke všem hrozbám a ochraně kritické infrastruktury. Klíčovou podmínkou ochrany kritické infrastruktury je krizové plánování, na něm se podílí Subjekty KI a státní orgány. Odvětví, o která se Směrnice o EKI zajímala, byla energetika (elektřina, ropa a zemní plyn), dopravu (silniční, železniční, leteckou, stejně jako vnitrozemskou, zámořskou a pobřežní vodní dopravu). Odpovědnost za ochranu KI byla ponechána jednotlivým členským státům EU, na jejichž území se KI nachází. Pro účely ochrany KI bylo nutné začít sdílet potřebné informace mezi jednotlivými státy EU. K určení národní KI si měl každý stát nastavit svá kritéria [21, 26].

3.3 Hrozby kritické infrastruktury

Následující kapitola nastíní hrozby ohrožující kritickou infrastrukturu. Jelikož je těchto hrozeb široké spektrum, činí to ochranu KI o to složitější. Jedná se o výčet možných hrozeb a je logické, že ne všechny musí být reálnou hrozbou pro jeden konkrétní stát nebo prvek KI. Bezpečností hrozby kritické infrastruktury je proto třeba pečlivě identifikovat a analyzovat. Značný rozvoj moderních technologií se zapříčinil o to, že se dnes dokáží bezpečnostní analýzy provádět se stále větším množstvím vstupních informací (dat) a díky tomu jsou výsledky stále pohotovější a přesnější. S pomocí takovýchto analýz a znalosti geografických podmínek České republiky, je možné zjistit konkrétní hrozby pro náš stát a následně říci, jak moc je daná hrozba reálná. Nejedná se o nikterak výjimečný přístup a stejně tak postupují i další státy na světě.

Důležitými proměnnými bezpečnostních analýz jsou pojmy hrozba a riziko. Hrozbu lze popsat, jako na chráněném zájmu většinou nezávislý jev, který může či v některých případech dokonce chce, zcela úmyslně poškodit tuto hodnotu. Závažnost takovéto hrozby závisí na tom, jakou cenu pro nás představuje ohrožená hodnota. Odpovědí na hrozbu je provedení opatření, vedoucích k eliminaci dané hrozby. Riziko lze chápat jako pravděpodobnost, že k dané hrozbě dojde a jaké následky bude mít na chráněný zájem (životy, zdraví osob a zvířat, majetek nebo životní prostředí) [11].

Hrozby, ohrožující kritickou infrastrukturu, lze rozdělit dle místa jejich působení na KI, do dvou skupin [27]:

1. Vnitřní hrozby.

Jedná se hrozby, které nemusí být vždy nutně zapříčiněny subjektem KI. Z vnitřních hrozeb, způsobených subjektem KI, můžeme zmínit např. přechodnou či trvalou změnu orientace poskytování výrobků

a služeb ať už z důvodu řešení mimořádné události nebo obchodního rozhodnutí vedení subjektu KI. Nesmíme zapomenout ani na možnost stávky zaměstnanců subjektu KI nebo úplného krachu subjektu kritické infrastruktury.

2. Vnější hrozby.

Všechny hrozby vznikající mimo tuto kritickou infrastrukturu. Jsou to všechny živelné pohromy a katastrofy, stejně jako průmyslové havárie v sousedních průmyslových objektech. Dále také problémy způsobené člověkem jako např. terorismus a úmyslný trestný čin nebo nedostatek pracovních sil z důvodu nemocnosti či neochota zaměstnanců subjektu KI pracovat kvůli jejich samotnému postižení mimořádnou událostí.

Pokud k naplnění takovéto hrozby opravdu dojde, hrozba má na obyvatele státu konkrétní dopady, znamená pro něj určitá omezení. Zmíněné situace člověku přinášejí diskomfort a jsou spojeny s určitým pocitem mimořádnosti. Definovat mimořádnou situaci nám pomůže zákon č. 239/2000 Sb., o integrovaném záchranném systému a změně některých zákonů. Zákon ve svém §2 říká, že mimořádnou událostí rozumíme škodlivé působení sil a jevů vyvolaných činností člověka, přírodními vlivy a také havárie, které ohrožují život, zdraví, majetek nebo životní prostředí a vyžadují provedení záchranných nebo likvidačních prací [28].

Mimořádné události lze rozdělit podle jevů, jež je způsobují, do tří skupin [4]:

1. Přírodní mimořádné události.

Tyto události představují veškeré přírodní a živelné katastrofy nebo ničivé meteorologické jevy. Jako příklad je možné uvést vulkanickou a seismickou činnost, povodně nebo větrné smrště.

2. Antropogenní mimořádné události.

Jedná se o mimořádné události, které jsou způsobeny přímou činností člověka nebo zprostředkovaně. Tyto mimořádné události zahrnují nedbalostních činy osob, jako jsou například nehody, průmyslové havárie a technologické poruchy, až po akty úmyslné, jako například terorismus, kybernetické útoky nebo jiná organizovaná trestná činnost.

3. Kombinované mimořádné události.

Tento druh mimořádné události zahrnuje přírodní mimořádné události, způsobené však předcházející lidskou činností (ať už krátkodobou nebo dlouhodobou), stejně jako antropogenní mimořádné události vyvolané stupňujícím se působením přírodních sil a živlů. Takovéto společné působení přírodních sil a antropogenních vlivů najednou je možné označit za tzv. domino efekt či synergický jev. Domino efekt lze chápat jako řetězec jednotlivých jevů, kdy každý jev, síla způsobí vznik jevu v řetězci následujícího (např. vlna tsunami způsobí zaplavení pobřežních oblastí, vlnou dojde k poškození technologie chemické továrny, díky poškození dojde k úniku nebezpečné látky do vzduchu a zamoření širokého okolí). Synergickým jevem je to, když jediná příčina (událost) způsobí současný vznik mnoha dalších jevů. Příkladem může být výše zmíněná technologie chemické továrny. Po jejím poškození vlnou tsunami, dojde k výbuchu

a při něm současně působí tlaková vlna, odlétající střepiny, uvolněná nebezpečná látka a v neposlední řadě také samotný požár.

V roce 2007 bylo, v rámci projednávání Komplexní strategie České republiky k řešení problematiky KI, takovýchto 13 nejzávažnějších hrozeb pojmenováno v návrhu Generálního ředitelství Hasičského záchranného sboru České republiky [29]:

1. technologické havárie;
2. technické poruchy a nedostatek náhradních dílů;
3. výpadky dodávek energií (elektřina, plyn, teplo, benzín apod.);
4. výpadky dodávek vody;
5. výpadky dodávek surovin (součástí) důležitých pro výrobu nebo poskytování služeb;
6. kolaps počítačových sítí;
7. narušení objektu KI z důvodu živelní pohromy nebo průmyslové havárie v „sousedním objektu“;
8. narušení objektu KI způsobené člověkem (terorismus, kriminální čin, důsledek války);
9. dočasná změna orientace (priorit) poskytování výrobků a služeb z důvodu řešení mimořádných událostí (krizová situace vojenského i nevojenského charakteru);
10. dlouhodobá nebo trvalá změna orientace poskytování výrobků a služeb z důvodu rozhodnutí managementu subjektu KI;
11. „krach“ firmy (ekonomické či jiné důvody);
12. stávka (zaměstnanců subjektu KI, stejně jako zaměstnanců subdodavatelských firem);
13. nedostatek (úbytek) pracovních sil, včetně zvýšené nemocnosti (z důvodu pandemie, infekční nemoci), odmítnutí zaměstnanců pracovat

např. při řešení vlastních (osobních) problémů souvisejících se vznikem mimořádných událostí.

3.4 Bezpečnostní opatření k ochraně kritické infrastruktury

Ochranu kritické infrastruktury mohou zajistit příslušná bezpečnostní opatření. Takováto opatření přicházejí na řadu ve chvíli, kdy je kritická infrastruktura jasně definována a jsou nám známy hodnoty (prvky KI), jež se snažíme opatřeními chránit, stejně jako hrozby těmto hodnotám hrozící. Nemalý vliv na výslednou podobu bezpečnostních opatření má jejich ekonomická stránka (investiční náklady a následné provozní náklady) [30].

Bezpečnostní opatření k ochraně KI jsou systémem ucelených a navzájem propojených opatření, jejichž cílem je zajištění ochrany prvků KI proti všem známým bezpečnostním rizikům. Samotné uskutečnění těchto opatření ovlivňují jednotlivá odvětví kritické infrastruktury svými specifickými podmínkami (technologická a provozní bezpečnost). Bezpečnostní opatření je možné rozdělit na opatření stálá a odstupňovaná. Stálá bezpečnostní opatření zajišťují ochranu KI za běžných podmínek (běžné úrovni bezpečnostních rizik). K využití odstupňovaných bezpečnostních opatření dochází ve chvíli, kdy došlo (oprávněně) ke zvýšení aktuální úrovně bezpečnostního rizika. Příkladem takového zhoršení bezpečnostní situace je například předpoklad teroristického útoku nebo hrozící válečný konflikt. Provedení jednotlivých odstupňovaných bezpečnostních opatření, je danými subjekty připraveno již během období s běžnou úrovní bezpečnostních hrozeb, nejedná se tedy o žádnou bezpečnostní „improvizaci ušitou horkou jehlou“ v časové tísní. Ve většině případů se jedná o doplnění technického zabezpečení objektu, zajištění dostatku záložních komunikačních kanálů nebo posílení stávajícího výkonu fyzické ochrany objektu [30].

Bezpečnostní opatření k ochraně KI lze rozdělit na [30]:

- fyzickou ochranu;
- bezpečnost informačních systémů;
- komunikační bezpečnost;
- kybernetickou bezpečnost;
- administrativní bezpečnost;
- personální bezpečnost.

3.4.1 Fyzická ochrana

Fyzickou ochranou kritické infrastruktury lze obecně chápat, jako vzájemně se prolínající celek, skládající se z bezpečnostních opatření třech základních skupin. Jedná se o vybudování systémů technického zabezpečení, dále provádění fyzické ostrahy objektu a třetí skupinou opatření je aplikace režimových opatření. Uvedené skupiny bezpečnostních opatření fyzické ochrany jsou úzce propojeny a jejich bezpečnostní přínos závisí na jejich vyváženosti. Podmínkou správně fungující fyzické ochrany je zajištění fungujících vazeb mezi těmito jednotlivými částmi [30].

Systémy technického zabezpečení jsou veškeré mechanické zábranné vybavení a zařízení, elektronické zabezpečovací systémy, audiovizuální systémy a další zařízení, mající za úkol zvýšení bezpečnosti KI. Cílem těchto technických opatření je zamezení nebo ztížení přístupu ke chráněnému zájmu ze strany nepovolaných osob a včasné odhalení neoprávněného vniknutí, sledování a dokumentaci pohybu osob a vozidel nebo včasnou detekci a signalizaci vzniku požáru, společně se snížením požárem vzniklých škod. Jedná se o všechny mechanická bezpečnostní opatření dnes běžně používaná domácnostech, jako například oplocení, mříže a zámky, bezpečnostní skla nebo trezory. Elektronickými zabezpečovacími systémy jsou myšleny veškeré poplachové a tísňové systémy, přivolávající fyzickou ostrahu či následně spouštějící některý

z dalších systémů technické ochrany, v neposlední řadě zde patří také kamerové systémy a elektronická požární signalizace (EPS) [30].

Fyzická ostraha objektu je bezpečnostním opatřením, realizovaným aktivní přístupem a činností osob – bezpečnostních pracovníků. Nutností je odpovídající rozsah znalostí, školení a výcviku těchto pracovníků, který musí odpovídat závažnosti analyzovaných bezpečnostních hrozeb a rizik, stejně jako zvláštnostem ostrahy daného objektu. Fyzickou ostrahu lze provádět v různých formách. Nejčastěji se jedná o recepční služby, pochůzkovou činnost uvnitř či vně areálu v předepsaných intervalech, patrolování, střežení využitím pultu centralizované ochrany s případným následným výjezdem zásahové skupiny apod [30].

Režimová opatření je možné považovat za bezpečnostní kodex daného objektu, zohledňující veškerá jeho místní specifika. Jedná se o komplexní soubor postupů a pokynů, organizujících daná bezpečnostní opatření a zajišťujících vzájemné vazby mezi systémy technického zabezpečení a uživateli objektu. Příkladem může být upravení režimu vstupu osob a vjezdu vozidel, režim manipulace s hmotným či nehmotným majetkem, režim identifikačních prvků (klíče, PIN kódy, karty) apod. [30].

3.4.2 Bezpečnost informačních systémů

Je soubor bezpečnostních opatření, směřujících k ochraně důležitých řídicích a regulačních systémů prvků KI. Cílem je zamezit neoprávněnému přístupu k citlivým informacím o kritické infrastruktuře, stejně jako o ochraně takovýchto informací, které by následně mohly být využity při pokusu o poškození nebo zničení určité části KI [30].

3.4.3 Komunikační bezpečnost

Lze ji zjednodušeně chápat, jako bezpečnost přenosových cest, které využívají řídicí a regulační systémy prvků KI. Komunikační bezpečnost zahrnuje zajištění přenosových cest informačních systémů, jimiž se přenášejí informace o ochraně KI [30].

3.4.4 Kybernetická bezpečnost

Kybernetickou bezpečnost tvoří ucelený systém bezpečnostních opatření proti hrozbám kybernetické kriminality a kybernetického terorismu. S rozvojem takovýchto „online“ řídicích sítí a zabezpečovacích systémů, roste také množství dat pohybujících se kyberprostorem a logicky také možnost jejich zneužití. Jako příklad takového zneužití, lze z nedávné historie uvést opakované útoky hackerů v Ázerbájdžánu, kdy se jim podařilo získat kontrolu nad místními kompresorovými stanicemi na dobu několika dnů až týdnů [30].

3.4.5 Administrativní bezpečnost

Administrativní bezpečnost je souborem komplexních opatření, směřujících k zajištění bezpečné manipulace s dokumentací obsahující informace o KI. Jedná se o informace, ke kterým je potřeba zamezit přístup nepovolaných osob, stejně jako dokumentů týkajících se bezpečnostních opatření ochrany KI [30].

3.4.6 Personální bezpečnost

Personální bezpečnost je jedním ze stěžejních bezpečnostních opatření ochrany KI. Jedná se o opatření, která se dotýkají také oblasti personální politiky. Cílem těchto opatření je výběr důvěryhodných osob, spolehlivě zajišťujících provoz prvků KI, zajištění jejich další vzdělávání v oblasti ochrany KI a pravidelné kontroly spolehlivosti zmíněných osob [30].

3.4.7 Management ochrany kritické infrastruktury

Managementem ochrany KI se rozumí komplexní systém řízení ochrany kritické infrastruktury. Zahrnuje prvky řízení (managementu) KI, postupů implementace jednotlivých druhů ochrany KI, bezpečnostní dokumentaci a vzdělávání. Součástí managementu ochrany KI jsou postupy pro řešení různých typů mimořádných událostí a krizových situací [30].

3.5 Určení prvku kritické infrastruktury ČR

Kritická infrastruktura je v ČR legislativně zakotvena v zákoně č. 240/2000 Sb., o krizovém řízení a jeho prováděcím nařízení vlády č. 432/2000 Sb. Postupem času bylo nutné do právního řádu implementovat požadavky Evropské unie (směrnice Rady o EKI z roku 2008). K tomu došlo novelizací zákona o krizovém řízení zákonem č. 430/2010 Sb. Díky těmto změnám kritická infrastruktura na území ČR dělí na národní a evropskou KI [5, 31].

Tato práce již zmínila, že pro každý prvek KI je podmínkou splnění kritérií (průřezových, odvětvových) určených v příloze nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury. Jednou z obecných podmínek pro určení toho, zda se jedná o prvek kritické infrastruktury či nikoliv, je posouzení nenahraditelnosti konkrétního prvku.

V případě nenahraditelnosti prvku, musíme při jeho narušení nebo zničení počítat s nutnými opravami nebo výstavbou prvku či pouze jeho části. Činnost prvku není možné obnovit v krátké době a do obnovy činnosti lze náhradu řešit pouze provizorně s tím, že dojde k významnému ovlivnění života obyvatel a fungování veřejné správy. Omezeno nebo zcela znemožněno bude zajišťování některých základních potřeb (např. dodávky elektřiny, plynu, komunikačních prostředků nebo služeb). Při těchto omezeních nemusí být vyhlášen krizový stav, ale nutností bude vyhlášení regulačního stupně, stavu nouze nebo omezení, která mohou dosáhnout celostátní úrovně [32].

Je-li prvek KI nahraditelný, jsou při jeho narušení nebo zničení také nutné opravy, rekonstrukce nebo výstavba prvku nebo jeho části. Jeho činnost je však možné nahradit jiným subjektem nebo provizorním způsobem v dostatečné úrovni a rozsahu [32].

Průřezová kritéria mají za cíl posoudit, dle stanovených mezních hodnot, závažnost vlivu narušení daného prvku kritické infrastruktury. Prvním průřezovým kritériem je počet obětí. Je nutné posoudit to, zda by narušení, poškození nebo zničení daného prvku, mělo za následek více než 250 mrtvých nebo by došlo k hospitalizaci více než 2 500 osob po dobu přesahující dobu 24 hodin. Dalším průřezovým kritériem je ekonomický dopad, který musí státu způsobit ztrátu vyšší než 0,5 % hrubého domácího produktu. Posledním kritériem je posouzení dopadu na veřejnost. Posuzujeme to, zda dojde k omezení poskytování nezbytných služeb či jinému závažnému zásahu do každodenního života, postihujícího více než 125 000 osob. Pokud posuzovaný objekt splnil, alespoň jedno z těchto tří průřezových kritérií, lze přistoupit k jeho dalšímu posouzení dle odvětvových kritérií [31].

Odvětvová kritéria prvků KI určují technické nebo provozní hodnoty prvků. Tyto kritéria jsou taxativně vyjmenována v příloze zmíněného nařízení vlády. Jedná se o prvky KI spadající například do odvětví energetiky, vodního hospodářství, potravinářství a zemědělství, zdravotnictví, dopravy a veřejné správy [31].

V případě, že daný objekt, budova nebo zařízení splňuje zmíněná průřezová a odvětvová kritéria, musí následně projít procesem označení za prvek kritické infrastruktury. Tento proces se liší podle toho, kdo je provozovatelem daného prvku KI [33].

1. Prvky KI, jejichž provozovatelem je organizační složka státu

Příslušná ministerstva, ústřední správní úřady, Česká národní banka (dále jen „ČNB“) zasílají Ministerstvu Vnitra České republiky návrhy na zařazení konkrétních prvků mezi národní kritickou infrastrukturu či evropskou kritickou infrastrukturu. MV ČR následně zpracuje seznam, který je podkladem pro určení prvků NKI nebo EKI (prvků, jejichž provozovatelem je organizační složka státu). Vláda na základě tohoto seznamu určí usnesením určí prvky NKI a EKI provozované organizační složkou státu. Vláda naposledy aktualizovala seznam prvků usnesením vlády č. 10 ze dne 7 ledna 2019.

2. Prvky, jejichž provozovatelem není stát

Tyto prvky NKI nebo EKI, provozované soukromými subjekty, určí příslušná ministerstva, ústřední správní úřady, ČNB opatřením obecné povahy a mají za povinnost o tom neprodleně informovat MV ČR.

Objekt či zařízení, které je označen za prvek KI, má určitá oprávnění, stejně jako povinnosti. Za jednu z hlavních výhod lze považovat to, že prvek KI má za krizových stavů možnost přednostního zásobování a na zaměstnance prvku KI, kteří jsou nezbytně nutní pro zajištění fungování této kritické infrastruktury, se nevztahuje ustanovení o pracovní povinnosti a pracovní výpomoci [7].

Provozovatel (subjekt KI) je ze zákona povinen se o prvek KI starat a chránit ho. Z dalších jeho povinností lze zmínit [7]:

1. Povinnost provozovatele objektu, stavby, zařízení nebo veřejné infrastruktury na výzvu příslušného správního úřadu poskytnou informace nezbytné k určení, zdali je objekt prvkem NKI či EKI.

Provozovatel je povinen poskytnout další součinnost při ochraně KI, spolupracovat a komunikovat s MV ČR a příslušným krajem.

2. Provozovatel je povinen určit styčného zaměstnance, který bude jeho jménem komunikovat s ústředními správními úřady a ponese zodpovědnost za správně zpracovanou dokumentaci. Dále bude poskytovat součinnost při plnění úkolů podle krizového zákona.
3. Povinností subjektu KI je také zpracovat „Plán krizové připravenosti subjektu KI“. Tento plán, který běžně není zpracováván v utajovaném režimu, se skládá ze základní, operativní a pomocné části. V dokumentu jsou pojmenovány možná rizika a hrozby daného prvku a subjektu KI, navrhuje opatření k jejich ochraně.
4. Povinnost subjektu KI strpět pravidelně kontroly ze strany příslušného ústředního správního úřadu.

3.6 Energetická oblast KI ČR

Tématem této bakalářské práce je ochrana kritické infrastruktury v odvětví zemní plyn, ropa a ropné produkty. Jednotlivá odvětví a konkrétní podmínky, za kterých lze daný prvek považovat za součást kritické infrastruktury ČR, nalezneme v příloze nařízení vlády č. 432/2010 Sb. Tato příloha byla v roce 2014 novelizována nařízením vlády č. 315/2014 Sb. a naposledy nařízením vlády č. 154/2020 Sb. [30].

Námi vybraná odvětví zemní plyn, ropa a ropné produkty, jsou ve zmíněné příloze uvedeny v bodě č. I, ENERGETIKA [6].

Tabulka 2 – Odvětvová kritéria proku KI, pro odvětví zemní plyn, ropa a ropné produkty. [6]

Zemní plyn
1. <u>Přepavní soustava</u>
a) vysokotlaký tranzitní plynovod se jmenovitým průměrem nejméně 700 mm,
b) vysokotlaký vnitrostátní plynovod se jmenovitým průměrem rovným nebo menším než 700 mm,
c) kompresorová stanice,
d) předávací stanice,
e) technický dispečink.
2. <u>Distribuční soustava</u>
a) vysokotlaký a středotlaký plynovod,
b) předávací a regulační stanice,
c) technický dispečink.
3. <u>Skladování plynu</u>
a) podzemní zásobník plynu se skladovací kapacitou nejméně 50 miliónů m ³ plynu,
b) technický dispečink.
Ropa a ropné produkty
1. <u>Přepavní soustava</u>
a) tranzitní ropovod se jmenovitým průměrem nejméně 500 mm, včetně vstupních bodů,
b) vnitrostátní ropovod se jmenovitým průměrem nejméně 200 mm, včetně vstupních bodů,
c) technický dispečink.
d) přečerpávací stanice,
e) koncové zařízení pro předání ropy,
f) začátek a konec zdvojení ropovodu a odbočky – ježkovací komora.

2. <u>Distribuční soustava</u>
a) produktovod se jmenovitým průměrem nejméně 200 mm, včetně vstupních bodů,
b) technický dispečink,
c) přečerpávací stanice.
3. <u>Skladování ropy a pohonných hmot</u>
a) zásobník a komplex zásobníků s kapacitou nejméně 40 000 m ³ ,
b) technický dispečink.
4. <u>Výroba pohonných hmot</u>
a) rafinérie s kapacitou atmosférické destilace nejméně 500 000 tun/rok.

3.7 Zemní plyn

Zemní plyn patří mezi nejdůležitější komodity. Toto neobnovitelné, fosilní palivo se stalo nepostradatelným zdrojem energie pro lidskou společnost. Zemní plyn plní funkci tzv. „výhřevného plynu“ se širokým spektrem uplatnění. Lidská společnost si zvykla na jeho využití k vaření, vytápění, ohřevu vody, v elektrárnách a teplárnách nebo dopravě. Česká republika je závislá na dovozu zemního plynu, většina importovaného plynu pochází z Ruska a zbylou část (přibližně jednu čtvrtinu dovezeného plynu v roce 2019) dodává Norsko. Na našem území jsou také ložiska zemního plynu, historickým milníkem byl v roce 1914 nález ložiska na území tehdejšího Rakouska-Uherska (v oblasti dnes náležící Slovenské republice, poblíž hranic s ČR). V současnosti je dobré zmínit nález ložiska zemního plynu v roce 2017, kdy se v oblasti Hodonínska podařilo těžařské společnosti Moravské naftové doly (dále také „MND“) najít ložisko zemního plynu o odhadované velikosti sto miliónů metrů krychlových [34, 35].

Zemní plyn je přírodní, hořlavý a vysoce výhřevný plyn, lehčí než vzduch, který je složený převážně z plynných uhlovodíků a dalších nehořlavých složek,

jejichž koncentrace se pohybují v řádu jednotek procent (zejména dusík a oxid uhličitý). Tento plyn se těží vrty ze země nebo z mořského dna a složení zemního plynu se liší podle ložiska [36, 37].

Tabulka 3 – Složení zemního plynu [36]

Metan	CH ₄	70-90 %
Ethan, Propan, Butan	C ₂ H ₆ , C ₃ H ₈ , C ₄ H ₁₀	0-20 %
Oxid uhličitý	CO ₂	0-8 %
Kyslík	O ₂	0-0,2 %
Dusík	N ₂	0-5 %
Sirovodík	H ₂ S	0-5 %
Vzácné plyny	Ar, He, Ne, Xe	Stopové množství

Běžné složení zemního plynu, používaného v rámci České republiky, je [37]:

- 98 % obj. metan (CH₄);
- 1,15 % obj. vyšších uhlovodíků;
- 0,8 % obj. dusík (N₂);
- 0,05 % obj. oxidu uhličitého (CO₂);
- 0,20 mg/m³ síry (S).

Možnosti přepravy zemního plynu jsou dvě. První možností je transport v plynném stavu, kdy je plyn soustavou potrubních systémů (plynovodů) a technologických zařízení, dopravován z místa těžby až ke konečnému spotřebiteli. Plynovody jsou v drtivé většině své délky vedeny po mořském dně nebo pod zemským povrchem. Na povrchu pouze tam, kde je to efektivnější či nezbytně nutné (průmyslové areály, vodní toky apod.). Druhou možností přepravy zemního plynu představuje jeho transport ve zkapalněném stavu, známý též jako „LNG“ (Liquefied Natural Gas). Přímou na místě těžby dochází k jeho zkapalnění podchlazením na teplotu – 162 °C,

poté je plyn přečerpán do speciálně upravených tanků na lodích (první LNG loď byla zprovozněna v Japonsku již v roce 1973). V těchto tankách (kryogenní tanky) je za stálé teploty přepravován do příslušných distribučních uzlů (terminálů), kde opět přechází do plynné fáze a je potrubím dále distribuován [37].

3.7.1 Plynárenská soustava ČR

Zajištění potřebného množství zemního plynu pro ČR, probíhá za pomoci plynárenské soustavy. Soustava je systém vzájemně propojených zařízení na výrobu, přepravu, distribuci a uskladnění plynu. Nezbytnou součástí takového soustavy jsou také řídicí a zabezpečovací systémy, informační systémy a technika, potřebná k řízení takovýchto zařízení [37].

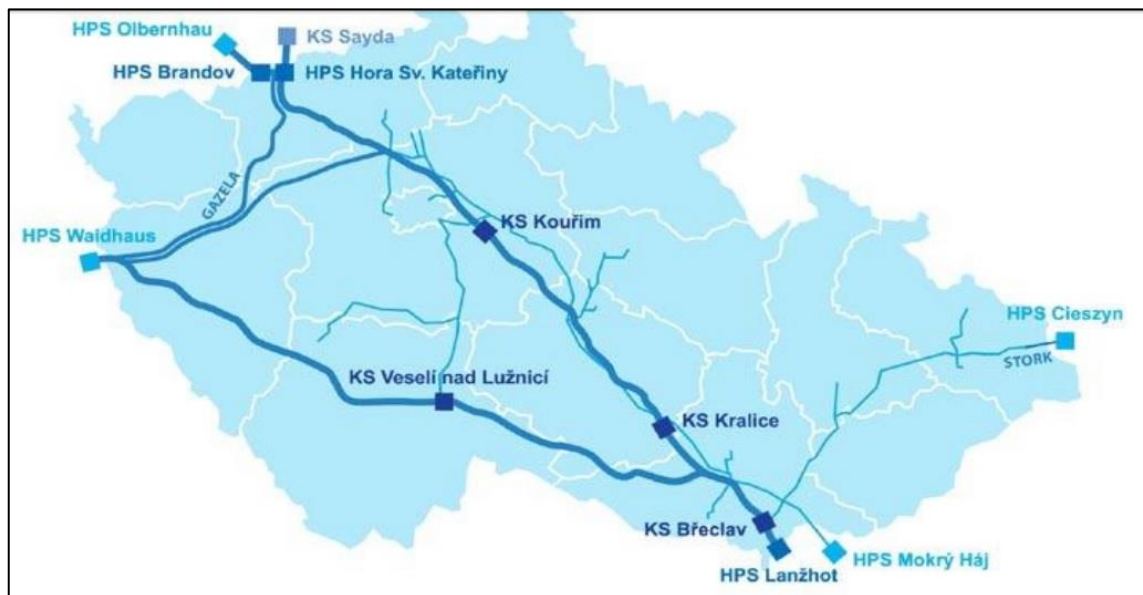
Zemní plyn je na území ČR přepravován a následně distribuován potrubními zařízeními (plynovody). Tato potrubí, o vnitřním průměru až 122 cm, poskytují možnost přepravovat zemní plyn rychlostí až 80 km/h. Průtok plynu plynovody zajišťují kompresorové stanice, nacházející se podél tras plynovodů. Dle provozního tlaku můžeme plynovody rozdělit na [35, 37]:

- Skupina plynovodů „A“ s provozním tlakem do 1,6 MPa:
 - podskupina A1 – nízkotlaké (NTL) s tlakem do 0,005 MPa včetně;
 - podskupina A2 – středotlaké (STL) s tlakem nad 0,005 do 0,4 MPa včetně;
 - podskupina A3 – vysokotlaké (VTL) s tlakem nad 0,4 do 1,6 MPa včetně.
- Skupina plynovodů „B“ s provozním tlakem nad 1,6 MPa:
 - podskupina B1 – vysokotlaké (VTL) s tlakem nad 1,6 do 4MPa včetně;
 - podskupina B2 – vysokotlaké (VTL) s tlakem nad 4 do 10 MPa včetně.

Z výše uvedené tabulky odvětvových kritérií vyplývá, že plynovody jsou na území České republiky součástí dvou soustav, soustavy přepravní a distribuční.

3.7.2 Přepravní soustava zemního plynu

Přepravní soustavou rozumíme skupinu vzájemně propojených vysokotlakých plynovodů podskupiny B2, předávacích a kompresních stanic a s nimi souvisejících technologických objektů, stejně jako jejich řídicích a zabezpečujících systémů, informačních a komunikačních technologií, propojených s plynárenskými soustavami v zahraničí. Ve zmíněných plynovodech zajišťuje přepravu plynu držitel licence k přepravě plynu (v ČR je to společnost NET4GAS, s.r.o.). Plynovody, které jsou součástí této přepravní soustavy, jsou provozovány ve veřejném zájmu. Přepravní soustava na území České republiky má délku více než 3800 km [37, 38].

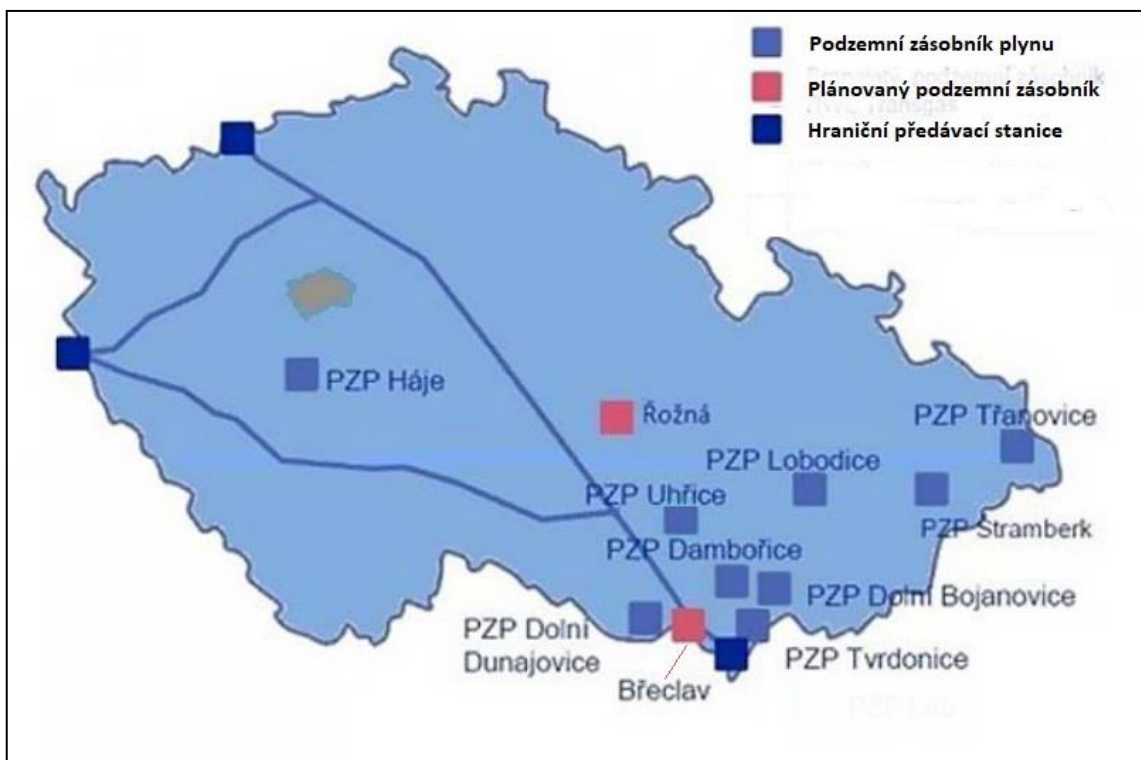


Obrázek 1 – Přepravní soustava České republiky [38]. HPS – hraniční předávací stanice; KS – kompresní stanice.

3.7.3 Skladování plynu

Součástí přepravní soustavy zemního plynu jsou také zásobníky plynu. Jedná se o zařízení (podzemní nebo nadzemní), včetně všech souvisejících technologických objektů a zařízení, informačních a komunikačních technologií, sloužící k uskladnění zemního plynu. V případě podzemních zásobníků plynu se využívá přírodních nebo uměle vytvořených prostor v podzemí,

které jsou obklopeny geologicky nepropustnými horninami, zabraňujícími úniku zemního plynu. Plyn může být skladován v plynné nebo kapalně fázi a zásobníky jsou přímo napojeny na plynárenskou soustavu České republiky. Důvodů ke vzniku zásobníků plynu je několik. Jako první můžeme jmenovat potřebu zajištění energetické bezpečnosti České republiky v případě problémů s dodávkami zemního plynu. Dále je zde také nutnost optimalizovat využití plynovodů během celého kalendářního roku. Pokud by došlo k dimenzování plynovodu dle spotřeby v zimě (během topné sezóny), plynovod by nebyl po zbytek roku dostatečně využíván. Z těchto důvodů se mimo topnou sezónu „přebytečný, volný plyn“ ukládá do zásobníků, ze kterých bude v zimě pokrývat zvýšenou spotřebu zemního plynu v ČR. Tato strategie má také nezanedbatelný ekonomický přínos, zemní plyn je v létě kupován za nižší cenu, než kterou má v topné sezóně, kdy je pak využíván. Celková kapacita všech podzemních zásobníků zemního plynu na území ČR v roce 2019 dosahovala 3,7 miliard m³ zemního plynu [37, 39].



Obrázek 2 – Podzemní zásobníky plynu (PZP) na území ČR [34].

Hraniční předávací stanice zajišťuje předání plynu, přepravovaného přes ČR (tranzitního plynu), do přepravní sítě sousedního státu. Oproti tomu „běžná“ předávací stanice představuje výstupní místo z přepravní soustavy plynu na území ČR. Ve zmíněných stanicích jsou na přepravní soustavu napojeny jednotlivé regionální distribuční sítě, dochází zde ke snížení tlaku plynu [37, 38].

3.7.4 Distribuční soustava

Distribuční soustavu tvoří síť vysokotlakých, středotlakých, nízkotlakých plynovodů (podskupin B1, A3, A2 a A1) a plynovodních přípojek, které jsou ve vlastnictví provozovatele distribuční soustavy. Dále také související technologické objekty, včetně řídicích a zabezpečovacích systémů a techniky, informačních a komunikační systémy. Jako příklad technologických objektů distribuční soustavy plynu můžeme jmenovat trasové uzávěry, armaturní uzly, regulační a odorizační stanice. V distribuční soustavě dochází k odorizaci zemního plynu. Zemní plyn je bez barvy, bez chuti a zápachu, proto se do něj z bezpečnostních důvodů přidávají těkavé látky s intenzivním a charakteristickým zápachem – odoranty. Distribuční soustava plynu v ČR dosahovala v roce 2019 délky 73 175 km [37, 39].

3.8 Ropa a ropné produkty

Ropa je tmavá, olejovitá kapalina, která je pro současnou civilizaci hlavním zdrojem energie. Toto fosilní palivo je organickým sedimentem, vznikajícím milióny let z těl odumřelých rostlin a živočichů. Možnosti jejího využití jsou tak široké, že se ropa stala v podstatě nepostradatelnou pro lidskou společnost. Ropa (pohonné hmoty z ní vyrobené) jsou základním palivem pro veškerou dopravu a je surovinou pro výrobu plastů nebo také léků. Jakákoliv současná masová produkce potravin by byla bez ropy nepředstavitelná, protože se z ní vyrábí hnojiva a také herbicidy nebo pesticidy.

To je důvod, proč ropa ve své důležitosti ostatní komodity jasně poráží a je někdy také nazývána „černým zlatem“ [40, 41].

VÝZNAM ROPY

- 95 % veškerých potravin je pěstována za přispění ropy
- 95 % dopravy zprostředkovávají ropné deriváty
- 95 % veškerého vyráběného zboží potřebuje pro svou výrobu ropu
- za každou kalorii běžně vyráběných potravin se skrývá 10 kalorií z ropy
- na výrobu jednoho typického počítače se spotřebuje ropa o množství desetinásobku jeho hmotnosti

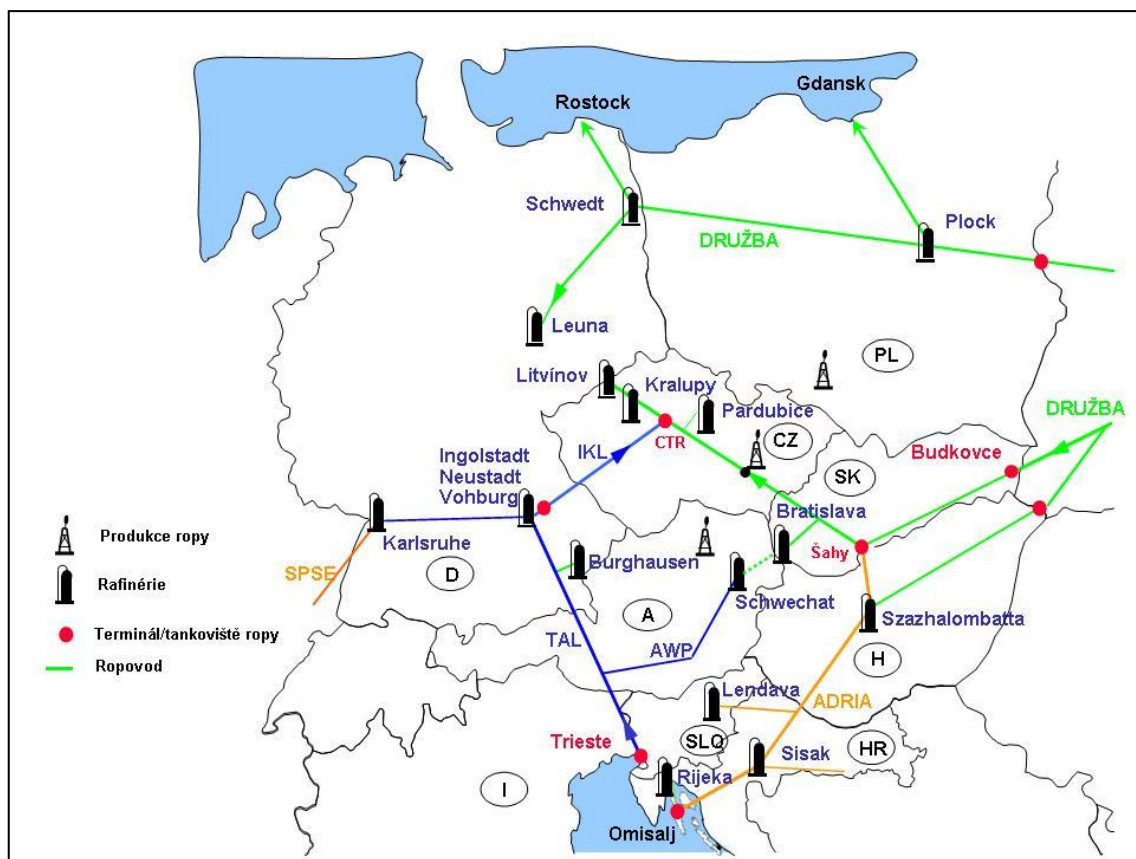
Obrázek 3 – Význam ropy pro společnost [40]

Ropu lze popsat jako žlutohnědou, až do černa zbarvenou a hořlavou kapalinu. Jedná se o bohatou směs kapalných uhlovodíků, ve které jsou rozpuštěny další plynné a pevné uhlovodíky a dále také jiné organické sloučeniny. Surová ropa sice hoří, ale za vzniku značného množství sazí, což je z pohledu využitelnosti ropy člověkem nežádoucí. Důležitým milníkem, který umožnil tak masivní rozvoj petrochemického průmyslu, bylo zvládnutí základního procesu zpracování ropy – frakční atmosférické destilace (průmyslově využívána až od poloviny 19. století). Podstatou destilace je oddělení jednotlivých frakcí uhlovodíků, za běžného (atmosférického) tlaku a na základě jejich odlišného bodu varu. Možnost, takto zpracovávat ropu v rafinériích, zajistila lidské civilizaci přístup k ropným produktům jako jsou topné plyny, oleje (topné, motorové, průmyslové), pohonné hmoty pro automobilovou, leteckou a lodní dopravu, rozpouštědla, parafín a dalšího množství chemikálií následně zpracovávaných chemickým průmyslem [40, 41].

Lze jí nalézt v nejsvrchnějších vrstvách zemské kůry, kde vytváří ropná ložiska. Tato ložiska jsou na pevnině, stejně jako pod dnem moří a oceánů. Mezi státy s největšími zásobami ropy patří například Venezuela, Saudská Arábie, Kanada, Irán a Irák. Česká republika má také na svém území naleziště ropy. Jedná nevelké ložisko na území Jihomoravského kraje, které pokrývá spotřebu ropy v ČR jen z několika málo procent. Jakmile je ropa z ložiska vrtem vytěžena, dochází k jejímu transportu do skladovacích zařízení (např. v přístavech) nebo rovnou ke jejímu koncovému uživateli. K přepravě ropy na velké vzdálenosti se využívá dvou možností, přepravy potrubním systémem (ropovody) nebo lodní přepravy (tankery). Pro transport ropy na kratší vzdálenosti lze využít cisteren silniční nebo železniční dopravy [40, 41].

Česká republika, jako stát střední Evropy, nemá dostatečné množství vlastních zdrojů ropy, a je proto nucena její drtivou většinu dovážet. Díky tomu, že stejný problém řešily i okolní průmyslově rozvinuté státy Evropy, docházelo od 2. poloviny 20. století k budování rozsáhlé sítě ropovodů napříč Evropou. Z pohledu ČR je zásobování strategicky důležitou ropou zajištěno ropovody Družba a IKL [41].

Družba je, se svými 5 100 km délkou, považován za nejdelší ropovod světa a zásobuje ruskou ropou 8 zemí Evropy (Německo, Polsko, ČR, Slovensko, Maďarsko, Ukrajina, Bělorusko a samozřejmě také samotné Rusko). Ropovod IKL vznikl v 90. letech 20. století jako alternativa k Družbě a také jako určitá „pojistka“ před energetickou závislostí České republiky na ruské ropě. Jeho název je odvozen od původně zamýšlené trasy tohoto ropovodu (Ingolstadt – Kralupy nad Vltavou – Litvínov). Začíná v Bavorsku (Vohlburgu), kde je napojen na evropský ropovod TAL (spojení s italským přístavem Terst) a pokračuje na území ČR, kde také končí [42, 43].



Obrázek 4 – Síť ropovodů v Evropě [41]

3.8.1 Ropovodná síť ČR

Přepravní (ropovodná) soustava ČR je sítí ropovodů, včetně veškerých souvisejících zařízení, předávacích a přečerpávacích stanic, řídicích a bezpečnostních systémů, informačních a komunikačních technologií. Vlastníkem a provozovatelem české sítě ropovodů je firma MERO ČR, a.s., jejímž stoprocentním vlastníkem je stát (Ministerstvo Financí ČR). Firma MERO ČR je jediným přepravcem, oprávněným dovážet ropu na území České republiky. Dále tato společnost zajišťuje skladování nouzových strategických zásob ropy v Centrálním tankovišti ropy Nelahozeves (dále také „CTR Nelahozeves“) [44].

Soustava ropovodů je na území ČR tvořena ropovody Družba a IKL. Ropovod Družba vstupuje na naše území pod řekou Moravou u Hodonína, přes Vysočinu pokračuje do Polabí, kde mívá Kralupy nad Vltavou a pokračuje

až do Litvínova. Délka ropovodu na našem území je 357 km a ropa v něm proudí potrubím o průměru 528 a 714 mm, při provozním tlaku od 4 do 64 barů. Družbou dopravená ropa pokrývá zhruba 2/3 spotřeby České republiky. Česká část ropovodu IKL dosahuje délky 169 km, vstupuje na naše území nedaleko od Rozvadova a pokračuje do CTR v Nelahozevsi a zásobuje ropou také přílehlou rafinerii v Kralupech nad Vltavou [44].



Obrázek 5 – Ropovody na území České republiky [44]

3.8.2 Skladování ropy

Jestliže je ČR energeticky závislá na ropě, dostatečné množství zásob této komodity může být způsobem, jak se chránit před jejím nedostatkem. Zmínili jsme fakt, že ČR se touto hrozbou v minulosti zabývala a výsledkem bylo vybudování ropovodu IKL. Vstupem do Evropské unie se Česká republika zavázala, že bude vlastnit zásoby ropy a ropných produktů na 90 dnů své průměrné denní spotřeby. Tato okolnost byla důvodem k vybudování Centrálního tankoviště ropy Nelahozeves. CTR Nelahozeves je určeno ke skladování strategických nouzových zásob ropy České republiky, dále také jako krátkodobý mezisklad ropy před její následnou distribucí

rafinériím. Areál tankoviště zabírá plochu 59 hektarů a je tvořen soustavou 17 samostatných nadzemních zásobníků. Čtyři nádrže jednotlivého objemu 50 000 m³, dále šest nádrží o objemu 100 000 m³ a sedm nádrží o objemu 125 000 m³. V pravidelných intervalech dochází ke kontrolám parametrů skladované ropy a její průběžné obměně. Při zajištění všech potřebných technologických postupů je možné uskladnit ropu, bez významnějších ztrát její kvality, po dobu až 15 let [44].



Obrázek 6 – Centrální tankoviště ropy Nelahozeves [44]

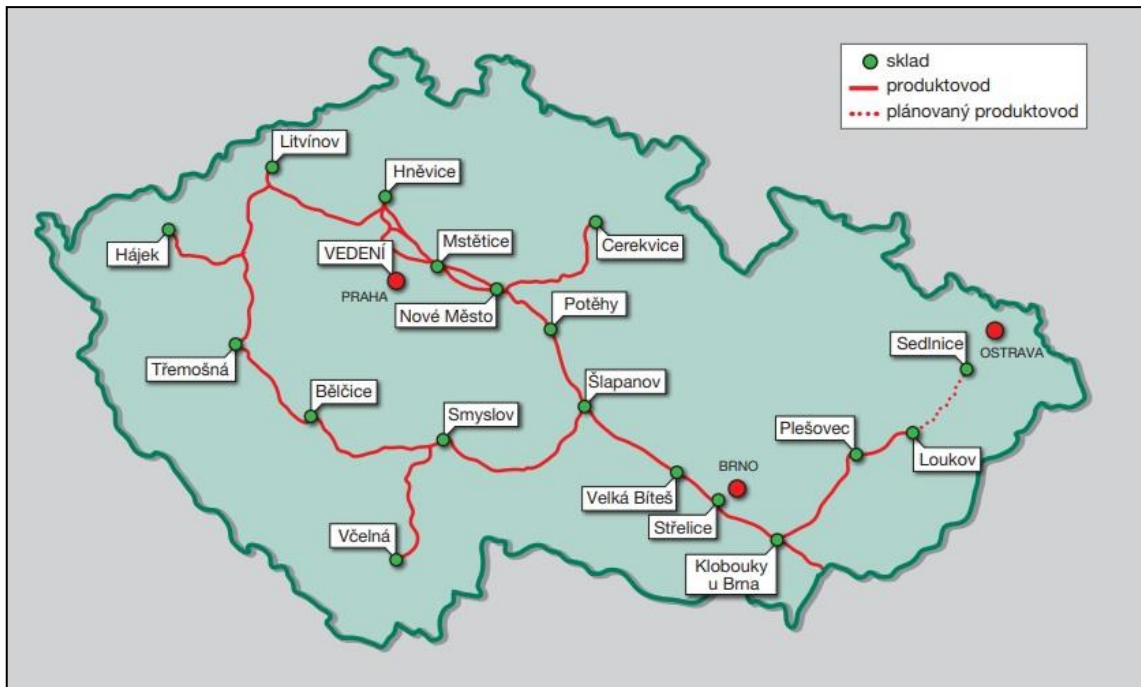
Vybudováním tohoto centrálního tankoviště byla vyřešena otázka skladování strategických zásob ropy, nikoliv však ropných produktů.

3.8.3 Ropné produkty

Česká republika je svým členstvím v Evropské unii a Mezinárodní energetické agentuře (IEA – International Energy Agency) nucena si zajistit zásoby ropy a ropných produktů v dostatečném množství k pokrytí průměrné denní spotřeby ČR na 90 dní. Tyto zásoby,

stejně jako mnohé další strategické zásoby, Česká republika zabezpečuje prostřednictvím Správy státních hmotných rezerv ČR. Ke skladování ropy a ropných produktů byly využity podnikatelské subjekty. Skladování ropy zajišťuje společnost MERO ČR a.s., v případě ropných produktů se jedná o společnost Čepro, a.s. Tato společnost skladuje uvedené množství strategických zásob jednotlivých uvedených ropných produktů a udržuje jejich požadovanou jakost, provádí jejich průběžné obměny. Mezi skladované ropné produkty patří automobilový benzín, motorová nafta, letecký petrolej, topné a mazací oleje [45].

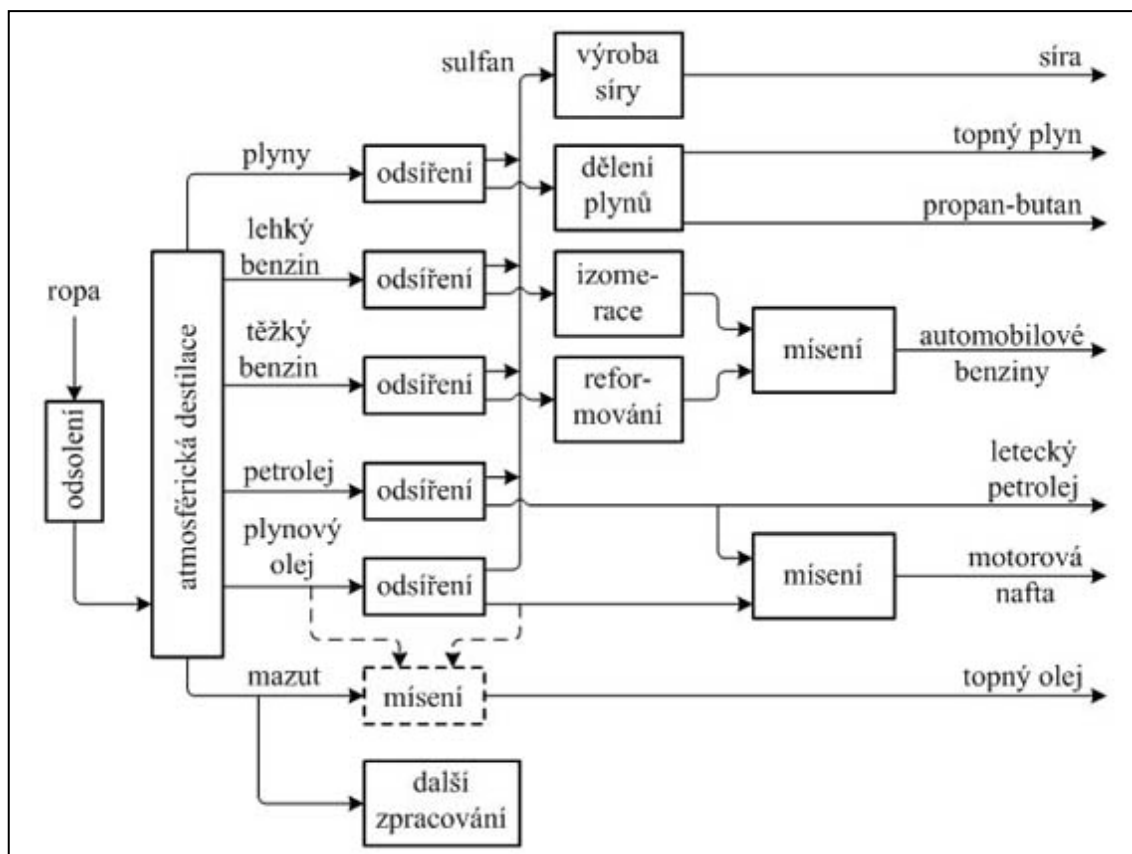
Firma Čepro a.s., jejímž stoprocentním vlastníkem je opět stát, má jako jeden z hlavních úkolů ochranu příslušných zásob státních hmotných rezerv. K uskladnění těchto strategických zásob využívá své široké sítě produktovodů a skladů. Síť produktovodů dosahuje na území ČR délky 1 100 km a její strategický význam zvyšuje přímé napojení na rafinerie v Záluží u Litvínova, Kralupech nad Vltavou. Ke skladování lze využít 18 skladů, disponujících více než 600 nádržemi s celkovou kapacitou přesahující 1,5 miliónů m³. Jednotlivé areály tvoří podzemní a nadzemí zásobníky, manipulační nádrže, plnicí stanoviště automobilových a železničních cisteren a další nezbytné technologické zázemí jako laboratoře nebo také hasičské stanice. Nejstarším a současně také největším skladem je areál v Hněvicích nedaleko Roudnice nad Labem. V areálu o rozloze 260 hektarů se nachází 101 nádrží ke skladování ropných produktů [46].



Obrázek 7 – Síť skladů a produktovodů společnosti Čepro a.s. v ČR [46].

3.8.4 Výroba pohonných hmot

V této práci jsme již zmínili, že výroba pohonných hmot probíhá v rafinériích pomocí atmosférické destilace. Při ní dochází k rozdělení ropy do jednotlivých frakcí a ty jsou následně využívány k výrobě jednotlivých pohonných hmot. Proces samotné výroby samozřejmě není takto jednoduchý. Pokusíme-li se postup výroby pohonných hmot značně zjednodušit, můžeme ho popsat, jako řetězec čtyř po sobě následujících kroků: odsolování ropy – frakční atmosférická destilace – vakuová destilace – petrochemická výroba. Nelze zapomenout na to, že během výrobního postupu dochází u jednotlivých frakcí ropy k odstraňování síry (oxid siřičitý – SO_2 , vznikající spalováním síry, poškozující životní prostředí) a někdy také ke snižování aromátů (benzen, toluen apod.) [47].



Obrázek 8 – Schéma zpracování ropy na pohonné hmoty [47]

Výroba pohonných hmot je z pohledu České republiky zajišťována společností Unipetrol a.s. (a jejími dceřinými firmami), která provozuje rafinérie v Záluží u Litvínova a Kralupech nad Vltavou. Stoprocentním vlastníkem Unipetrolu je polská společnost PKN ORLEN, která odkoupila rozhodující podíl akcií v roce 2005. Ropa do zmíněných rafinérií proudí z Ruské federace ropovodem Družba nebo ropovodem IKL. Dodávka ropy v řádu jednotek procent, zajišťované společností Moravské naftové doly, je do rafinérií dopravována ropovodem Družba nebo cisternami po železnici. Rafinérie ropu přebírají na hranici svého areálu a uskladňují ji pro následné zpracování. Expedice vyrobených produktů z rafinérie probíhá pomocí cisteren po silnici nebo železnici. V případě, že je odběratelem ropných produktů společnost Čepro a.s., putují pohonné hmoty do jejich skladů produktovody [48].

Rafinérie v Záluží u Litvínova je moderní rafinérií, provozující dvě jednotky destilace ropy. Roční kapacita zpracované ropy litvínovské rafinérie činí zhruba 5,5 miliónů tun. Zpracovávána je zde sirná ropa, dodávaná ropovody Družba a IKL. I to je důvodem toho, proč je součástí rafinérie řada dalších technologických zařízení, zvyšujících kvalitu primárně destilovaných produktů. Mezi hlavní produkty patří automobilové benzíny, motorová nafta a zkapalněný ropný plyn (LPG). Z dalších strategických výrobků a surovin pro petrochemickou výrobu lze zmínit výrobu topných olejů, asfaltů, olejové hydrogenázy (ropného polotovaru k výrobě mazacích olejů) apod [48].

Rafinérie v Kralupech, naposledy modernizovaná v roce 2018, je druhou rafinérií společnosti Unipetrol. Ročně dokáže zpracovat 3,3 miliónů tun ropy, což je zhruba jedna třetina veškeré zpracované ropy v ČR. Kralupská rafinérie zpracovává ropu z ropovodu IKL s nízkým obsahem síry (ropa pocházející z Ázerbájdžánu, Kazachstánu nebo Saudské Arábie) a českou ropu od společnosti MND. Díky své technologii je tato rafinérie určena k výrobě vysokooktanových bezolovnatých benzínů a je také výrobcem leteckého petroleje JET A1, který je odebírán mezinárodním letištěm Praha/Ruzyně. Expedice produktů probíhá převážně automobilovými a železničními cisternami [48, 49].

4 METODIKA

V následující části bakalářské práce bude provedena bezpečnostní analýza výše zmíněných oblastí kritické infrastruktury České republiky, tedy zemního plynu, ropy a ropných produktů.

Oblast kritické infrastruktury se s rozvojem moderních technologií stává stále složitější, dochází k propojování jednotlivých systémů a struktur. To jsou okolnosti, díky kterým je také ochrana KI stále komplikovanější a finančně nákladnější. Ochrana může být rozdělena do dvou rovin: prevence a represe. Analýza je nezbytným preventivním krokem k ochraně kritické infrastruktury. Z důvodu zmíněné rozsáhlosti KI jí nelze dostatečně chránit jako celek a je tedy nutné se soustředit na ochranu kritických míst systémů KI [4, 50].

Ochrana kritické infrastruktury je tedy závislá na správně vypracované a kvalitní analýze rizik. Pomocí takovýchto analýz lze hrozící rizika odhalit a následně je snížit na přijatelnou míru. Použití běžně užívaných metod analýzy rizik však nebylo odborníky, z oblasti ochrany kritické infrastruktury, shledáno jako zcela vhodné. Důvodem je to, že běžné metody analýzy vyhodnocují očekávanou výši škody, což není pro oblast kritické infrastruktury ideální. Dalším problémem, při použití těchto metod, je neexistence odpovídajících statistik pro výpadky posuzovaných infrastruktur. Z tohoto důvodu začala být využívána metoda založená na principu „posouzení kritičnosti“. Cílem metody není zjištění, kdo nebo co ohrožuje jednotlivé prvky nebo procesy, ale zda může být takovýto kritický proces značně poškozený či dokonce dojít k jeho úplnému výpadku [4, 50].

4.1 Analýza AKIS

Jednou z možných metod, umožňující získání rychlého přehledu o daném sektoru KI, je analýza metodou AKIS. Tuto metodu poprvé uvedl do praxe v roce 2002 německý Spolkový úřad pro bezpečnost informační techniky. Analýza metodou AKIS umožňuje získat v krátkém čase dostatečně detailní informace na to, abychom získali přehled a znalost o fungování dané infrastruktury [50].

Nejprve se vytvoří přehled o analyzovaných sektorech KI a dojde k jejich rozčlenění. Je nutné se blíže seznámit s posuzovaným sektorem, pochopit význam sektoru pro společnost. Je zapotřebí zjistit, jak sektor funguje, identifikovat případné klíčové podniky. Takto zkoumaný sektor je možné rozdělit na jednotlivá odvětví nebo služby, u kterých je následně nutné určit kritické provozní procesy (procesy, které mají z hlediska kritičnosti význam) [3].

V dalším kroku dojde ke zhodnocení procesů a vyhodnotí se jejich kritičnost. Pro vypovídající hodnotu takového zhodnocení je zapotřebí spolupracovat s odborníky v daném sektoru. Při hodnocení kritičnosti je potřeba využít znalosti dané problematiky, poznatky z praxe a fundované názory na to, jaké riziko představuje určitá hrozba či jaké následky narušení konkrétního procesu KI bude mít. Je-li to možné, necháme posuzovaný sektor zhodnotit větším počtem odborníků. Kombinací dopadu a pravděpodobnosti výpadku získáme kritičnost daného procesu. Pro hodnocení kritičnosti, výsledků odpovědí odborníků, je možné jednotlivé procesy uspořádat do matice kritičnosti [3, 50].

Společně s kritičností bude hodnocena také zranitelnost daného odvětví (respektive sektoru). Zranitelnost lze popsat jako určitou slabinu, či stav

analyzovaného prvku, procesu nebo služby. Tato hodnota vyjadřuje to, jak moc je zkoumané aktivum citlivé na působení dané hrozby.

Pro potřeby naší analýzy AKIS byla jednotlivá odvětví rozdělena následovně.

1) Odvětví zemního plynu.

- **Sektor č. 1 – přepravní soustava;**
 - tranzitní nebo vnitrostátní plynovody;
 - kompresorová stanice;
 - předávací stanice.
- **Sektor č. 2 – distribuční soustava;**
 - vysokotlaké a středotlaké plynovody;
 - předávací a regulační stanice;
 - technický dispečink.
- **Sektor č. 3 – skladování plynu;**
 - podzemní zásobník plynu;
 - technický dispečink.

2) Odvětví ropy a ropných produktů.

- **Sektor č. 1 – přepravní soustava;**
 - tranzitní, vnitrostátní ropovod;
 - přečerpávací stanice;
 - technický dispečink.
- **Sektor č. 2 – distribuční soustava;**
 - produktovody;
 - přečerpávací stanice;
 - technický dispečink.

- **Sektor č. 3 – skladování ropy a pohonných hmot;**
 - zásobníky;
 - technický dispečink.
- **Sektor č. 4 – výroba pohonných hmot;**
 - rafinérie.

Získaná struktura byla zpracována do podoby dotazníků, které byly použity k šetření. Dotazníky (přílohy č. 2 a 3) byly rozeslány odborníkům, zainteresovaným firmám v daných odvětví zemního plynu, ropy a ropných produktů.

5 VÝSLEDKY

Dotazníky byly rozeslány firmám zainteresovaným v daných odvětvích kritické infrastruktury, napříč všemi určenými sektory. Většina oslovených firem, odborníků však odmítla dotazník vyplnit a potřebné informace poskytnout. Důvodem, dle jejich slov, bylo především to, že se jedná o velmi citlivé informace týkající se bezpečnosti kritické infrastruktury. Tato okolnost zapříčinila to, že se stalo prakticky nemožné, pro potřeby této bakalářské práce, vypracovat analýzu metodou AKIS, poskytující konkrétní data či relevantní hodnoty. Na druhou stranu tato situace jednoznačně potvrzuje fakt, že ochrana kritické infrastruktury není v České republice brána na lehkou váhu.

Nedostatečná zpětná odezva na dotazníkové šetření však nevylučuje možnost vypracovat analýzu metodou AKIS tak, aby tato práce vysvětlila samotný princip tvorby takovéto analýzy. Z tohoto důvodu byly autorem práce doplněny další, jím vyplněné dotazníky, potřebné k vypracování vzorové analýzy metodou AKIS.

Již jsme zmínili, že je žádoucí provést dotazníkové šetření mezi co největším počtem odborníků. Větší počet dotazovaných může být jistou pojistkou validních výstupních dat zpracovávané analýzy. Protože v našem případě nebudou konkrétní hodnoty primárním cílem zmíněné analýzy, dojde v každém odvětví k vyhodnocení pouze 4 dotazníků, které jsou k vypracování vzorové analýzy metodou AKIS zcela dostačující.

5.1 Analýza AKIS odvětví zemního plynu

Tabulka 4 – Dotazník 1 (vlastní)

DOTAZNÍK OHROŽENÍ KRITICKÉ INFRASTRUKTURY – ODVĚTVÍ ZEMNÍ PLYN (ANALÝZA METODOU AKIS) (Autor: Daniel Ondra)								
Jméno: Jaroslav Damborský					Firma: MND Gas Storage a.s.			
	Sektor 1 – Přepravní soustava			Sektor 2 – Distribuční soustava			Sektor 3 – Skladování plynu	
	Tranzitní nebo vnitrostátní plynovody	Kompresorová stanice	Předávací stanice	VysokoTL. a středoTL. plynovody	Předávací a regulační stanice	Technický dispečink	Podzemní zásobník plynu	Technický dispečink
Zranitelnost							2	5
Riziko ÚMYSLNÉHO poškození člověkem							2	0
Riziko poškození člověkem z NEDBALOSTI							1	1
Riziko poškození živelnými pohromami							2	0
Současná bezpečnostní opatření provozovatele							98	95
Pravděpodobnost zasažení velkého počtu lidí při selhání prvku plyn. soustavy							0	0

Oslovený respondent se rozhodl zhodnotit pouze sektor č. 3 odvětví zemního plynu, ve kterém pracuje. Není tudíž možné sestavit pořadí jednotlivých sektorů odvětví zemního plynu.

Tabulka 5 – Zranitelnost dle dotazníku 1 (vlastní)

ZRANITELNOST DLE DOTAZNÍKU 1			
Sektor č. 1 (přepravní soustava)	Tranzitní nebo vnitrostátní plynovody	X	X
	Kompresorová stanice	X	
	Předávací stanice	X	
Sektor č. 2 (distribuční soustava)	Vysokotlaké. a středotlaké plynovody	X	X
	Předávací a regulační stanice	X	
	Technický dispečink	X	
Sektor č. 3 (skladování plynu)	Podzemní zásobník plynu	2 %	3,5 %
	Technický dispečink	5 %	

Z prvního dotazníku z pohledu zranitelnosti nelze sektory č. 1 a 2 zhodnotit. Respondentem hodnocený sektor č. 3 dosáhl zranitelnosti 3,5 %.

Tabulka 6 – Riziko poškození dle dotazníku 1 (vlastní)

RIZIKO POŠKOZENÍ DLE DOTAZNÍKU 1			
Sektor č. 1 (přepravní soustava)	Tranzitní nebo vnitrostátní plynovody	X	X
	Kompresorová stanice	X	
	Předávací stanice	X	
Sektor č. 2 (distribuční soustava)	Vysokotlaké. a středotlaké plynovody	X	X
	Předávací a regulační stanice	X	
	Technický dispečink	X	
Sektor č. 3 (skladování plynu)	Podzemní zásobník plynu	1,6 %	0,95 %
	Technický dispečink	0,3 %	

Respondent v první dotazníku také nevyplnil riziko poškození prvních dvou sektorů odvětví zemního plynu. Sektor č. 3 byl hodnocen rizikem poškození 0,95 %.

Tabulka 7 – Dotazník 2 (vlastní)

DOTAZNÍK OHROŽENÍ KRITICKÉ INFRASTRUKTURY – ODVĚTVÍ ZEMNÍ PLYN (ANALÝZA METODOU AKIS) (Autor: Daniel Ondra)								
Jméno: Martin Janíčko					Firma: MND a.s.			
	Sektor 1 – Přepravní soustava			Sektor 2 – Distribuční soustava			Sektor 3 – Skladování plynu	
	Tranzitní nebo vnitrostátní plynovody	Kompresorová stanice	Předávací stanice	VysokoTL. a středoTL. plynovody	Předávací a regulační stanice	Technický dispečink	Podzemní zásobník plynu	Technický dispečink
Zranitelnost	15	15	15	25	20	30	20	15
Riziko ÚMYSLNÉHO poškození člověkem	50	50	50	50	50	50	15	15
Riziko poškození člověkem z NEDBALOSTI	50	50	50	50	50	50	15	15
Riziko poškození živelnými pohromami	50	50	50	45	50	50	40	15
Současná bezpečnostní opatření provozovatele	15	15	25	15	10	10	20	10
Pravděpodobnost zasažení velkého počtu lidí při selhání prvku plyn. soustavy	25	15	25	25	25	30	40	15

Tabulka 8 – Zranitelnost dle dotazníku 2 (vlastní)

ZRANITELNOST DLE DOTAZNÍKU 2			
Sektor č. 1 (přepravní soustava)	Tranzitní nebo vnitrostátní plynovody	15 %	15 %
	Kompresorová stanice	15 %	
	Předávací stanice	15 %	
Sektor č. 2 (distribuční soustava)	Vysokotlaké. a středotlaké plynovody	25 %	25 %
	Předávací a regulační stanice	20 %	
	Technický dispečink	30 %	
Sektor č. 3 (skladování plynu)	Podzemní zásobník plynu	20 %	17,5 %
	Technický dispečink	15 %	

Respondent druhého dotazníku vyhodnotil z hlediska zranitelnosti sektor č. 2 jako nejzranitelnější (25 %). Úsek č. 3 (skladování plynu) je s hodnotou 17,5 % zranitelný o něco méně a nejméně zranitelným se jeví sektor č. 1.

Tabulka 9 – Riziko poškození dle dotazníku 2 (vlastní)

RIZIKO POŠKOZENÍ DLE DOTAZNÍKU 2			
Sektor č. 1 (přepravní soustava)	Tranzitní nebo vnitrostátní plynovody	50 %	50 %
	Kompresorová stanice	50 %	
	Předávací stanice	50 %	
Sektor č. 2 (distribuční soustava)	Vysokotlaké. a středotlaké plynovody	48,3 %	49,43 %
	Předávací a regulační stanice	50 %	
	Technický dispečink	50 %	
Sektor č. 3 (skladování plynu)	Podzemní zásobník plynu	23,3 %	19,15 %
	Technický dispečink	15 %	

Druhý dotazník označil z hlediska rizika poškození sektory č. 1 a 2 za téměř stejně rizikové. Nejrizikovější je sektor č. 2 s rizikem poškození 50 %. Těsně jej následuje sektor č. 2 s rizikem poškození 49,43 %. Nejbezpečnějším sektorem odvětví zemního plynu se stal, dle dotazníku 2, sektor č. 3.

Tabulka 10 – Dotazník 3 (vlastní)

DOTAZNÍK OHROŽENÍ KRITICKÉ INFRASTRUKTURY – ODVĚTVÍ ZEMNÍ PLYN (ANALÝZA METODOU AKIS) (Autor: Daniel Ondra)								
Jméno: Autor 1					Firma: XXX			
	Sektor 1 - Převravní soustava			Sektor 2 - Distribuční soustava			Sektor 3 - Skladování plynu	
	Tranzitní nebo vnitrostátní plynovody	Kompresorová stanice	Předávací stanice	VysokoTL. a středotl. plynovody	Předávací a regulační stanice	Technický dispečink	Podzemní zásobník plynu	Technický dispečink
Zranitelnost	15	20	15	15	20	20	25	20
Riziko ÚMYSLNÉHO poškození člověkem	20	20	20	10	15	5	10	5
Riziko poškození člověkem z NEDBALOSTI	20	20	20	10	10	5	5	5
Riziko poškození živelnými pohromami	10	15	10	10	10	10	10	10
Současná bezpečnostní opatření provozovatele	90	85	85	80	85	90	90	90
Pravděpodobnost zasažení velkého počtu lidí při selhání prvku plyn. soustavy	40	35	40	25	25	20	40	35

Tabulka 11 – Zranitelnost dle dotazníku 3 (vlastní)

ZRANITELNOST DLE DOTAZNÍKU 3			
Sektor č. 1 (převravní soustava)	Tranzitní nebo vnitrostátní plynovody	15 %	16,67 %
	Kompresorová stanice	20 %	
	Předávací stanice	15 %	
Sektor č. 2 (distribuční soustava)	Vysokotlaké. a středotlaké plynovody	15 %	18,33 %
	Předávací a regulační stanice	20 %	
	Technický dispečink	20 %	
Sektor č. 3 (skladování plynu)	Podzemní zásobník plynu	25 %	22,5 %
	Technický dispečink	20 %	

Dotazník 3 označil z hlediska zranitelnosti za nejzranitelnější sektor č. 3 se zranitelností 22,5 %. Sektor č. 2 je s 18,33 % o něco méně zranitelný a sektor č. 1 je nejméně zranitelným sektorem s 16,67 %.

Tabulka 12 – Riziko poškození dle dotazníku 3 (vlastní)

RIZIKO POŠKOZENÍ DLE DOTAZNÍKU 3			
Sektor č. 1 (přepravní soustava)	Tranzitní nebo vnitrostátní plynovody	16,6 %	17,17 %
	Kompresorová stanice	18,3 %	
	Předávací stanice	16,6 %	
Sektor č. 2 (distribuční soustava)	Vysokotlaké. a středotlaké plynovody	10 %	9,4 %
	Předávací a regulační stanice	11,6 %	
	Technický dispečink	6,6 %	
Sektor č. 3 (skladování plynu)	Podzemní zásobník plynu	8,3 %	7,45 %
	Technický dispečink	6,6 %	

Nejrizikovějším sektorem z hlediska poškození byl v dotazníku 3 sektor č. 1 s hodnotou rizika 17,17 %. Sektor č. 2 dosáhl rizika 9,4 % a nejméně rizikovým byl sektor č. 3 s hodnotou rizika poškození 7,45 %.

Tabulka 13 – Dotazník 4 (vlastní)

DOTAZNÍK OHROŽENÍ KRITICKÉ INFRASTRUKTURY - ODVĚTVÍ ZEMNÍ PLYN (ANALÝZA METODOU AKIS) (Autor: Daniel Ondra)								
Jméno: Autor 2					Firma: XXX			
	Sektor 1 - Přepravní soustava			Sektor 2 - Distribuční soustava			Sektor 3 - Skladování plynu	
	Tranzitní nebo vnitrostátní plynovody	Kompresorová stanice	Předávací stanice	VysokoTL. a středoTL. plynovody	Předávací a regulační stanice	Technický dispečink	Podzemní zásobník plynu	Technický dispečink
Zranitelnost	10	15	15	15	15	15	5	5
Riziko ÚMYSLNÉHO poškození člověkem	5	15	15	10	10	5	5	5
Riziko poškození člověkem z NEDBALOSTI	5	10	10	5	5	5	10	5
Riziko poškození živelnými pohromami	5	10	10	10	10	5	5	5
Současná bezpečnostní opatření provozovatele	95	95	95	90	95	85	95	95
Pravděpodobnost zasažení velkého počtu lidí při selhání prvku plyn. soustavy	20	15	10	20	15	10	20	10

Tabulka 14 – Zranitelnost dle dotazníku 4 (vlastní)

ZRANITELNOST DLE DOTAZNÍKU 4			
Sektor č. 1 (přepravní soustava)	Tranzitní nebo vnitrostátní plynovody	10 %	13,33 %
	Kompresorová stanice	15 %	
	Předávací stanice	15 %	
Sektor č. 2 (distribuční soustava)	Vysokotlaké. a středotlaké plynovody	15 %	15 %
	Předávací a regulační stanice	15 %	
	Technický dispečink	15 %	
Sektor č. 3 (skladování plynu)	Podzemní zásobník plynu	5 %	5 %
	Technický dispečink	5 %	

Dotazník 4 z hlediska zranitelnosti vyhodnotil za nezranitelnější sektor č. 2 s hodnotou zranitelnosti 15 %. Nižší hodnoty zranitelnosti dosáhl sektor č. 1 s hodnotou 13,3 % a nejméně zranitelným byl určen sektor č. 3 s 5 %.

Tabulka 15 – Riziko poškození dle dotazníku 4 (vlastní)

RIZIKO POŠKOZENÍ DLE DOTAZNÍKU 4			
Sektor č. 1 (přepravní soustava)	Tranzitní nebo vnitrostátní plynovody	5 %	9,4 %
	Kompresorová stanice	11,6 %	
	Předávací stanice	11,6 %	
Sektor č. 2 (distribuční soustava)	Vysokotlaké. a středotlaké plynovody	8,3 %	7,2 %
	Předávací a regulační stanice	8,3 %	
	Technický dispečink	5 %	
Sektor č. 3 (skladování plynu)	Podzemní zásobník plynu	6,6 %	5,8 %
	Technický dispečink	5 %	

Respondent dotazníku 4 z hlediska rizika poškození vyhodnotil za nejrizikovější s hodnotou 9,4 % sektor č. 1. Druhý skončil s 7,4 % sektor č. 2 a nejméně rizikovým sektor č. 3 s rizikem 5,8 %.

Tabulka 16 – Celková zranitelnost odvětví zemního plynu (vlastní)

CELKOVÁ ZRANITELNOST ODVĚTVÍ ZEMNÍHO PLYNU						
		Dotazník 1	Dotazník 2	Dotazník 3	Dotazník 4	Výsledek
Sektor č. 1	Tranzitní a vnitrostátní plynovody	X	15 %	16,67 %	13,33 %	15 %
	Kompresorová stanice					
	Předávací stanice					
Sektor č. 2	Vysokotlaké a středotlaké plynovody	X	25 %	18,33 %	15 %	19,44 %
	Předávací a regulační stanice					
	Technický dispečink					
Sektor č. 3	Podzemní zásobník plynu	3,5 %	17,5 %	22,5 %	5 %	12,1 %
	Technický dispečink					

V celkovém vyhodnocení zranitelnosti odvětví zemního plynu je nejzranitelnějším sektorem sektor č. 2 se zranitelností 19,44 %.

Méně zranitelný je sektor č. 1 o zranitelnosti 15 % a nejbezpečnějším sektorem odvětví zemního plynu je sektor č. 3 s hodnotou zranitelnosti 12,1 %.

Tabulka 17 – Celkové riziko poškození odvětví zemního plynu (vlastní)

CELKOVÉ RIZIKO POŠKOZENÍ ODVĚTVÍ ZEMNÍHO PLYNU						
		Dotazník 1	Dotazník 2	Dotazník 3	Dotazník 4	Výsledek
Sektor č. 1	Tranzitní a vnitrostátní plynovody	X	15 %	16,6 %	9,4 %	14,9 %
	Kompresorová stanice					
	Předávací stanice					
Sektor č. 2	Vysokotlaké a středotlaké plynovody	X	25 %	18,3 %	7,2 %	19,4 %
	Předávací a regulační stanice					
	Technický dispečink					
Sektor č. 3	Podzemní zásobník plynu	0,9 %	17,5 %	22,5 %	5,8 %	12,1 %
	Technický dispečink					

Sektor č. 2 je také celkově vyhodnocen za nejrizikovějším z hlediska rizika poškození. S hodnotou 14,9 % skončil sektor č. 1 druhý a nejméně rizikovým sektorem z hlediska poškození je z odvětví zemního plynu sektor č. 3 s rizikem poškození 12,1 %.

Z obou posuzovaných hledisek (zranitelnosti a rizika poškození) je v odvětví zemního plynu nejzranitelnějším sektor č. 2 (distribuční soustava). Na tento výsledek má s velkou pravděpodobností vliv značná délka distribuční soustavy na území ČR (přes 73 000 km). Tato okolnost, společně s velkým množstvím odběrných míst plynu, logicky vylučuje možnost důkladného zabezpečení každé jednotlivé části distribuční soustavy. Na druhou byla distribuční soustava ve všech vyhodnocených dotaznících hodnocena jako sektor s nízkou pravděpodobností zasažení velkého počtu lidí při selhání prvku plynárenské soustavy. Nejnižší zranitelnost, stejně jako riziko poškození, vykazuje sektor č. 3. Jedná se o relativně nízký počet objektů (zásobníků plynu).

Otázku bezpečnosti je tedy u nich možné řešit do sebemenšího detailu a takto snížit rizika na přijatelnou míru.

5.2 Analýza AKIS ropy a ropných produktů

Tabulka 18 – Dotazník 5 (vlastní)

DOTAZNÍK OHROŽENÍ KRITICKÉ INFRASTRUKTURY – ODVĚTVÍ ROPA A ROPNÉ PRODUKTY (ANALÝZA METODOU AKIS) (Autor: Daniel Ondra)									
Jméno: Autor 3					Firma: X				
	Sektor 1 - Převážná soustava			Sektor 2 - Distribuční soustava			Sektor 3 - Skladování ropy a PHM		Sektor 4 - Výroba PHM
	Tranzitní, vnitrostát. ropovod	Přečerpávací stanice	Technický dispečink	Produktovody	Přečerpávací stanice	Technický dispečink	Zásobníky	Technický dispečink	Rafrinérie
Zranitelnost	5	15	5	5	10	5	5	10	20
Riziko ÚMYSLNÉHO poškození člověkem	10	15	10	15	15	10	10	5	10
Riziko poškození člověkem z NEDBALOSTI	10	10	10	10	15	10	10	5	20
Riziko poškození živelnými pohromami	10	15	5	10	10	10	5	5	20
Současná bezpečnostní opatření provozovatele	95	95	95	90	90	90	99	95	95
Pravděpodobnost zasažení velkého počtu lidí při selhání prvku ropné soustavy	50	50	40	30	30	30	50	40	60

Tabulka 19 – Zranitelnost dle dotazníku 5 (vlastní)

ZRANITELNOST DLE DOTAZNÍKU 5			
Sektor č. 1 (přepravní soustava)	Tranzitní a vnitrostátní ropovod	5 %	8,33 %
	Přečerpávací stanice	15 %	
	Technický dispečink	5 %	
Sektor č. 2 (distribuční soustava)	Produktovody	5 %	6,67 %
	Přečerpávací stanice	10 %	
	Technický dispečink	5 %	
Sektor č. 3 (skladování plynu)	Zásobníky ropy	5 %	7,5 %
	Technický dispečink	10 %	
Sektor č. 4 (výroba PHM)	Rafinérie		20 %

Z hlediska zranitelnosti byl v dotazníku 5 označen za nejzranitelnější sektor č. 4 s hodnotou zranitelnosti (20 %). Ostatní tři sektory dosahovaly velmi podobných hodnot zranitelnosti v rozmezí 6,67 – 8,33 %.

Tabulka 20 – Riziko poškození dle dotazníku 5 (vlastní)

RIZIKO POŠKOZENÍ DLE DOTAZNÍKU 5			
Sektor č. 1 (přepravní soustava)	Tranzitní a vnitrostátní ropovod	10 %	10,55 %
	Přečerpávací stanice	13,33 %	
	Technický dispečink	8,33 %	
Sektor č. 2 (distribuční soustava)	Produktovody	11,67 %	11,67 %
	Přečerpávací stanice	13,33 %	
	Technický dispečink	10 %	
Sektor č. 3 (skladování plynu)	Zásobníky ropy	8,33 %	6,67 %
	Technický dispečink	5 %	
Sektor č. 4 (výroba PHM)	Rafinérie		16,67 %

Respondent v dotazníku 5 vyhodnotil sektor č. 4 za nejrizikovější z hlediska možného poškození (16,67 %). Sektory č. 1 a 2 byly ohodnoceny podobným rizikem (10,55 %, resp. 11,67 %) a nejméně rizikovým sektorem byl sektor č. 3 (6,67 %).

Tabulka 21 – Dotazník 6 (vlastní)

DOTAZNÍK OHROŽENÍ KRITICKÉ INFRASTRUKTURY – ODVĚTVÍ ROPA A ROPNÉ PRODUKTY (ANALÝZA METODOU AKIS)									
(Autor: Daniel Ondra)									
Jméno: Autor 4					Firma: X				
	Sektor 1 – Přepravní soustava			Sektor 2 – Distribuční soustava			Sektor 3 – Skladování ropy a PHM		Sektor 4 – Výroba PHM
	Tranzitní, vnitrostát. ropovod	Přečerpávací stanice	Technický dispečink	Produktovody	Přečerpávací stanice	Technický dispečink	Zásobníky	Technický dispečink	Rafinérie
Zranitelnost	2	5	2	5	5	1	1	5	15
Riziko ÚMYSLNĚHO poškození člověkem	10	10	10	20	20	20	10	5	15
Riziko poškození člověkem z NEDBALOSTI	15	15	15	20	15	15	15	10	30
Riziko poškození živelnými pohromami	5	10	15	5	10	15	5	5	25
Současná bezpečnostní opatření provozovatele	80	80	80	80	80	80	99	95	90
Pravděpodobnost zasažení velkého počtu lidí při selhání prvku ropné soustavy	40	40	40	30	30	30	50	50	50

Tabulka 22 – Zranitelnost dle dotazníku 6 (vlastní)

ZRANITELNOST DLE DOTAZNÍKU 6			
Sektor č. 1 (přepravní soustava)	Tranzitní a vnitrostátní ropovod	2 %	3 %
	Přečerpávací stanice	5 %	
	Technický dispečink	2 %	
Sektor č. 2 (distribuční soustava)	Produktovody	5 %	3,67 %
	Přečerpávací stanice	5 %	
	Technický dispečink	1 %	
Sektor č. 3 (skladování plynu)	Zásobníky ropy	1 %	3 %
	Technický dispečink	5 %	
Sektor č. 4 (výroba PHM)	Rafinérie		15 %

Jako nejvíce zranitelný byl dotazníkem 6 označen sektor č. 4. Sektory č. 1 (přepravní soustava) a č. 3 (skladování plynu) byly nejméně rizikovými sektory s rizikem 3 %.

Tabulka 23 – Riziko poškození dle dotazníku 6 (vlastní)

RIZIKO POŠKOZENÍ DLE DOTAZNÍKU 6			
Sektor č. 1 (přepravní soustava)	Tranzitní a vnitrostátní ropovod	10 %	13,33 %
	Přečerpávací stanice	11,67 %	
	Technický dispečink	13,33 %	
Sektor č. 2 (distribuční soustava)	Produktovody	15 %	15 %
	Přečerpávací stanice	15 %	
	Technický dispečink	16,67 %	
Sektor č. 3 (skladování plynu)	Zásobníky ropy	10 %	10 %
	Technický dispečink	10 %	
Sektor č. 4 (výroba PHM)	Rafinérie		23,33 %

Dotazník 6 stanovil z hlediska rizika poškození za nejrizikovější sektor č. 4 s hodnotou rizika 23,33 %. Druhým nejrizikovějším sektorem se stal sektor č. 2 s 15 %. Nejbezpečnějším sektorem z hlediska rizika byl sektor č. 3 s rizikem 10 %.

Tabulka 24 – Dotazník 7 (vlastní)

DOTAZNÍK OHROŽENÍ KRITICKÉ INFRASTRUKTURY – ODVĚTVÍ ROPA A ROPNÉ PRODUKTY (ANALÝZA METODOU AKIS)									
(Autor: Daniel Ondra)									
Jméno: Autor 5					Firma: X				
	Sektor 1 – Převážná soustava			Sektor 2 – Distribuční soustava			Sektor 3 – Skladování ropy a PHM		Sektor 4 – Výroba PHM
	Tranzitní, vnitrostát. ropovod	Přečerpávací stanice	Technický dispečink	Produktovody	Přečerpávací stanice	Technický dispečink	Zásobníky	Technický dispečink	Rafinérie
Zranitelnost	20	20	20	30	30	20	40	30	40
Riziko ÚMYSLNÉHO poškození člověkem	1	15	15	20	20	10	1	5	25
Riziko poškození člověkem z NEDBALOSTI	10	10	10	20	15	10	10	10	40
Riziko poškození živelnými pohromami	10	10	10	10	10	10	5	5	20
Současná bezpečnostní opatření provozovatele	95	90	85	85	90	85	99	99	80
Pravděpodobnost zasažení velkého počtu lidí při selhání prvku ropné soustavy	50	50	50	50	50	50	50	50	50

Tabulka 25 – Zranitelnost dle dotazníku 7 (vlastní)

ZRANITELNOST DLE DOTAZNÍKU 7			
Sektor č. 1 (převážná soustava)	Tranzitní a vnitrostátní ropovod		20 %
	Přečerpávací stanice		20 %
	Technický dispečink		20 %
Sektor č. 2 (distribuční soustava)	Produktovody		30 %
	Přečerpávací stanice		30 %
	Technický dispečink		20 %
Sektor č. 3 (skladování plynu)	Zásobníky ropy		40 %
	Technický dispečink		30 %
Sektor č. 4 (výroba PHM)	Rafinérie		40 %

Čtvrtý sektor v dotazníku 7 dosáhl z hlediska zranitelnosti nejhorších výsledků (40 %). Jako druhý nejzranitelnější byl označen sektor č. 3 se zranitelností 35 %. Nejméně zranitelným sektorem se stal sektor č. 1 (20 %).

Tabulka 26 – Riziko poškození dle dotazníku 7 (vlastní)

RIZIKO POŠKOZENÍ DLE DOTAZNÍKU 7			
Sektor č. 1 (přepravní soustava)	Tranzitní a vnitrostátní ropovod	3,67 %	9 %
	Přečerpávací stanice	11,67 %	
	Technický dispečink	11,67 %	
Sektor č. 2 (distribuční soustava)	Produktovody	16,67 %	13,89 %
	Přečerpávací stanice	15 %	
	Technický dispečink	10 %	
Sektor č. 3 (skladování plynu)	Zásobníky ropy	5,33 %	6 %
	Technický dispečink	6,67 %	
Sektor č. 4 (výroba PHM)	Rafinérie		28,33 %

Za nejrizikovější z hlediska případného poškození byl v dotazníku 7 označen sektor č. 4. Nejméně rizikovými sektory se stal sektor č.3 (6 %), následován sektorem č. 1 (9 %).

Tabulka 27 – Dotazník 8 (vlastní)

DOTAZNÍK OHROŽENÍ KRITICKÉ INFRASTRUKTURY - ODVĚTVÍ ROPA A ROPNÉ PRODUKTY (ANALÝZA METODOU AKIS)									
(Autor: Daniel Ondra)									
Jméno: Autor 6					Firma: X				
	Sektor 1 - Převážná soustava			Sektor 2 - Distribuční soustava			Sektor 3 - Skladování ropy a PHM		Sektor 4 - Výroba PHM
	Tranzitní, vnitrostát. ropovod	Přečerpávací stanice	Technický dispečink	Produktovody	Přečerpávací stanice	Technický dispečink	Zásobníky	Technický dispečink	Rafinérie
Zranitelnost	15	25	20	25	25	20	50	40	50
Riziko ÚMYSLNÉHO poškození člověkem	5	10	10	10	20	20	5	10	20
Riziko poškození člověkem z NEDBALOSTI	5	10	10	20	20	20	5	10	45
Riziko poškození živelnými pohromami	10	10	10	30	30	30	10	5	30
Současná bezpečnostní opatření provozovatele	99	95	90	90	90	90	99	99	85
Pravděpodobnost zasažení velkého počtu lidí při selhání prvku ropné soustavy	60	40	40	40	40	50	60	55	70

Tabulka 28 – Zranitelnost dle dotazníku 8 (vlastní)

ZRANITELNOST DLE DOTAZNÍKU 8			
Sektor č. 1 (převážná soustava)	Tranzitní a vnitrostátní ropovod	15 %	20 %
	Přečerpávací stanice	25 %	
	Technický dispečink	20 %	
Sektor č. 2 (distribuční soustava)	Produktovody	25 %	23,33 %
	Přečerpávací stanice	25 %	
	Technický dispečink	20 %	
Sektor č. 3 (skladování plynu)	Zásobníky ropy	50 %	45 %
	Technický dispečink	40 %	
Sektor č. 4 (výroba PHM)	Rafinérie		50 %

Respondent vyhodnotil v dotazníku 8 za nejzranitelnější sektory č. 4 (50 %) a č. 3 (45 %). Za nejméně zranitelný byl označen sektor č. 1 s hodnotou zranitelnosti 20 %.

Tabulka 29 – Riziko poškození dle dotazníku 8 (vlastní)

RIZIKO POŠKOZENÍ DLE DOTAZNÍKU 8			
Sektor č. 1 (přepravní soustava)	Tranzitní a vnitrostátní ropovod	6,67 %	8,89 %
	Přečerpávací stanice	10 %	
	Technický dispečink	10 %	
Sektor č. 2 (distribuční soustava)	Produktovody	20 %	22,22 %
	Přečerpávací stanice	23,33 %	
	Technický dispečink	23,33 %	
Sektor č. 3 (skladování plynu)	Zásobníky ropy	6,67 %	7,5 %
	Technický dispečink	8,33 %	
Sektor č. 4 (výroba PHM)	Rafinérie		31,67 %

Z hlediska možného poškození byl v dotazníku 8 za nejrizikovější označen sektor č. 4. Naopak nejbezpečnějším sektorem z hlediska rizika poškození se stal sektor č. 3 s hodnotou rizika 7,5 %.

Tabulka 30 – Celková zranitelnost odvětví ropy a ropných produktů (vlastní)

CELKOVÁ ZRANITELNOST ODVĚTVÍ ROPY A ROPNÝCH PRODUKTŮ						
		Dotazník 5	Dotazník 6	Dotazník 7	Dotazník 8	Výsledek
Sektor č. 1	Tranzitní a vnitrostátní ropovod	8,33 %	3 %	20 %	20 %	12,83 %
	Přečerpávací stanice					
	Technický dispečink					
Sektor č. 2	Produktovody	6,67 %	3,67 %	26,67 %	23,33 %	15,09 %
	Přečerpávací stanice					
	Technický dispečink					
Sektor č. 3	Zásobníky ropy	7,5 %	3 %	35 %	45 %	22,62 %
	Technický dispečink					
Sektor č. 4	Rafinérie	20 %	15 %	40 %	50 %	31,25 %

Vyhodnotíme-li celkovou zranitelnost odvětví ropy a ropných produktů, je dle získaných výsledků nejzranitelnější sektor č. 4 se zranitelností 31,25 %. Druhým nejzranitelnějším sektorem je sektor č. 3 s hodnotou zranitelnosti 22,62 %. Nejbezpečnějším sektorem odvětví ropy a ropných produktů je z hlediska zranitelnosti sektor č. 1 (12,83 %).

Tabulka 31 – Celkové riziko poškození odvětví ropy a ropných produktů (vlastní)

CELKOVÉ RIZIKO POŠKOZENÍ ODVĚTVÍ ROPY A ROP. PRODUKTŮ						
		Dotazník 5	Dotazník 6	Dotazník 7	Dotazník 8	Výsledek
Sektor č. 1	Tranzitní a vnitrostátní ropovod	10,55 %	13,33 %	9 %	8,89 %	10,44 %
	Přečerpávací stanice					
	Technický dispečink					
Sektor č. 2	Produktovody	11,67 %	15 %	13,89 %	22,22 %	15,7 %
	Přečerpávací stanice					
	Technický dispečink					
Sektor č. 3	Zásobníky ropy	6,67 %	10 %	6 %	7,5 %	7,54 %
	Technický dispečink					
Sektor č. 4	Rafinérie	16,67 %	23,33 %	28,33 %	31,67 %	25 %

Sektor č. 4 je kromě největší zranitelnosti také sektorem s největším rizikem poškození (25 %). Druhý nejrizikovější sektor č. 2 je již od sektoru č. 4 svou hodnotou výsledného rizika značně vzdálen (15,7 %). Jednoznačně nejméně rizikovým sektorem je z hlediska možného poškození sektor č. 3 s rizikem 7,54 %.

Nejvyšší hodnoty zranitelnosti a také rizika poškození u sektoru č. 4 (rafinérie) mohou být způsobeny samotnou strukturou těchto petrochemických provozů. Jedná se o rozlehlé areály s mnoha složitými technologiemi, ve kterých se pohybuje značné množství zaměstnanců. Z těchto důvodů nelze některé hrozby a rizika zcela eliminovat.

6 DISKUZE

Pokoušíme-li se o jakoukoliv bezpečnostní analýzu objektu, systému či infrastruktury, je zásadní podmínkou znalost jeho současného bezpečnostního stavu. Takovéto informace nám, společně s dostatečnou znalostí zkoumané oblasti, umožní z hlediska bezpečnosti zmapovat vnitřní prostředí hodnoceného objektu (mnohdy ovlivnitelného samotnou činností objektu), stejně jako prostředí vnější, které ho obklopuje (prostředí neovlivnitelné). Zkoumání současného bezpečnostního stavu by mělo vést k odhalení míst, která jsou slabinami z pohledu bezpečnosti. Využití jakékoliv bezpečnostní analýzy má smysl tehdy, jestliže dojde v návaznosti na získané informace k vytvoření odpovídajících opatření.

Česká republika je svrchovaným, samostatným státem, založeným na demokratických principech a hodnotách. Je součástí mezinárodních společenství OSN a NATO, které jsou svým způsobem jistou zárukou naší bezpečnosti z hlediska vnějšího napadení. S ohledem na bezpečnostní situaci ČR je také nutné zmínit fakt, že je Česká republika dlouhodobě hodnocena jako jedna z nejbezpečnějších zemí na světě a v každoročně zveřejňovaném žebříčku se pravidelně umísťuje okolo 6. místa. Na tomto ocenění má bezpochyby svůj velký podíl dobře fungující bezpečnostní systém České republiky. Takováto příznivá bezpečnostní situace se, společně s proaktivním přístupem ČR, nepochybně projevuje také v oblasti bezpečnosti kritické infrastruktury. Na území ČR neoperují žádné militantní či separatistická hnutí nebo ozbrojené skupiny.

Přes všechny tyto pozitivní informace nelze některá rizika brát na lehkou váhu. Jako příklad lze zmínit hrozbu teroristického útoku. Terorismus si totiž ve 21. století našel novou, účinnou strategii – udeřit bez varování tam, kde to nikdo nečeká. Útočící jedinci nebo malé skupiny teroristů, mnohdy

ozbrojené běžně dostupnými věcmi (nože, mačety, automobily), mají za cíl zabít či zranit co největší množství osob. Z těchto důvodů nebude možné hrozbu teroristického útoku zcela eliminovat. Podíváme-li se zpět do historie, nelze opomenout další hrozby jakými jsou přírodní katastrofy a technologické havárie, schopné poškodit či dokonce zcela zničit důležité prvky kritické infrastruktury ČR v oblasti zemního plynu nebo ropy a ropných produktů.

Plynárenská soustava ČR byla vybudována za vysokých technologických standardů. Je pravidelně udržována a provozována za nejpřísnějších bezpečnostních a provozních podmínek. Tyto národní standardy jsou mnohdy přísnější než ty, které požaduje po svých členských zemích Evropská unie. Provozovatelem kompletní přepravní soustavy na území ČR je jediná společnost, což je z pohledu bezpečnosti a krizového řízení zcela jistě výhodou. K zajištění potřebných nezbytných dodávek zemního plynu České republice slouží jeho uskladněné zásoby. Skladovací lokality se stále rozšiřují a v posledních několika letech se množství skladovaného zemního plynu pohybuje v rozmezí 35 až 40 procent roční spotřeby.

Rozsah poškození plynárenské soustavy a následných omezení dodávek plynu by byl značně závislý na místě, kde by k poškození došlo. Za nejcitlivější místo můžeme jistě označit přepravní soustavu zemního plynu, to z důvodu velké závislosti České republiky na dováženém zemním plynu. Jistým druhem ochrany před tímto rizikem je rozmanitost zdrojů zemního plynu (včetně jeho dodavatelských cest), skýtající šanci alespoň částečně nahradit výpadek dodávky zemního plynu odjinud. Česká republika v současnosti odebírá cca 2/3 spotřebovaného zemního plynu z Ruské federace, zbytek tvoří ostatní zdroje. Současná síť plynovodů v Evropě je tak rozvinutá a propojená, že je možné otočit směr běžné přepravy zemního plynu a tím nahradit výpadek ochromené části plynovodné sítě.

Plynovody jsou na většině své trasy napříč ČR bezpečně uloženy v dostatečné hloubce pod povrchem země. Pouze na místech, kde překonávají jisté geografické překážky (např. říční toky) či procházejí průmyslovými areály, jsou plynovody vedeny po zemském povrchu. Takováto místa jsou právě lokalitou, kde by mohlo dojít k ohrožení či poškození plynovodu při povodních sesouvající se půdou nebo předměty unášenými rozvodněnými vodními toky.

Technologická havárie jsou další možnou příčinou výpadku dodávky zemního plynu. Riziko technologických havárií lze podstatně eliminovat propracovaným systémem kontrol, údržby nebo opravárenských činností. Takto striktně stanovené a dodržované technologické postupy, bezpečnostní předpisy jsou společně s revizemi, kontrolami a pravidelným školením nutností pro správně fungující kritickou infrastrukturu. Přepravní soustava plynu je v České republice takto pravidelně kontrolována a udržována. Do modernizace stávajících ropovodů byly investovány nemalé částky a díky těmto opatřením se daří riziko technologické havárie nebo poruchy držet na přijatelné úrovni.

Veškerá zmíněná rizika nejsou ve své podstatě pro fungování potřebných dodávek zemního plynu zcela kritická. Pokud nastane pouze jedno z nich, nemusí nutně dojít ani k omezení dodávek zemního plynu do ČR. Výskyt dvou nebo dokonce tří takovýchto událostí (výpadek dvou hraničních předávacích stanic, pokles těžby dodávaného plynu společně s poruchou na zásobnících) je vysoce nepravděpodobný.

Za silné stránky oblasti zemního plynu můžeme označit:

- kvalitně vybudovanou a precizně udržovanou přepravní soustavu;
- jediného provozovatele přepravní soustavy;
- relativně větší počet zdrojů zemního plynu;

- možnost zpětného toku plynu v soustavě;
- vysokou kapacitu zásobníků zemního plynu.

Za slabé stránky oblasti zemního plynu můžeme považovat:

- relativně vysokou závislost na plynu z Ruské federace;
- nedostatek vlastních zdrojů zemního plynu;
- komerční provoz zásobníků plynu (nákup plynu za účelem zisku);
- nedostatečné propojení sever – jih (Polsko – ČR – Rakousko).

Ropa je bezpochyby klíčovou energetickou surovinou ČR. Převážnou část ropy však musíme dovážet, zdroje nacházející se na území České republiky pokrývají celkovou spotřebu pouze v řádu jednotek procent. Tento fakt je již sám o sobě jistým rizikem, následkem zhoršení obchodně-politické situace v zemích, kudy ropovody vedou, by mohlo dojít k zásadnímu dlouhodobému omezení těžby nebo dodávek ropy. Česká republika má zajištěny dodávky ropy pomocí ropovodů Družba (Přátelství) a IKL. Podíl ruské ropy, importované ropovodem Družba, rok od roku klesá a v roce 2015 tvořil cca 56 % veškeré dovezené ropy (v roce 2009 to bylo 70 % a roku 2013 zhruba 64 %). Produkce důležitých ropných produktů (zejména pohonných hmot) je tedy v ČR zcela závislá na těchto dodávkách. Krátkodobé výpadky dodávek ropy dokáže ČR pokrýt ze svým vlastních zásob, ty v současnosti dokáží zabezpečit potřebnou ropu zhruba na 90 dní průměrné denní spotřeby. Jediným provozovatelem ropovodné sítě na území ČR a Centrálního tankoviště ropy Nelahozeves je státem vlastněná společnost MERO ČR, a.s.

Rafinérie v Záluží u Litvínova je schopna zpracovávat ropu z ropovodu Družba, která je svým složením bohatější na síru, zatímco méně sirnatou ropu z ropovodu IKL, pocházející z Ázerbájdžánu nebo Kazachstánu, dokáže využít rafinérie v Kralupech nad Vltavou. Tento fakt je důležitý proto,

že každá z rafinérií na území ČR, dokáže zpracovávat pouze jistý druh ropy. V případě dlouhodobého výpadku dodávek daného druhu ropy, by tato okolnost znamenala podstatný problém pro dotčenou rafinérii. Výpadek by musel být nahrazen zásobami jednotlivých rafinérií, petrochemických výrobců a distributorů pohonných hmot. V případě kritického nedostatku ropy nebo pohonných hmot, má vláda ČR možnost vyhlásit stav ropné nouze. Při takovémto stavu je oprávněna zavést opatření směřující k omezení spotřeby ropy a ropných produktů.

Výše zmínění teroristé v současnosti vyhledávají takzvané „měkké cíle“. Terčem jejich násilných činů se mnohdy stávají civilisté nebo právě kritická infrastruktura. U ropy a ropných produktů je nutné zmínit další riziko spojené s člověkem, a to majetkovou trestnou činností. Pokusy o zcizení ropy přímo z ropovodu, jsou v současnosti téměř nemožné. Moderní technologie, využívané při provozu ropovodů na našem území, jsou schopny detekovat odchylku znamenající možný únik ropy nebo krádež již do dvou minut. Reálné riziko zcizení ropy (nebo spíše z ní vyrobených produktů) nastává až při následné manipulaci, jejich stáčení nebo transportu. Transport a skladování strategických zásob ropných produktů (pohonných hmot) státu zajišťuje společnost Čepro a.s. svými produktovody a sítí skladů. Riziko krádeže je možné podstatně snížit odpovídajícími (v práci uvedenými) bezpečnostními opatřeními, jako jsou systémy technického zabezpečení, fyzická ostraha nebo režimová opatření. V případě dlouhodobých výpadků dodávek ropy, následného vyhlášení stavu ropné nouze a omezení distribuce pohonných hmot pro obyvatele, by nemalým bezpečnostním rizikem mohla být síť produktovodů firmy Čepro a.s., zajišťující právě přepravu nedostatkových pohonných hmot.

Za silné stránky oblasti ropy a ropných produktů můžeme označit:

- široké spektrum dodavatelů ropy a jejich přepravních cest;
- dostatečné nouzové zásoby ropy a ropných produktů;
- odpovídající legislativní rámec ropné bezpečnosti;
- zapojení ČR do mezinárodního systému ropné bezpečnosti (IEA, EU);
- hustou vnitrostátní sítí produktovodů;
- nouzové zásoby ropy a ropných produktů pod dohledem státu.

Za slabé stránky jsou oblasti ropy a ropných produktů můžeme považovat:

- nedostatek vlastních zdrojů ropy;
- omezený vliv státu na soukromé rafinérie a na jejich budoucnost.

Kritická infrastruktura oblasti zemního plynu má s oblastí ropy a ropných produktů mnoho společného. Obě zajišťují strategicky významnou surovinu, na kterých jsou v současnosti životně závislé mnohá odvětví průmyslu. Celková roční spotřeba zemního plynu, stejně jako ropy, každým rokem stoupá, ale Česká republika přitom nemá dostatečné vlastní zdroje. Tento handicap se snaží ČR vyrovnat dostatečným množstvím nouzových zásob a svým aktivním zapojením v rámci EU, při řešení otázek těchto klíčových komodit. Tato opatření jsou schopna zabezpečit náhradní dodávky surovin při krátkodobých jejich výpadech. Zmíněný aktivní politicky – obchodní přístup ČR k otázce rozvoje plynovodní a ropovodní sítě v Evropě, by mohl do budoucna zajistit větší diverzifikaci dodavatelů a přepravních tras ropy a zemního plynu.

Z důvodů uvedených v této práci by se mohlo zdát, že vlastnit kritickou infrastrukturu odvětví zemního plynu a ropy a ropných produktů, by mělo být pro stát jasnou prioritou. Realita je však poněkud jiná.

Stát je vlastníkem společností MERO ČR a.s. a Čepro a.s., nepatří mu však žádná ze dvou zmíněných rafinérií na území České republiky (ty jsou dnes ve vlastnictví polské skupiny PKN ORLEN). Stát tedy není schopen garantovat, zda a jak dlouho budou rafinérie funkční, zda se majitel rozhodne investovat do jejich modernizace apod. Tato skutečnost může být do budoucna pro Českou republiku problémem.

Živelných pohrom se s největší pravděpodobností v současnosti nemusíme zvlášť obávat. V posledních letech je nejaktuálnějším problémem dlouhodobé sucho. Větrné smrště způsobují zpravidla spíše škody na budovách a elektrické přenosové soustavě. Zmiňovali jsme možnost poškození přepravních soustav povodněmi. Ty jsou za současného stavu, dlouhodobého období sucha, spíše nepravděpodobné. Pravděpodobnější je jejich výskyt na malém území (lokální povodeň). Takováto blesková povodeň by ovšem nedokázala poškodit kritickou infrastrukturu zemního plynu nebo ropy a ropných produktů natolik, že by došlo k rozsáhlému výpadku infrastruktury.

Ochrana kritické infrastruktury se jistě bude dále vyvíjet a zdokonalovat. Příkladem mohou být rozvíjející se nové moderní technologie, dokonalejší IT systémy. Ty zcela jistě dostanou šanci podílet se svým dílem na ochraně kritické infrastruktury a tím jí posunout na novou, bezpečnější úroveň.

7 ZÁVĚR

Tato práce přinesla shrnutí problematiky ochrany kritické infrastruktury České republiky se zaměřením na odvětví zemního plynu, ropy a ropných produktů. Teoretická část čtenáři přiblížila historický vývoj problematiky ochrany KI, nabídla vysvětlení proč, případně před čím je nutné kritickou infrastrukturu chránit. V této práci byl vysvětlen legislativní proces určení prvku kritické infrastruktury a dále také to, že problematika ochrany kritické infrastruktury není pouze problémem České republiky, ale má mezinárodní přesah.

Cílem práce bylo provedení analýzy zmíněných odvětví metodou AKIS. Tato analýza byla vypracována a dostatečně popsána. Dalším cílem této bakalářské práce bylo čtenáři vysvětlit skutečnost, že ochrana kritické infrastruktury je složitým procesem, který vyžaduje spolupráci velkého množství zainteresovaných subjektů.

8 SEZNAM POUŽITÝCH ZKRATEK

BRS	Bezpečnostní rada státu
CTR Nelahozeves	Centrální tankoviště ropy Nelahozeves
ČNB	Česká národní banka
ČR	Česká republika
EKI	Evropská kritická infrastruktura
EPCIP	Evropský program na ochranu kritické infrastruktury
EU	Evropská unie
IEA	International Energy Agency – Mezinárodní energetická agentura
HZS ČR	Hasičský záchranný sbor České republiky
KI	Kritická infrastruktura
LNG	Liquefied Natural Gas – Zkapalněný zemní plyn
LPG	Liquefied Petroleum Gas – Propan – butan
MND	Moravské naftové doly, a.s.
MV	Ministerstvo Vnitra ČR
NKI	Národní kritická infrastruktura
PZP	Podzemní zásobník plynu
USA	Spojené státy americké
Výbor CNP	Výbor pro civilní a nouzové plánování
Y2K problém	IT problém roku 2000

9 SEZNAM POUŽITÉ LITERATURY

1. KOLEKTIV AUTORŮ POD VEDENÍM MINISTERSTVA ZAHRANIČNÍCH VĚCÍ ČR. *Bezpečnostní strategie České republiky*. Praha: Ministerstvo zahraničních věcí České republiky, 2015. ISBN 978-80-7441-005-5.
2. SVOBODA, Zdeněk. *Kritická infrastruktura a její ochrana* [online]. Ostrava, 2010 [cit. 2020-07-10]. Dostupné z: <http://hdl.handle.net/10084/79174>. Diplomová práce. Vysoká škola báňská – Technická univerzita Ostrava.
3. BREHOVSKÁ, Lenka. *Možné důsledky teroristického ohrožení na elektrizační soustavu České republiky*. Zlín, 2009. Dostupné také z: <https://theses.cz/id/a3tkw5/>. Diplomová práce. Univerzita Tomáše Bati ve Zlíně, Fakulta technologická. Vedoucí práce doc. Ing. Josef Janošec, CSc.
4. ŠENOVSKÝ, M., V. ADAMEC a P. ŠENOVSKÝ. *Ochrana kritické infrastruktury*. Ostrava: Edice SPBI Spektrum, 2007. ISBN 978-80-7385-025-8.
5. *Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon)*. In: *Zákony pro lidi.cz* [online]. © AION CS 2010-2020 [cit. 2020-07-16]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2000-240>
6. *Úplné znění (ÚZ) č. 1300 - Krizové zákony, HZS, Požární ochrana, Obnova území*. Ostrava: Sagit, 2019. ÚZ. ISBN 978-80-7488-333-0.
7. MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. *Ochrana kritické infrastruktury – Terorismus a měkké cíle* [online]. Praha, 2020 [cit. 2020-07-10]. Dostupné z: <https://www.mvcr.cz/cthh/clanek/ochrana-kriticke-infrastruktury-ochrana-kriticke-infrastruktury.aspx>
8. VLÁDA ČR. *Usnesení vlády č. 165 ze dne 25. 2. 2008 k vyhodnocení stavu realizace Konceptu ochrany obyvatelstva do roku 2006 s výhledem do roku 2015 a o Konceptu ochrany obyvatelstva do roku 2013 s výhledem do roku 2020*. Praha, 2008.

9. SVOBODA, Zdeněk. *Kritická infrastruktura a její ochrana*. Ostrava. 2010 [cit. 2020-07-13]. Dostupné z: < <https://theses.cz/id/3rpun1/>>. Diplomová práce. Vysoká škola báňská – Technická universita Ostrava, Fakulta bezpečnostního inženýrství. Vedoucí práce Danuše Kratochvílová.
10. LOEB, Zachary. *The lessons of Y2K, 20 years later*. [online]. Washington, 2019 [cit. 2020-07-13]. Dostupné z: <https://www.washingtonpost.com/outlook/2019/12/30/lessons-yk-years-later/>
11. KOŇAŘÍK, Jiří. *Komparace přístupů k ochraně kritické infrastruktury v České republice a Velké Británii*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2012, 72 s. Dostupné také z: <http://hdl.handle.net/10563/19367>. Diplomová práce. Univerzita Tomáše Bati ve Zlíně. Fakulta aplikované informatiky, Ústav elektroniky a měření. Vedoucí práce Hromada, Martin.
12. ŘÍHA, Josef. *Kritická infrastruktura a riziko mimořádné události* [online]. 10. 2007 [cit. 2020-07-13]. Dostupné z: https://www.uur.cz/images/5-publikacni-cinnost-a-knihovna/casopis/2007/2007-04/08_kriticka.pdf
13. BROWN, Kathi Ann. *Critical Path: A Brief History of Critical Infrastructure Protection in The United States*. Virginia, USA: Spectrum Publishing Group, 2006. ISBN 978-0-913969-06-9. Dostupné také z: https://cip.gmu.edu/wp-content/uploads/2016/06/CIPHS_CriticalPath.pdf
14. KOVAŘÍK, Jaroslav. *Kritická infrastruktura a ochrana obyvatelstva*. In: Sborník přednášek konference Ochrana obyvatel – Ochrana kritické infrastruktury. Ostrava: 2007. Sdružení požárního a bezpečnostního inženýrství. s. 145-153. ISBN 80-86634-51-5.
15. GAVENDOVÁ, Hana. *Komparace ochrany kritické infrastruktury v České republice a Evropské unii*. Brno, Duben 2009. Dostupné z: http://is.muni.cz/th/50593/esf_m/Gavendova_Diplomova_prace.pdf. Diplomová práce. Masarykova univerzita. Vedoucí práce Ing. Eduard BAKOŠ.

16. GENERÁLNÍ ŘEDITELSTVÍ HASIČSKÉHO ZÁCHRANNÉHO SBORU ČR. *Hasičský záchranný sbor České republiky – Postavení a úkoly*. [online]. Praha, 2020 [cit. 2020-07-13]. Dostupné z: <https://www.hzscr.cz/clanek/postaveni-a-ukoly-postaveni-a-ukoly.aspx>
17. Zákon č. 320/2015 Sb., o Hasičském záchranném sboru České republiky a o změně některých zákonů (zákon o hasičském záchranném sboru). In: <i>Zákony pro lidi.cz</i> [online]. © AION CS 2010-2020 [cit. 2020-07-16]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2015-320>
18. MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. *Ministerstvo Vnitra ČR – Ochrana kritické infrastruktury* [online]. Praha, 2020 [cit. 2020-07-13]. Dostupné z: <https://www.mvcr.cz/cthh/clanek/ochrana-kriticke-infrastruktury-ochrana-kriticke-infrastruktury.aspx>
19. KOTÍK, David. *Ochrana kritické infrastruktury Evropské unie* [online]. Zlín, 2008 [cit. 2020-07-13]. Dostupné z: <https://theses.cz/id/n87bfl/>. Diplomová práce. Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky. Vedoucí práce doc. Ing. Luděk Lukáš, CSc..
20. BEZPEČNOSTNÍ RADA STÁTU. *Příloha usnesení č. 30/2007*. Praha, 2007. Dostupné také z: <https://www.vlada.cz/assets/ppov/brs/cinnost/zaznamy-z-jednani/usn-30-07-priloha.pdf>
21. VLÁDA ČR. *Usnesení vlády č. 140 ze dne 22. 2. 2010 ke Komplexní strategii České republiky k řešení problematiky kritické infrastruktury a k Národnímu programu ochrany kritické infrastruktury* [online]. Praha, 2010. Dostupné z: https://www.dataplan.info/img_upload/7bdb1584e3b8a53d337518d988763f8d/komplexni-strategie-a-narodni-program.pdf
22. NOVOTNÝ, Petr. *Určování regionálních subjektů a proků kritické infrastruktury* [online]. Ostrava, 2017 [cit. 2020-07-13]. Dostupné z: <http://hdl.handle.net/10084/120157>. Disertační práce. Vysoká škola báňská – Technická univerzita Ostrava.

23. EVROPSKÁ KOMISE. *Sdělení Komise Radě a Evropskému parlamentu – Ochrana kritické infrastruktury při boji proti terorismu* KOM/2004/0702 [online]. Brusel, 2004. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:52004DC0702>
24. EVROPSKÁ KOMISE. *Zelená kniha o evropském programu na ochranu kritické infrastruktury: KOM(2005) 576 v konečném znění* [online]. Brusel, 2005. Dostupné z: <https://eur-lex.europa.eu/legalcontent/CS/TXT/?uri=celex%3A52005DC0576>
25. EVROPSKÁ KOMISE. *Evropský program na ochranu kritické infrastruktury* KOM(2006) 786 [online]. Brusel, 2006 [cit. 2020-03-18]. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex:52006DC0786>
26. EVROPSKÁ RADA. *Směrnice Rady č. 2008/114/ES ze dne 8. 12. 2008 o určování a označování evropských kritických infrastruktur a posouzení potřeby zvýšit jejich ochranu* [online]. Brusel, 2008 [cit. 2020-07-13]. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32008L0114&from=CS>
27. MARTÍNEK, Bohumír. *Východiska a principy zajištění ochrany kritické infrastruktury v České republice*. Časopis 112 [online]. Praha: MV-generální ředitelství HZS ČR, 4/2008, 14. dubna 2008, VII, str. 22 – 24 [cit. 2020-07-16]. ISSN 1213-7057. Dostupné z: <https://www.hzscr.cz/clanek/archiv-2004-az-2008-503464.aspx>
28. *Zákon č. 239/2000 Sb., o integrovaném záchranném systému a o změně některých zákonů*. In: *Zákony pro lidi.cz* [online]. © AION CS 2010-2020 [cit. 2020-07-16]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2000-239>
29. GENERÁLNÍ ŘEDITELSTVÍ HZS ČR. *Kritická infrastruktura – návrh tezí Komplexní strategie ČR k řešení problematiky kritické infrastruktury ČR*. Praha: MV – Generální ředitelství HZS ČR, 2007. PO-762-90/CNP-2007.
30. *Ochrana kritické infrastruktury*. Praha: Česká asociace bezpečnostních manažerů, 2011. ISBN 978-80-260-1215-3.

31. *Nařízení vlády č. 432/2010 Sb., o kritériích pro určení proku kritické infrastruktury*. In: <i>Zákony pro lidi.cz</i> [online]. © AION CS 2010-2020 [cit. 2020-07-16]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2010-432>
32. MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. *Komplexní strategie ČR k řešení problematiky kritické infrastruktury* [online]. Praha: Generální ředitelství HZS ČR, 2010. Dostupné také z: <https://www.databaze-strategie.cz/cz/mv/strategie/komplexni-strategie-cr-k-reseni-problematiky-kriticke-infrastruktury-2010?typ=download>
33. GENERÁLNÍ ŘEDITELSTVÍ HASIČSKÉHO ZÁCHRANNÉHO SBORU ČR. *Hasičský záchranný sbor České republiky – Postavení a úkoly*. [online]. Praha, 2020 [cit. 2020-07-13]. Dostupné z: <https://www.hzscr.cz/clanek/postaveni-a-ukoly-postaveni-a-ukoly.aspx>
34. BUDÍN, Jan. *Zemní plyn – těžba, vlastnosti a rozdělení*. OENERGETICE.CZ [online]. OM Solutions s.r.o, 12. duben 2015 [cit. 2020-07-17]. Dostupné z: <https://oenergetice.cz/plyn/zemni-plyn-tezba-vlastnosti-a-rozdeleni>
35. *Odkud k nám proudí fosilní paliva: Znáte ropovody a plynovody v ČR?* EP Energy Trading s.r.o. [online]. 17. 6. 2019 [cit. 2020-07-17]. Dostupné z: <https://www.epet.cz/odkud-k-nam-proudi-fosilni-paliva-znate-ropovody-a-plynovody-v-cr/>
36. *Zemní plyn*. Wikipedie.cz [online]. 2020 [cit. 2020-07-17]. Dostupné z: https://cs.wikipedia.org/wiki/Zemní_plyn
37. KOLEKTIV AUTORŮ MV – GŘ HZS ČR. *Plynárenská zařízení: Taktika zásahu při mimořádných událostech spojených s rizikem úniku zemního plynu*. In: <i>Konspekty odborné přípravy jednotek požární ochrany</i> Praha: MV – Generální ředitelství HZS ČR, 2019.
38. *Distribuce zemního plynu – 2. část: Distribuční soustava zemního plynu*. E.ON Distribuce [online]. 2020 [cit. 2020-07-19]. Dostupné z: <https://www.eon-distribuce.cz/clanek/distribuce-zemniho-plynu-2-cast>

39. *Distribuce zemního plynu – 1. část: Zemní plyn od těžby po dálkovou přepravu.* E.ON Distribuce [online]. 2020 [cit. 2020-07-19]. Dostupné z: <https://www.eon-distribuce.cz/clanek/distribuce-zemniho-plynu-1-cast>
40. *Ropovodná síť v ČR.* ROPA.cz [online]. 2013 [cit. 2020-07-19]. Dostupné z: <https://www.ropa.cz/ropovodna-sit-v-cr/>
41. *Svět ropy.* Petroleum.cz [online]. 2010 [cit. 2020-07-19]. Dostupné z: <http://www.petroleum.cz/svet-ropy.aspx>
42. *Ropovod Družba 50 let v provozu.* MERO ČR, a.s. [online]. 2015 [cit. 2020-07-19]. Dostupné z: <https://www.mero.cz/druzba/>
43. *Ropovod IKL 20 let v provozu.* MERO ČR, a.s. [online]. 2016 [cit. 2020-07-19]. Dostupné z: <https://www.mero.cz/ikl/>
44. *MERO Česká republika.* MERO ČR, a.s. [online]. 2020 [cit. 2020-07-19]. Dostupné z: <https://mero.cz>
45. *ČEPRO, a.s. Pomáháme státu: Ochránování zásob SSHR.* ČEPRO, a.s. [online]. 2019 [cit. 2020-07-19]. Dostupné z: <https://www.ceproas.cz/produkty-a-sluzby/ochranovani-zasob-sshr>
46. *ČEPRO, a.s. Spolehlivý zdroj – ČEPRO* [online]. ASTROPRINT, 2013 [cit. 2020-07-19]. Dostupné z: https://www.ceproas.cz/public/files/userfiles/O_nas/kniha_Cepro_20_historie.pdf
47. BUDÍN, Jan. *Zpracování ropy: 2. část – výroba pohonných hmot.* OENERGETICE.CZ [online]. 5. červen 2015 [cit. 2020-07-19]. Dostupné z: <https://oenergetice.cz/ropa/zpracovani-ropy-2-cast-vyroba-pohonnych-hmot>
48. *Unipetrol: Rafinérie.* UNIPETROL RPA [online]. [cit. 2020-07-19]. Dostupné z: <https://www.unipetrolrpa.cz/CS/o-nas/Rafinerie/Stranky/Rafinerie.aspx>
49. ZENKNER, Petr. *Kralupy, kde se zpracovává třetina ropy v Česku, čeká největší odstávka v historii. Unipetrol na ni vydá na 1,1 miliardy.* Hospodářské noviny [online]. 20. 3. 2018 [cit. 2020-07-19]. Dostupné z:

<https://archiv.ihned.cz/c1-66084810-kralupy-kde-se-zpracovava-tretina-ropy-v-cesku-ceka-nejvetsi-odstavka-v-historii-unipetrol-na-ni-vyda-na-1-1-miliardy>

50. VOSTAL, Jan. *Softwarová podpora metody hodnocení hierarchie stromu pro hodnocení zranitelnosti prvků kritické infrastruktury* [online]. Ostrava, 2017 [cit. 2020-07-19]. Dostupné z: <http://hdl.handle.net/10084/118575>. Diplomová práce. Vysoká škola báňská – Technická univerzita Ostrava.

10 SEZNAM POUŽITÝCH OBRÁZKŮ

Obrázek 1 Přepravní soustava České republiky	43
Obrázek 2 Podzemní zásobníky plynu (PZP) na území ČR	44
Obrázek 3 Význam ropy pro společnost	46
Obrázek 4 Síť ropovodů v Evropě	48
Obrázek 5 Ropovody na území České republiky	49
Obrázek 6 Centrální tankoviště ropy Nelahozeves.....	50
Obrázek 7 Síť skladů a produktovodů společnosti ČEPRO v ČR.....	52
Obrázek 8 Schéma zpracování ropy na pohonné hmoty	53

11 SEZNAM POUŽITÝCH TABULEK

Tabulka 1 Oblasti a služby kritické infrastruktury ČR	22
Tabulka 2 Odvětvová kritéria prvku KI pro odvětví zemní plyn, ropa a ropné produkty	39
Tabulka 3 Složení zemního plynu	41
Tabulka 4 Dotazník 1	60
Tabulka 5 Zranitelnost dle dotazníku 1	61
Tabulka 6 Riziko poškození dle dotazníku 1	61
Tabulka 7 Dotazník 2	62
Tabulka 8 Zranitelnost dle dotazníku 2	62
Tabulka 9 Riziko poškození dle dotazníku 2	63
Tabulka 10 Dotazník 3	64
Tabulka 11 Zranitelnost dle dotazníku 3	64
Tabulka 12 Riziko poškození dle dotazníku 3	65
Tabulka 13 Dotazník 4	66
Tabulka 14 Zranitelnost dle dotazníku 4	66
Tabulka 15 Riziko poškození dle dotazníku 4	67
Tabulka 16 Celková zranitelnost odvětví zemního plynu	67
Tabulka 17 Celkové riziko poškození odvětví zemního plynu	68
Tabulka 18 Dotazník 5	69
Tabulka 19 Zranitelnost dle dotazníku 5	70
Tabulka 20 Riziko poškození dle dotazníku 5	70
Tabulka 21 Dotazník 6	71
Tabulka 22 Zranitelnost dle dotazníku 6	71
Tabulka 23 Riziko poškození dle dotazníku 6	72
Tabulka 24 Dotazník 7	73
Tabulka 25 Zranitelnost dle dotazníku 7	73
Tabulka 26 Riziko poškození dle dotazníku 7	74

Tabulka 27 Dotazník 8	75
Tabulka 28 Zranitelnost dle dotazníku 8	75
Tabulka 29 Riziko poškození dle dotazníku 8	76
Tabulka 30 Celková zranitelnost odvětví ropy a ropných produktů	76
Tabulka 31 Celkové riziko poškození odvětví ropy a ropných produktů	77

12 SEZNAM PŘÍLOH

Příloha 1 Principy Evropského programu na ochranu kritické infrastruktury

Příloha 2 Dotazník pro odvětví zemního plynu

Příloha 3 Dotazník pro odvětví ropy a ropných produktů

Příloha 1 – Zásady Evropského programu na ochranu kritické infrastruktury

[25]

2.3. Zásady

Následující základní zásady budou vodítkem při provádění EPCIP:

- **Subsidiarita** – úsilí Komise v oblasti ochrany kritické infrastruktury se bude zaměřovat na infrastrukturu, která je kritická spíše z evropského než vnitrostátního či regionálního pohledu. Ačkoli se Komise zaměří na evropské kritické infrastruktury, může v případě potřeby a s přihlédnutím ke stávajícím pravomocem Společenství a dostupným zdrojům poskytnout podporu členským státům v souvislosti s vnitrostátními kritickými infrastrukturami.
- **Doplňkovost** – Komise se vyvaruje zdvojení stávajícího úsilí, na úrovni EU i vnitrostátní či regionální úrovni, pokud je toto úsilí při ochraně kritické infrastruktury prokazatelně efektivní. EPCIP bude tedy navazovat na existující odvětvová opatření a doplňovat je.
- **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.
- **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 kritické infrastruktury a také státní či další příslušné orgány.
- **Proporcionálnost** – 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.
- **Odvětvový přístup** – jelikož různá odvětví mají odlišné zkušenosti, odborné znalosti a požadavky týkající se ochrany kritické infrastruktury, bude EPCIP rozvíjen podle odvětví a prováděn podle dohodnutého seznamu odvětví ochrany kritické infrastruktury.

Příloha 2 – Dotazník pro odvětví zemního plynu

DOTAZNÍK OHROŽENÍ KRITICKÉ INFRASTRUKTURY – ODVĚTVÍ ZEMNÍ PLYN (ANALÝZA METODOU AKIS) (Autor: Daniel Ondra)								
Jméno:					Firma:			
	Sektor 1 – Přepravní soustava			Sektor 2 – Distribuční soustava			Sektor 3 – Skladování plynu	
	Tranzitní nebo vnitrostátní plynovody	Kompresorová stanice	Předávací stanice	VysokoTL. a středoTL. plynovody	Předávací a regulační stanice	Technický dispečink	Podzemní zásobník plynu	Technický dispečink
Zranitelnost								
Riziko ÚMYSLNÉHO poškození člověkem								
Riziko poškození člověkem z NEDBALOSTI								
Riziko poškození živelnými pohromami								
Současná bezpečnostní opatření provozovatele								
Pravděpodobnost zasažení velkého počtu lidí při selhání prvku plyn. soustavy								

Legenda:

Zranitelnost: Zranitelností je myšlen nedostatek, slabina či současný stav analyzovaného aktiva, díky kterému může hrozba realizovat svůj nežádoucí vliv na dané aktivum. Zranitelnost vyjadřuje citlivost aktiva na působení hrozby (hodnocení 0 až 100, kdy 0 znamená „nezranitelné aktivum“ a 100 „zcela snadno zranitelné“).

Riziko: Riziko poškození daného aktiva (0 až 100, kdy 0 znamená to, že „dané riziko neexistuje“).

Bezpečnostní opatření: Zhodnocení v současnosti zavedených bezpečnostních opatření provozovatelem (hodnocení 0 až 100, kdy 0 znamená „zcela nezabezpečen“ a 100 „maximální možné zabezpečení“).

Pravděpodobnost zasažení velkého počtu lidí při selhání: Hodnocení 0 až 100, kdy 0 znamená „není šance, že dojde k zasažení velkého počtu lidí“ a 100 „zcela jistě bude zasaženo velké množství lidí“.

Příloha 3 – Dotazník pro odvětví ropy a ropných produktů

DOTAZNÍK OHROŽENÍ KRITICKÉ INFRASTRUKTURY – ODVĚTVÍ ROPA A ROPNÉ PRODUKTY (ANALÝZA METODOU AKIS)									
(Autor: Daniel Ondra)									
Jméno:					Firma:				
	Sektor 1 – Převážná soustava			Sektor 2 – Distribuční soustava			Sektor 3 – Skladování ropy a PHM		Sektor 4 – Výroba PHM
	Tranzitní, vnitrostát. ropovod	Přečerpávací stanice	Technický dispečink	Produktovody	Přečerpávací stanice	Technický dispečink	Zásobníky	Technický dispečink	Rafinérie
Zranitelnost									
Riziko ÚMYSLNÉHO poškození člověkem									
Riziko poškození člověkem z NEDBALOSTI									
Riziko poškození živelnými pohromami									
Současná bezpečnostní opatření provozovatele									
Pravděpodobnost zasažení velkého počtu lidí při selhání prvku ropné soustavy									

Legenda:

Zranitelnost: Zranitelnost je myšlen nedostatek, slabina či současný stav analyzovaného aktiva, díky kterému může hrozba realizovat svůj nežádoucí vliv na dané aktivum. Zranitelnost vyjadřuje citlivost aktiva na působení hrozby (hodnocení 0 až 100, kdy 0 znamená „nezranitelné aktivum“ a 100 „zcela snadno zranitelné“).

Riziko: Riziko poškození daného aktiva (0 až 100, kdy 0 znamená to, že „dané riziko neexistuje“).

Bezpečnostní opatření: Zhodnocení v současnosti zavedených bezpečnostních opatření provozovatelem (hodnocení 0 až 100, kdy 0 znamená „zcela nezabezpečen“ a 100 „maximální možné zabezpečení“).

Pravděpodobnost zasažení velkého počtu lidí při selhání: Hodnocení 0 až 100, kdy 0 znamená „není šance, že dojde k zasažení velkého počtu lidí“ a 100 „zcela jistě bude zasaženo velké množství lidí“.