
**ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE**

**Fakulta biomedicínského inženýrství**

**Katedra zdravotnických oborů a ochrany obyvatelstva**


# Možnosti zvýšení zabezpečení kritické infrastruktury

# Possibilities of Increasing the Security of Critical Infrastructure

Diplomová práce

Studijní program: Ochrana obyvatelstva

Studijní obor: Civilní nouzové plánování

Vedoucí práce: Ing. Jiří Halaška, Ph.D.


**Bc. Vojtěch Poleno**



**Kladno, květen 2017**

České vysoké učení technické v Praze, Fakulta biomedicínského inženýrství

Katedra zdravotnických oborů a ochrany obyvatelstva | Akademický rok: 2016/2017

# Zadání diplomové práce

| | |
|---|---|
| Student: | **Bc. Vojtěch Poleno** |
| Studijní obor: | Civilní nouzové plánování |
| Téma: | **Možnosti zvýšení zabezpečení kritické infrastruktury** |
| Téma anglicky: | Possibilities of Increasing the Security of Critical Infrastructure |

Zásady pro vypracování:

Předmětem diplomové práce je analyzovat bezpečnostní hrozby, které by mohly ohrozit funkčnost prvků kritické infrastruktury a navrhnout možnosti zvýšení zabezpečení prvků kritické infrastruktury v případě zvýšení rizika ohrožení kritické infrastruktury. V teoretické části diplomové práce budou nastíněny metody střežení a zabezpečení prvků kritické infrastruktury. V praktické části práce bude analyzována současná bezpečnostní situace a z ní vyplývající hrozby pro funkčnost kritické infrastruktury. Na základě SWOT analýzy a analýzy rizik budou navrženy technické a organizační prostředky a metody střežení modelového prvku kritické infrastruktury v období bez výskytu přímých hrozeb prvku kritické infrastruktury. Dále budou navrženy možnosti zvýšení zabezpečení prvku kritické infrastruktury v případě zvýšeného rizika ohrožení.

Seznam odborné literatury:

[1] PROCHÁZKOVÁ, Dana, Bezpečnost kritické infrastruktury, ed. 1., Praha: České vysoké učení technické v Praze, 2012, ISBN 978-80-01-05103-0
[2] ŠENOVSKÝ, Michail, ADAMEC, Vilém a ŠENOVSKÝ, Pavel, Ochrana kritické infrastruktury, ed. 1., Ostrava: Sdružení požárního a bezpečnostního inženýrství, 2007, ISBN 9788073850258
[3] PROCHÁZKOVÁ, Dana, Základy řízení bezpečnosti kritické infrastruktury, ed. 1., Praha: České vysoké učení technické v Praze, 2013, ISBN 8001052451
[4] ŠENOVSKÝ, Michail, Zranitelnost kritické infrastruktury, ed. 1., Ostrava: Sdružení požárního a bezpečnostního inženýrství, 2008, ISBN 978-80-7385-058-6

| | |
|---|---|
| Vedoucí: | Ing. Jiří Halaška, Ph.D. |
| Konzultant: | Ing. Jan Farny |

Zadání platné do: 20.08.2018

..... vedoucí katedry / pracoviště

..... děkan

V Kladně dne 12.12.2016

# Prohlášení

Prohlašuji, že jsem diplomovou práci s názvem **Možnosti zvýšení zabezpečení kritické infrastruktury** 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).

V Kladně dne 16. 5. 2017

…….……..……..

podpis

## Poděkování

Děkuji Ing. Jiřímu Halaškovi, Ph.D. za vedení, cenné připomínky a rady při zpracování této diplomové práce. Dále bych chtěl poděkovat Ing. Janu Farnemu za podnětné konzultace a rady při zpracování praktické části práce.

## Abstrakt

Předmětem diplomové práce je problematika zabezpečení kritické infrastruktury se zaměřením na fyzické narušení bezpečnosti.

V teoretické části diplomové práce je zpracován přístup k ochraně kritické infrastruktury na úrovni Evropské unie a jeho implementace v České republice. Dále je zde krátce pojednáno o problematice kybernetické bezpečnosti, kterou, přestože není předmětem diplomové práce, nelze opomíjet. V poslední části je vypracován přehled metod a prostředků zajištění objektové bezpečnosti a bezpečnosti areálu.

Obsahem praktické části je vytvoření komplexního systému zabezpečení typového prvku kritické infrastruktury. Na základě zabezpečení reálného prvku kritické infrastruktury jsou vytvořena bezpečnostní opatření pro běžnou situaci. S využitím SWOT analýzy systému zabezpečení a analýzy rizik zpracované v softwarovém nástroji RISKAN jsou navržena možná opatření ke zvýšení úrovně zabezpečení prvku kritické infrastruktury v případě zvýšeného rizika fyzického narušení bezpečnosti prvku kritické infrastruktury.

Prvky systému zabezpečení jsou zpracovány ve formě tabulek a je popsán způsob jejich nasazení. V diskusi je provedena komparace navrhovaného systému zabezpečení s komerčně nabízeným způsobem ochrany objektů a reakcí na zvýšené ohrožení aplikované v zahraničí. V závěru jsou shrnuty výsledky a cíle práce.



## Klíčová slova

Kritická infrastruktura, technické prostředky zabezpečení, objektová bezpečnost, střežení, mechanická ochrana

## Abstract

The subject of the diploma thesis is the issue of security of critical infrastructure with a focus on physical security breach.

The theoretical part of the diploma thesis deals with the approach to the protection of critical infrastructure at the level of the European Union and its implementation in the Czech Republic. There is also briefly discussed the issue of cyber security, which, although not a diploma thesis, can not be omitted. The last part provides an overview of the methods and means of an object security and a grounds security.

The practical part consists of the creation of a complex security system of a model critical infrastructure. Security measures for the normal situation are created on the basis of the security of a real critical infrastructure. Using the SWOT analysis of the security and the risk analysis developed in the RISKAN software tool, possible measures are proposed to increase the level of security of the critical infrastructure in the event of an increased threat of a physical breach to the critical infrastructure security.

The elements of the security system are processed in the form of tables and their deployment is described. In the discussion, a comparison of the proposed security system with a commercially offered way of protecting objects and response to increased threats applied abroad is carried out. In conclusion there are summarized the results and objectives of the work.



## Keywords

Critical infrastructure, technical means of security, object security, guarding, mechanical protection

# OBSAH

# 1 ÚVOD

Oblast ochrany kritické infrastruktury se dostala do popředí zájmu a byla podrobně rozpracována na počátku tohoto tisíciletí, ale ochrana strategicky důležitých objektů a později infrastruktury prochází prakticky celou historií lidstva, tj. historií válek. Přístup k ochraně kriticky důležité infrastruktury se měnil podle typů hrozeb a podle technologického rozvoje společnosti, v současnosti se, nejen v Evropě, k ochraně kritické infrastruktury volí komplexní přístup odrážející provázanost různých odvětví i států a to zejména k ochraně před nevojenskými hrozbami (Procházková, 2012).

Pojem „kritická infrastruktura“ je poměrně nový, ale zajištění ochrany životně důležitých objektů, oblastí a infrastruktury bylo důležitým cílem států či jiných uskupení od počátku jejich existence. Jako hrozba, proti které byla ochrana směřována, však byla výhradně vojenského charakteru, případně byly důležité objekty (např. sýpky, sklady aj.) chráněny proti vlastnímu obyvatelstvu, a to především z důvodu rabování. Ochrana však nebyla komplexněji plánována a organizována. (Macaulay, 2008)

Ochrana klíčových infrastruktur byla podrobněji rozpracována poprvé ve Spojených státech amerických, a to již v 18. století. Důvodem byla v té době vysoká míra industrializace a rizika spojená s kolonizací týkající se zejména výstavby a ochrany železnic. Naopak nutnost ochrany strategických objektů a infrastruktury v obou světových válkách byla ve Spojených státech rozpracována, ale ovšem nebylo nutné ji prakticky aplikovat, neboť americké území (s výjimkou ojedinělého „balónového“ bombardování Japonskem) nebylo válkou přímo zasaženo. (Brown, 2006)

V Evropě byla ochrana klíčových prvků infrastruktury součástí obranných strategií především od 19. století (Aradau, 2010). Po zkušenostech z první světové války se ochrana infrastruktury i obyvatelstva výrazně orientovala na protileteckou obranu. S narůstající hrozbou vypuknutí války s nacistickým Německem se v Československu prioritně vytvářela protiletecká ochrana vojenských objektů a klíčových továren a ochrana měst spočívala v zatemňování. (John, 1996)

Druhá polovina dvacátého století se nesla ve znamení studené války. Protože se předpokládalo, že případná válka mezi východním a západním blokem by byla jaderná, do popředí se dostala ochrana infrastruktury a obyvatelstva proti účinkům zbraní hromadného ničení. Mimo jaderný útok se připravovala obrana klíčových průmyslových podniků proti vojenskému napadení.

V Československu se ale od osmdesátých let na ochranu klíčové infrastruktury začalo přistupovat i s uvážením jiných rizik, než vojenského útoku. Bylo to dáno mj. snížením rizika vypuknutí jaderné války vlivem odzbrojovacích smluv mezi Spojenými státy a Sovětským svazem a narůstajícím počtem přírodních mimořádných událostí. (Šenovský M., Adamec a Šenovský P., 2007)

Po konci studené války otázka ochrany kritické infrastruktury na několik let ustoupila jiným problémům spojeným s koncem bipolárního rozdělení světa. Znovu se touto problematikou v Evropě začaly zabývat Německo a Velká Británie. V roce 1999 byl v Německu přijat dokument „Informačně technické ohrožení klíčových infrastruktur v Německu," ve kterém byla obecně specifikována kritická infrastruktura a její možná ohrožení. Ve stejném roce ve Velké Británii vzniklo Národní koordinační centrum pro bezpečnost infrastruktury, jehož úkolem bylo určit systému důležité pro funkci státu a jejichž vyřazení by ohrozilo obyvatelstvo a koordinovat činnosti k jejich ochraně. (Štětina, 2014)

Přelomová událost (nejen) pro ochranu kritické infrastruktury byl teroristický útok 11. září 2001. Po tomto datu se zajištění ochrany kritické infrastruktury stalo primárním cílem a úkolem státu. (Kovařík, 2007) Konkrétní kroky učiněné v rámci Evropské unie a České republiky jsou zpracovány v následujících kapitolách číslo 2 a 3.

Nejnovějším trendem v hrozbách pro kritickou infrastrukturu a s tím související nutností adekvátních opatření je hrozba kybernetického útoku. Většina prvků kritické infrastruktury využívá přístupu na internet a v takovém případě existuje riziko útoku z kyberprostoru prakticky z libovolného místa na světě. Náklady na zajištění kybernetické bezpečnosti každoročně narůstají a roste i počet a velikost hrozeb. Zároveň je nutné počítat s tím, že absolutní zabezpečení není reálně dosažitelné. (Martellini, 2013) Problém

představuje i určitá roztříštěnost prvků kritické infrastruktury ve smyslu různých vlastníků/provozovatelů a jiných technologií a zabezpečení, která používají. (Bruijne a Eeten, 2007) Hrozby pro kritickou infrastrukturu

Hrozby pro kritickou infrastrukturu mohou být přírodního charakteru nebo způsobené činností člověka. Mohou se též vyskytnout kombinované hrozby, tj. přírodní událost způsobená činností člověka (např. nevhodnými zásahy do rázu krajiny) nebo antropogenní události, které vznikly v důsledku přírodního jevu (např. rabování za povodní). Podle zdroje je hrozby možné rozlišit na vnitřní a vnější, přičemž za vnější hrozby se obvykle považuje hrozba vojenského konfliktu. (Šenovský M., Adamec a Šenovský P., 2007) Terorismus může mít charakter vnitřní i vnější hrozby, přičemž v současnosti se pracuje s pojmem „globální terorismus," který prostupuje celým světem bez ohledu na státní hranice.

V Komplexní strategie České republiky k řešení problematiky kritické infrastruktury jsou hrozby uvedeny obecně pouze odkazem na Bezpečnostní strategii České republiky z roku 2003. V návrhu tezí ke Komplexní strategii zpracovaným Ministerstvem vnitra – Generálním ředitelstvím HZS ČR je však definováno 13 konkrétních hrozeb: Technologické havárie, technické poruchy, výpadek dodávek energií, vody a surovin, selhání počítačových sítí, stávka, nedostatek pracovních sil, ukončení činnosti subjektu kritické infrastruktury, dočasná nebo dlouhodobá změna orientace subjektu kritické infrastruktury a narušení prvku kritické infrastruktury z důvodu přírodní nebo antropogenní události. (Ministerstvo vnitra – Generální ředitelství HZS ČR, 2007)

Aktuální Bezpečnostní strategie ČR z roku 2015 přímo jako jednu z hrozeb pro bezpečnost státu identifikuje „ohrožení funkčnosti kritické infrastruktury." Z důvodu celkové propojenosti kritické infrastruktury se jedná o komplexní přírodní, technické a asymetrické hrozby. Konkrétně jsou uvedena ohrožení energetické sítě: *„Politicky motivované manipulace s dodávkami strategických surovin, vstup cizího kapitálu s potenciálně rizikovým původem a cíli do kritické infrastruktury ČR, sabotáže, kybernetické útoky či hospodářská kriminalita"* (Kolektiv autorů pod vedením Ministerstva zahraničních věcí ČR, 2015, s. 12)

# 2 OCHRANA KRITICKÉ INFRASTRUKTURY NA ÚROVNI EVROPSKÉ UNIE

Pojem „kritická infrastruktura," a s tím související problematika vymezení kritické infrastruktury a její ochrana, byl do českého právního řádu zanesen v roce 2010 zákonem 430/2010 Sb., kterým došlo ke změně zákona 240/2001 Sb., o krizovém řízení a změně některých zákonů (krizový zákon), ve znění pozdějších předpisů.

V rámci Evropské unie se však pro oblast komplexní ochrany kritické infrastruktury začaly podnikat konkrétní kroky již v roce 2004. Evropská rady požádala Komisi o přípravu programu k ochraně kritické infrastruktury, konkrétně se jednalo Evropský program na ochranu kritické infrastruktury a Výstražnou informační síť kritické infrastruktury (CIWIN) Jednalo se především reakci na teroristické útoky 11. září 2001 a především pak na teroristické útoky v Madridě v březnu roku 2004.

## 2.1 Zelená kniha o Evropském programu na ochranu kritické infrastruktury

Vytvoření zelené knihy předcházely dva semináře uspořádané Komisí. První seminář se konal 6. a 7. června 2005. Účastnily se ho členské státy Evropské unie a po jeho konci členské státy poskytly Komisi dokumenty, ve kterých specifikovaly svůj přístup k ochraně kritické infrastruktury. Tyto dokumenty posloužily jako základ dalšího postupu při určování vývoje ochrany kritické infrastruktury. Druhý seminář se konal 13. září 2005 a kromě členských států EU se jej účastnily též průmyslová sdružení. Cílem bylo pokročit ve vytváření jednotného systému ochrany kritické infrastruktury. Výsledkem semináře pak bylo rozhodnutí Komise o předložení zelené knihy, ve které je popsán Evropský program na ochranu kritické infrastruktury (EPSIP - European Programme for Critical Infrastructure Protection) a možnosti, které nabízí. Zelená kniha byla Komisí přijata 17. listopadu 2005.

Hlavní cíl zelené knihy je zapojit co největší počet subjektů odpovědných za ochranu jednotlivých prvků i celého systému kritické infrastruktury. Jedná se o vlastníky a provozovatele kritické infrastruktury, profesní a odvětvová sdružení, ale i všechny úrovně veřejné správy a veřejnost. Na základě zpětné vazby od výše uvedených subjektů lze získat bezpečnostní politiky vhodné k ochraně kritické infrastruktury.

V zelené knize jsou dále předloženy možnosti, které mohou být využity Komisí pro zřízení Evropského programu na ochranu kritické infrastruktury a Výstražné informační sítě kritické infrastruktury. Důvodem předložení možností ochrany kritické infrastruktury je mj. získat konkrétní odezvu na jednotlivé metody a získané poznatky využít při spuštění EPCIP. (Komise evropských společenství, 2005)

## 2.2 Evropský program na ochranu kritické infrastruktury

Po výše uvedeném postupu přípravy a tvorby byl Evropský program na ochranu kritické infrastruktury schválen 12. prosince 2006. Přestože byl vytvořen jako reakce na teroristické útoky, jeho cílem je zajištění bezpečnosti kritické infrastruktury proti všem reálným hrozbám, ale důraz je kladen na ochranu kritické infrastruktury proti teroristickým útokům.

Základním cílem EPCIP je zajištění existence přiměřené úrovně ochrany kritické infrastruktury, která je rovnoměrná napříč všemi státy Evropské unie. Současně je cílem vytvoření minima prostoru pro jakékoliv selhání soustavy či prvku kritické infrastruktury a poskytnutí okamžitých, předem ověřených opatření k řešení vzniklého problému.

Při ochraně kritické infrastruktury se nepočítá s jednotnou úrovní zabezpečení všech prvků kritické infrastruktury. Při určení úrovně zabezpečení se uvažuje s možnými dopady selhání konkrétního prvku kritické infrastruktury a nutnými náklady zajištění bezpečnosti. Principem přiměřené ochrany je nalézt optimum mezi náklady na vytvoření a udržování určité úrovně bezpečnosti a možnými negativními následky v případě narušení funkce prvku kritické infrastruktury.

Evropský program na ochranu kritické infrastruktury vychází z pěti základních principů, které jsou subsidiarita, doplňkovost, důvěrnost, spolupráce zainteresovaných subjektů, proporcionalita a odvětvový přístup. Princip subsidiarity spočívá v přenesení odpovědnosti z unijních orgánů na nižší úroveň. Odpovědnost za zajištění ochrany kritické infrastruktury spadá především na subjekty na národní úrovni. Činnost Komise se zaměřuje především na problematiku ochrany kritické infrastruktury s příhraničním dosahem, přičemž odpovědnost za ochranu vlastního majetku zůstává na vlastnících a provozovatelích prvků kritické infrastruktury. (Komise evropských společenství, 2006)

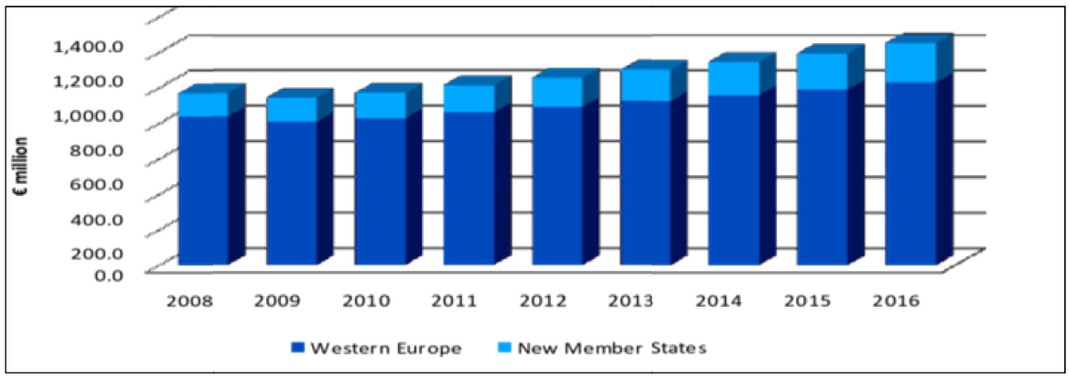
Terorismus, přírodní katastrofy a další ohrožení kritické infrastruktury nejsou vázány státními hranicemi, proto na aspekty ochrany a zabezpečení nelze nahlížet pouze na vnitrostátní úrovni. Z důvodu propojení hospodářství států Evropské unie může mít narušení kritické infrastruktury na území jednoho státu dopad na celkovou ekonomiku unie a následně i na partnery Evropské unie. Ochrana kritické infrastruktury tedy přispívá i k zabezpečení hospodářství a pomáhá posilovat konkurenceschopnost Evropské unie na světových trzích. Spolupráce při zajišťování kritické infrastruktury včetně sdílení informací probíhá i se státy sousedícími s Evropskou unií. V případě celosvětové kritické infrastruktury, jako jsou informační a komunikační technologie, se předpokládá globální spolupráce, především prohlubování spolupráce se zeměmi bývalé G8.

Při zavádění EPCIP byl stanoven akční plán, který určil cíle, kterých bylo třeba dosáhnout, včetně požadovaných termínů plnění cílů. Byly stanoveny tři oblasti činností – strategické aspekty EPCIP uplatnitelné ve všech oblastech ochrany KI, oblast evropské kritické infrastruktury a podpora členských států v rámci vnitrostátní kritické infrastruktury. Pro zajištění jednotného postupu při určování evropské kritické infrastruktury společného zvyšování jejího zabezpečení byla v roce 2008 vydána směrnice Rady 2008/114/EK o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu. Odpovědnost za zajištění ochrany kritické infrastruktury však mají členské státy, na jejichž území se kritická infrastruktura nachází. Vnitrostátní kritická infrastruktura se určuje podle kritérií, která si určí sám členský stát, ale mělo by se přihlédnout k následujícím kritériím narušení funkce kritické infrastruktury: rozsah zasaženého území, veřejný dopad, hospodářský dopad, politický dopad, psychologický dopad, dopad na veřejné zdraví a dopad na životní prostředí. Základním klíčovým prvkem zabezpečení ochrany kritické infrastruktury je krizové plánování, na kterém se podílí vlastníci/provozovatelé prvků kritické infrastruktury, státní orgány a využívá se i sdílení informací mezi členskými státy. (Komise Evropských společenství, 2006)

Pro sdílení informací byla primárně vytvořena Výstražná informační síť kritické infrastruktury (CIWIN), která umožňuje bezpečné sdílení informací týkajících se ochrany kritické infrastruktury napříč všemi členskými státy Evropské unie. Síť byla vytvořena návrhem rozhodnutí Rady KOM(2008) 676 v konečném znění 2008/0200 (CNS) o výstražné informační síti kritické infrastruktury (CIWIN). Z počátku bylo nejasné nastavení

financování sítě, což byl důvod, proč se Česká republika jako jediný členský stát EU do projektu na počátku nepřipojila. Protože se se sítí počítá jako s hlavním nástrojem sdílení informací, Česká republika se nakonec k projektu připojila v lednu 2013. (Hasičský záchranný sbor České republiky, 2017)

Přestože bezpečnost kritické infrastruktury je odpovědností jednotlivých členských států, na opatření je možné čerpat dotace z evropských fondů, při tvorbě Evropského programu na ochranu kritické infrastruktury se jednalo zejména o program „Prevence, připravenost k obraně proti terorismu a jiným bezpečnostním rizikům a zvládání jejich následků“ stanovený pro časové rozmezí 2007 – 2013. Program představoval příležitost pro získání finančních prostředků z evropských fondů pro financování opatření na ochranu kritické infrastruktury nejen na úrovni Evropské unie, ale též na národní úrovni. Financování se využilo zejména na tvorbu strategií, metodik, posouzení rizik a zranitelnosti a pro rozvoj nástrojů ochrany kritické infrastruktury. (Komise Evropských společenství, 2006)




*Graf 1 - Investice do ochrany kritické infrastruktury v EU; zdroj: Hawk ISM and SBC, 2014*

Na výše uvedeném grafu jsou znázorněny investice do zabezpečení kritické infrastruktury v členských státech Evropské unie. Na první pohled je zde zřejmý výrazný nepoměr mezi investicemi západoevropských států a třinácti nových členů EU. Je však nutné zohlednit též počet obyvatel nově přijatých států, který je přibližně 90 milionů, což je méně než pětina obyvatel Evropské unie. Se zohledněním počtu obyvatel jsou výdaje nových členských států a starých členských států na přibližně podobné úrovni. Souhrnné investice do zabezpečení kritické infrastruktury za celou EU dosáhly výše 1,2 miliardy eur.

## 2.3 Ochrana kritické infrastruktury v rámci boje proti terorismu

Jako reakce na teroristické útoky na vlaky v Madridu 11. března 2004 byl mj. vytvořen dokument „Ochrana kritické infrastruktury při boji proti terorismu“ ve formě Sdělení komise Radě a Evropskému parlamentu ze dne 20. října 2004.

Ve výše uvedeném dokumentu se konkrétně hovoří o hrozbě kybernetického útoku a kaskádových událostech. U kybernetického útoku se nepředpokládá velký počet obětí, ale mohlo by dojít k omezení nebo úplné ztrátě kriticky důležitých služeb, jako například telekomunikačních služeb. Existuje ovšem možnost kybernetického útoku na chemická zařízení nebo zařízení pro přepravu plynu, který by si mohl vyžádat lidské životy a velké materiální škody.

Katastrofickým příkladem může být selhání jednoho prvku kritické infrastruktury, který vede k selhání dalších prvků následovaný masivním kaskádovým efektem. Jako příklad je uvedeno selhání energetických sítí vedoucí k přerušení funkce čističek odpadních vod a vodáren. Možný je i konvenční bombový útok spojený s přerušením dodávek elektrické energie či telekomunikačních služeb, což by vedlo k prodloužení reakční doby a šíření paniky mezi veřejností. (Lazari, 2014)

Ochrana kritické infrastruktury musí vycházet z analýz hrozeb, zranitelnosti a minulých incidentů. Pro tyto analýzy je klíčový dostatek informací, který by měl být zajištěn mimo jiné vzájemným sdílením informací mezi členskými státy Evropské unie. Z důvodu nereálnosti ochrany veškeré infrastruktury před všemi typy hrozeb musí být též stanoveny nejrizikovější oblasti a určena minimální úroveň bezpečnosti, která zajistí obdobné zabezpečení kritické infrastruktury ve všech členských státech. Za stanovení a implementaci konkrétních opatření jsou zodpovědné jednotlivé státy, respektive vlastníci a provozovatelé prvků kritické infrastruktury, kteří se musí řídit národními právními předpisy. Úloha Evropské unie spočívá v koordinaci ochrany evropské kritické infrastruktury a poskytování podpory členským státům, zejména v případě teroristických útoků či jiných rizik vyžadujících okamžitou reakci.

Při určování ochrany prvku kritické infrastruktury by se mělo vycházet ze tří hledisek: Rozsahu, závažnosti a času. Hledisko rozsahu představuje velikost území, které je zasaženo.

Dělí se na mezinárodní, vnitrostátní, teritoriální/oblastní a místní úroveň. V rámci časového hlediska se uvažuje doba, za kterou se dostaví následky narušení funkce kritické infrastruktury, zdali jsou následky okamžité či opožděné. Jako kritéria hodnocení dopadu lze použít veřejný dopad (počet obětí, počet zasažených obyvatel, evakuace), hospodářský dopad (vliv na HDP, zhoršení kvality výroby a služeb), dopad na životní prostředí, míra závislosti prvku kritické infrastruktury s dalšími prvky a politický dopad (snížení důvěry veřejnosti ve vládu). Dopad ztráty prvku kritické infrastruktury může být hodnocen jako velký, mírný, minimální nebo žádný. (Komise evropských společenství, 2004)


*Obrázek 1 - Mapa teroristických útoků v EU od roku 2014 do července 2016; zdroj: The Sun, 2016*

V posledních několika letech sledujeme výrazný nárůst počtu teroristických útoků v zemích Evropské unie. Na obrázku 1 jsou zobrazeny teroristické útoky s oběťmi na životech, které se uskutečnily v Evropě a blízkém okolí od roku 2014 do 26. července 2016. Po tomto datu teroristické útoky neustaly a počet obětí přibývá i v roce 2017.

Často se jedná o činy jednotlivých radikalizovaných islamistů, kteří útok plánují bez napojení na teroristickou organizaci. Bez ohledu na organizátora cílily všechny teroristické útoky výhradně na civilní obyvatelstvo nebo příslušníky ozbrojených sil a ozbrojených bezpečnostních sborů. Přes nutnost ochrany obyvatelstva na veřejných prostranstvích

a kulturních či jiných akcí s velkým počtem návštěvníků, neměla by se podceňovat ani bezpečnostní opatření prvků kritické infrastruktury. Fakt, že teroristé doposud neútočili na kritickou infrastrukturu, nelze považovat důvod, že se tak nebude dít ani v budoucnu.

## 2.4 Budování bezpečnější evropské kritické infrastruktury

Po komplexním přezkoumání a analýzách funkčnosti Evropského programu na ochranu kritické infrastruktury vydala Evropská komise 4. září 2013 pracovní dokument o novém přístupu k EPCIP s názvem „Budování bezpečnější Evropské kritické infrastruktury." V dokumentu jsou navrženy přepracované přístupy k ochraně kritické infrastruktury ve fázích prevence, připravenosti a odezvy.

Ve fázi prevence se uplatní analýzy vytvořené na základě dříve získaných informací a zkušeností s ochranou kritické infrastruktury provozovatelů výše uvedených čtyř infrastruktur. Zároveň se využijí nové poznatky a nástroje posouzení a zvládání rizik a další nové možnosti poskytnuté výzkumným a vývojovým sektorem. Při přípravě zabezpečení je také třeba věnovat zvýšenou pozornost kybernetickým hrozbám, které v moderním světě mohou zasáhnout a ohrozit většinu kritické infrastruktury.

Pro zlepšení připravenosti na mimořádné události ohrožující kritickou infrastrukturu Evropská unie podporuje strategie pro připravenost, které jsou založené na kontingenčním plánování, odborné přípravě, společných cvičeních, zátěžových testech a zvyšování všeobecného povědomí o ochraně kritické infrastruktury. Podporuje se též dialog mezi členskými státy a vlastníky/provozovateli kritických infrastruktur. *„Cílem je u členských států a jiných aktérů závislých na kritické infrastruktuře zvýšit povědomí o tom, jak se mohou v rámci odezvy připravit na události, které mohou zasáhnout evropskou kritickou infrastrukturu."* (Evropská komise, 2013, s. 9)

Cílem vylepšení odezvy je zlepšit a posílit spojení mezi vlastníky/provozovateli kritické infrastruktury a systémy včasného varování. Nástroje včasného varování proti přírodním katastrofám by mohly ukázat potenciální hrozby vůči prvkům kritické infrastruktury. Zároveň se přezkoumá současný Mechanismus civilní ochrany Unie (2007/779/EK, Euratom: Rozhodnutí Rady z 8. listopadu 2007 o vytvoření Mechanismus civilní ochrany Společenství (přepracovaná verze)), který počítá pouze s okamžitou odezvou na krizovou

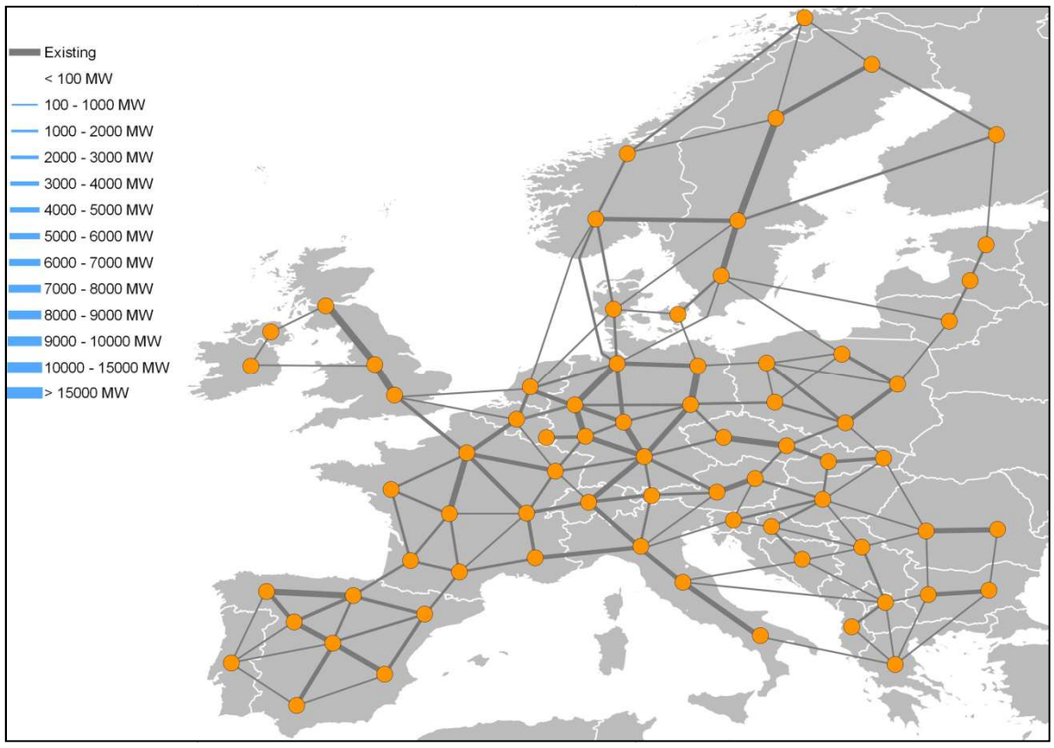
situaci, ale mohl by být rozšířen o skupiny odborníků, které by pomohly členským státům s obnovou poškozené kritické infrastruktury v dlouhodobém horizontu. (Evropská komise, 2013)

**Nový přístup k EPCIP**

Pro první fázi nového praktického přístupu k ochraně kritické infrastruktury byly vybrány čtyři infrastruktury, které mají celoevropský rozměr z důvodu zefektivnění ochrany a zvýšení odolnosti. Výběr probíhal na základě třech kritérií – příhraničního rozsahu, zájmu vlastníků/provozovatelů se podílet na pilotních úkolech a symboličnosti infrastruktury (pokrytí energetiky, dopravy a vesmíru). Tyto čtyři infrastruktury jsou Eurocontrol, plynová přenosová síť, elektrická přenosová síť a navigační systém Galileo.

EUROCONTROL funguje jako Síťový manager sítě ATM (uspořádání letového provozu) pro Evropskou unii v rámci systému Jednotné Evropské nebe. EUROCONTROL disponuje širokou infrastrukturou nacházející se po celé EU a její vyřazení z provozu by mohlo vést k mnoha kaskádovitým efektům. Výrazný dopad by v tomto případě mohl mít kybernetický útok. Pro zvýšení odolnosti lze využít dřívější krizové situace, které měly závažný dopad na řízení letového provozu, zejména se jedná o teroristické útoky 11. září 2001, výbuch islandské sopky v roce 2010 a silné sněžení též v roce 2010. (Evropská komise, 2013)

Elektrická a plynová přenosová jsou vystavěny bez úvahy národních hranic, tudíž jediné narušení sítí v jednom státu se může šířit do států okolních a způsobit celoevropský výpadek. Zároveň narušení funkce těchto sítí by mělo kritické následky v dalších oblastech, což by vedlo k mnoha následným negativním dopadům, např. na hospodářství, nouzové služby, šíření informací, dopravu atd. Vyřazení elektrické přenosové sítě z provozu se považuje za jeden z nejhorších možných scénářů. U plynové přenosové sítě se dále musí počítat s možnými politickými riziky, které by mohly ohrozit přístup k této strategické surovině. (Evropská komise, 2013)




*Obrázek 2 – Odhad struktury elektrické přenosové sítě v EU v roce 2020; zdroj: http://blogs.dnvgl.com/energy/integration-of-renewable-energy-in-europe*

Navigační systém GALILEO byl vybrán jakožto jeden z největších evropských projektů představující jedinou společnou evropskou vesmírnou infrastrukturu. Systém především nalézá široké možnosti uplatnění v klíčových oblastech ekonomiky, přispívá k zajišťování bezpečnosti a hraje významnou roli i v každodenním životě občanů. Jakožto vesmírná infrastruktura, systém GALILEO čelí specifickým rizikům. Jedná se o možnost rušení signálu ze satelitů, ať již úmyslné nebo neúmyslné, neautorizovaný přístup, interference, ale též vzrůstající množství trosek na oběžné dráze Země. V současnosti nemá EU k dispozici žádný systém sledování trosek a satelitů a je zcela závislá na informacích a varováních od Spojených států. (Evropská komise, 2013) Z hlediska České republiky je důležité, že v Praze sídlí administrační centrum tohoto navigačního systému.

# 3 OCHRANA KRITICKÉ INFRASTRUKTURY V ČESKÉ REPUBLICE

Kritická infrastruktura je v českém právním řádu zakotvena v zákoně č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon). Do tohoto zákona byla ochrana kritické infrastruktury implementována zákonem č. 430/2010 Sb. zákon, kterým se mění zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů. Novelizovaný krizový zákon vstoupil v platnost 30. prosince 2010 a nabyl právní účinnosti 1. ledna 2011. Tímto zákonem byla do českého právního řádu zapracována Směrnice Rady 2008/114/ES ze dne 8. prosince 2008 o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu. (Zákon č. 430/2010 Sb., 2010)

Prvky kritické infrastruktury, jejichž provozovatelem je organizační složka státu, byly určeny usnesením vlády České republiky ze dne 14. prosince 2011 č. 934 k určení prvků kritické infrastruktury, jejichž provozovatelem je organizační složka státu. Kritéria pro určení prvků kritické infrastruktury byla určena nařízením vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury. Prvky kritické infrastruktury, které jsou vlastněny, provozovány nebo užívány nestátními subjekty, byly postupně určeny opatřením obecné povahy příslušnými ministerstvy na základě průřezových a odvětvových kritérií. (Hasičský záchranný sbor České republiky, 2017)

## 3.1 Prvky kritické infrastruktury v České republice

V České republice, obdobně jako v jiných státech Evropské unie, ale i jiných vyspělých státech jako například Spojené státy nebo Kanada, se rozlišují prvky kritické infrastruktury, jejichž provozovatelem je organizační složka státu a prvky kritické infrastruktury, které jsou provozovány nestátním subjektem kritické infrastruktury.

Hlavní rozdíl je v určování prvků kritické infrastruktury. Příslušná ministerstva a jiné ústřední správní orgány zpracovaly návrh prvků kritické infrastruktury, které provozuje organizační složka státu spadající do jejich působnosti. Tento seznam následně zaslaly Ministerstvu vnitra. Ze zaslaných návrhů vytvořilo Ministerstvo vnitra seznam, který předložilo vládě ke schválení, ke kterému došlo 14. prosince 2011 výše uvedeným

usnesením vlády č. 934/2011. Ke konci roku 2011 bylo určeno celkem 103 prvků kritické infrastruktury, jejichž provozovatelem byla organizační složka státu. Z toho 64 prvků spadalo do oblasti veřejné správy, 35 prvků do odvětví nouzových služeb a 4 prvky byly určeny v oblasti komunikačních a informačních systémů. V současné době (k 14. prosinci 2016) je určeno 415 prvků kritické infrastruktury provozovaných organizační složkou státu.

Pokud provozovatelem prvku kritické infrastruktury není organizační složka státu, prvky jsou určeny přímo příslušnými ministerstvy nebo jinými ústředními správními orgány formou opatření obecné povahy. Ministerstva a jiné ústřední správní orgány přitom postupují podle správního řádu (zákon č. 500/2004 Sb., správní řád). O určení prvků kritické infrastruktury jsou povinny bez zbytečného odkladu informovat Ministerstvo vnitra, které vede celkový přehled. (Minář, 2012)

K říjnu 2012 bylo v sedmi odvětvích určeno 1333 prvků kritické infrastruktury, jejichž provozovatelem není organizační složka státu, které provozovalo 152 subjektů kritické infrastruktury. (Rosinová, 2012) V tomto případě počet prvků kritické infrastruktury do roku 2016 mírně poklesl na 1306 určených prvků.

Aktuální počet prvku kritické infrastruktury na území České republiky, které provozuje (neprovozuje) organizační složka státu, je uveden v následující tabulce. Jedná se o informace platné k 14. prosinci 2016, kdy byly usnesením vlády č. 1139 schválen aktualizovaný seznam prvků kritické infrastruktury, jejichž provozovatelem je organizační složka státu.

*Tabulka 1 - Prvky kritické infrastruktury k 14. prosinci 2016; zdroj: Usnesení vlády České republiky č. 1139, 2016*

| Odvětví | Počet prvků kritické infrastruktury, jejichž provozovatelem je: | | Celkem |
|---|---|---|---|
| | Organizační složka státu | Není organizační složka státu | |
| **Energetika** | 0 | 303 | 303 |
| **Vodní hospodářství** | 0 | 11 | 11 |
| **Potravinářství a zemědělství** | 0 | 0 | 0 |
| **Zdravotnictví** | 0 | 0 | 0 |
| **Doprava** | 0 | 13 | 13 |
| **Komunikační a informační systémy** | 55 | 886 | 941 |
| **Finanční trh a měna** | 0 | 74 | 74 |
| **Nouzové služby** | 279 | 19 | 298 |
| **Veřejná správa** | 81 | 0 | 81 |
| **Celkem** | **415** | **1306** | **1721** |

Počet subjektů, které provozují 1721 prvků kritické infrastruktury v České republice je 147. Více než polovinu prvků kritické infrastruktury provozovaných organizační složkou státu provozuje Hasičský záchranný sbor ČR, respektive Hasičské záchranné sbory krajů, konkrétně se jedná o 258 prvků kritické infrastruktury. To je dáno tím, že jako prvky kritické infrastruktury jsou určeny operační a informační střediska HZS a výjezdové stanice. Celkový počet prvků kritické infrastruktury se od prvního určení prvků kritické infrastruktury v roce 2011 (2012 pro prvky kritické infrastruktury, jejichž provozovatelem není organizační složka státu) zvýšil o 285 ze 1436 na 1721 prvků.

## 3.2 Povinnosti subjektu kritické infrastruktury

Hlavním dokumentem zajištění ochrany kritické infrastruktury je plán krizové připravenosti subjektu kritické infrastruktury. Povinnost zpracovat plán krizové připravenosti subjektu kritické infrastruktury je uvedena v krizovém zákoně, přičemž podrobnosti zpracování a obsahu plánu stanovuje nařízení vlády č. 462/2000 Sb., k provedení § 27 odst. 8 a § 28 odst. 5 zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon). Určené subjekty kritické infrastruktury byly povinny zpracovat plán krizové připravenosti subjektu kritické infrastruktury do 12. prosince 2012. Pro zpracování plánů krizové připravenosti zpracovalo Ministerstvo vnitra metodiku MV-140690-1/PO-PKR-2011. Účelem metodiky je zajistit obdobný způsob zpracování plánů u všech subjektů zpracovávající plány krizové připravenosti. Plán krizové připravenosti subjektu kritické infrastruktury se skládá ze základní, operativní a pomocné části.

V základní části plánu jsou uvedeny zejména informace o provozovateli prvku kritické infrastruktury a identifikace a hodnocení rizik. Zásadní součástí základní části plánu je analýza rizik včetně analýzy ohrožení a potenciálních dopadů. Analýza je základním východiskem pro tvorbu opatření k zajištění ochrany konkrétního kritické infrastruktury, která jsou uvedena v operativní části plánu krizové připravenosti.

Obsahem operativní části plánu krizové připravenosti subjektu kritické infrastruktury nejsou pouze postupy a opatření k minimalizaci rizik pro funkčnost prvku kritické infrastruktury vyplývajících z analýzy rizik. V této části je dále uveden přehled opatření, která prvek kritické infrastruktury plní na základě krizového plánu příslušného orgánu krizového řízení a všechna opatření, která za tímto účelem prvek kritické infrastruktury realizuje. Pokud je prvek kritické infrastruktury současně dodavatelem mobilizační dodávky, součástí operační části je i plán opatření hospodářské mobilizace. Součástí je i přehled spojení na příslušné orgány krizového řízení a přehled dalších plánů zpracovaných podle jiných právních předpisů, které by bylo možné využít k řešení krizových situací.

Z hlediska řešení krizové situaci jsou nejdůležitější součástí pomocné části geografické podklady. Dalším obsahem pomocné části je přehled smluv, které uzavřel subjekt kritické infrastruktury s dalšími osobami k plnění opatření prvku kritické infrastruktury, zásady

manipulace s plánem, přehled právních předpisů, které je při přípravě na mimořádné události nebo krizové situace možno využít a další související dokumenty.

Subjekt kritické infrastruktury je dále povinen určit styčného bezpečnostního zaměstnance, přičemž určení zaměstnance bez zbytečného odkladu oznámí příslušnému ministerstvu nebo jinému ústřednímu správnímu úřadu. Styčný bezpečnostní zaměstnanec zajišťuje součinnost mezi subjektem kritické infrastruktury a příslušným ministerstvem nebo jiným ústředním správním úřadem. Styčný bezpečnostní zaměstnanec musí být odborně způsobilý (tříletá praxe v alespoň jedné z následujících oblastí: krizové řízení, ochrana obyvatelstva a zajišťování bezpečnosti ČR nebo dosáhl vysokoškolského vzdělání v těchto oblastech). (Zákon č. 240/2000 Sb., krizový zákon)

## 3.3 Komplexní strategie České republiky k řešení problematiky ochrany kritické infrastruktury

Prioritním úkolem vlády každého státu by mělo být zajištění bezpečnosti občanů a naplňování jejich životních potřeb, ekonomické prosperity, ochrana životního prostředí a kvalitní technickou infrastrukturu. Zejména v případě mimořádných událostí a krizových situací je nezbytné zabránit vzniku takové úrovně ohrožení, která by měla negativní následky na společnost. Za tímto účelem musí být zajištěno plynulé fungování základních, životně důležitých zdrojů, infrastruktur a služeb a zabezpečena jejich adekvátní ochrana a spolehlivost.

V současné době je pouze velmi nízká pravděpodobnost vypuknutí válečného konfliktu, který by mohl přímo ohrozit území České republiky a v následující dekádě se nepředpokládá žádná změna. Zvyšuje se však pravděpodobnost jiných hrozeb, které by potenciálně mohly kritickou infrastrukturu ohrozit. Z vývoje posledních let v České republice i v Evropě se ukazuje, že nejvyšší ohrožení pramení z přírodních katastrof a nevojenských mimořádných událostí způsobených lidským faktorem. Musí se též počítat s rizikem omezení nebo úplného zastavení dodávek strategických surovin, na kterých je kritická infrastruktura závislá.

Strategie vychází z analýzy stavu kritické infrastruktury v České republice i ve světě a navazuje na předchozí dokumenty, které projednávala vláda ČR, Bezpečnostní rada státu a zejména její Výbor pro civilní nouzové plánování. Mezi tyto dokumenty patří zejména: „Zpráva o řešení problematiky kritické infrastruktury v České republice," ke které Bezpečností rada státu přijala 3. července 2007 usnesení č. 30, „Harmonogram dalšího postupu zpracování dokumentů Komplexní strategie České republiky k řešení problematiky kritické infrastruktury a Národního programu ochrany kritické infrastruktury," který projednala vláda 25. února 2008 a vydala usnesení č. 170 a „Aktualizace usnesení vlády č. 170 k Harmonogramu dalšího postupu zpracování dokumentů Komplexní strategie České republiky k řešení problematiky kritické infrastruktury a Národního programu ochrany kritické infrastruktury," kterou vláda schválila 2. března 2009 usnesením č. 222. Do strategie je současně promítnuta Směrnice Rady EU č. 2008/114/ES o určování a označování evropských kritických infrastruktur a o posuzování potřeby zvýšit jejich ochranu, která vstoupila v platnost 12. ledna 2009. (Ministerstvo vnitra, 2010)

**Principy a cíle strategie**

*„Základním principem řešení problematiky kritické infrastruktury je zajištění fungování klíčových a strategických infrastruktur s cílem zabezpečit ochranu obyvatelstva."* (Ministerstvo vnitra, 2010, s. 5) Kritická infrastruktura prostupuje všemi odvětvími státního hospodářství a základní životní potřeby společnosti jsou závislé na životně důležité infrastruktuře. Dle platné Bezpečnostní strategie České republiky je jednou ze základních povinností vlády ochrana životních zájmů státu a ochrana obyvatel, do čehož spadá i ochrana kritické infrastruktury. Koordinační roli pro ochranu kritické infrastruktury plní Ministerstvo vnitra, a to v rámci České republiky i koordinace se zahraničím. Spolupráce se zahraničím je důležitým faktorem komplexní ochrany kritické infrastruktury, neboť se musí uvažovat s mezinárodním charakterem kritické infrastruktury a vzájemnými vazbami mezi jednotlivými prvky kritické infrastruktury i různými odvětvími.

Členské státy Evropské unie se shodly na nutnosti přistupovat k hrozbám komplexně. Hlavním důvodem je nezbytnost okamžité reakce na nepředvídatelnou mimořádnou událost. Východiskem trvalého zvyšování ochrany a odolnosti prvků kritické infrastruktury je vytvoření základního legislativního rámce a stanovení dalších technických a organizačních podmínek. V oblasti analýz je nezbytným předpokladem vycházet

z realistického hodnocení situace a budoucího vývoje, především v oblasti finančních zdrojů.

Pro proces zajišťování ochrany kritické infrastruktury jsou klíčoví zástupci státu (vláda, ministerstva a jiné ústřední správní úřady) a především vlastníci/provozovatelé konkrétního prvku kritické infrastruktury. Vlastníci/provozovatelé prvku kritické infrastruktury jsou ze zákona (č. 240/2000 Sb., krizový zákon) přímo odpovědni za realizaci konkrétních opatření pro ochranu prvku kritické infrastruktury. Jsou povinni kontinuálně zajišťovat odolnost prvku kritické infrastruktury, která je ovlivňována řadou faktorů. Zejména přírodní podmínky se mění jen velmi pomalu, ale např. stav ekonomiky, sociální podmínky a s tím související nálady ve společnosti nebo mezinárodní bezpečnostní a politické prostředí podléhají velmi rychlým proměnám. Rychlost změn a obtížnost jejich predikce klade vysoké nároky na analýzy a systémy včasného varování. Klíčový je systém komunikace a výměny informací mezi státními subjekty a subjekty kritické infrastruktury i proces výměny informací navzájem mezi jednotlivými subjekty kritické infrastruktury. (Ministerstvo vnitra, 2010)

**Výzkum a vzdělávání pro ochranu KI**

Oblast kritické infrastruktury patří mezi jednu ze základních priorit bezpečnostního výzkumu v České republice. Vládou schválená Meziresortní koncepce bezpečnostního výzkumu a vývoje České republiky navazuje na priority Evropské unie a NATO. Účelem bezpečnostního výzkumu je dosáhnout takové úrovně poznatků, techniky a technologií, které České republice umožní získat, udržet a rozvíjet schopnosti potřebné pro ochranu obyvatelstva a zajištění bezpečnosti státu.

Pro zajištění podmínek efektivního řešení mimořádných událostí velkého rozsahu a krizových situací je kromě výzkumu a zavádění nových technologií důležitá odborná příprava a vzdělávání příslušných pracovníků. Pro oblast kritické infrastruktury je důležité zajištění odborné kvalifikace styčných bezpečnostních pracovníků, kteří zodpovídají za koordinaci činnosti a spolupráci mezi subjektem kritické infrastruktury a státními orgány, případně dalšími subjekty kritické infrastruktury. Cíloví pracovníci pro oblast kritické infrastruktury by měli být vzděláváni podle současného vzdělávacího procesu určeného pro

krizové řízení podle „vzdělávacích modulů A – J“ zpracovaných v Koncepci vzdělávání v oblasti krizového řízení schválené Bezpečnostní radou státu. (Ministerstvo vnitra, 2010)

## 3.4 Národní program ochrany kritické infrastruktury

Národní program ochrany kritické infrastruktury je navazující dokument na výše uvedenou Komplexní strategii. Cílem Programu bylo rozpracovat záměry obecně stanovené ve Strategii do konkrétních kroků.

Pro splnění podmínek Evropského programu na ochranu kritické infrastruktury bylo nutné do českého právního řádu implementovat směrnici Rady 2008/114/ES. Za tímto účelem byla vytvořena pracovní skupina, která se skládala ze zástupců dotřených ministerstev a jiných ústředních správních úřadů. Výsledkem byla novelizace zákona č. 240/2000 Sb. (krizový zákon).

K určování prvků kritické infrastruktury jsou v krizovém zákoně stanovena odvětvová a průřezová kritéria. Při vytváření těchto kritérií se vycházelo ze základního předpokladu nenahraditelnosti kritické infrastruktury. Rozumí se tím skutečnost, že pro obnovení funkce infrastruktury jsou nutné opravy nebo výstavba nového prvku a výstup infrastruktury nemůže být v krátkém období nahrazen, přičemž provizorní řešení výrazně zasáhne do života obyvatelstva a funkcí státu. (Ministerstvo vnitra, 2010)

**Konkrétní nositelé úkolů**

Národní program ochrany kritické infrastruktury stanovuje konkrétní státní i nestátní subjekty, které plní stanovené úkoly. Opatření na ochranu kritické infrastruktury realizují subjekty kritické infrastruktury, jejichž povinnosti jsou zpracovány v samostatné podkapitole.

Koordinační roli pro celou problematiku kritické infrastruktury plní Ministerstvo vnitra. V souvislosti s koordinací ochrany kritické infrastruktury je Ministerstvo vnitra stanoveno jako kontaktní místo pro spolupráci v rámci Evropské unie a současně plní úkoly vyplývající pro Českou republiku z jejího členství v EU. Dále předkládá vládě návrh průřezových a odvětvových kritérií a návrh oblastí kritické infrastruktury a konkrétních prvků kritické

infrastruktury. Vlády poté projednává a schvaluje navržená odvětvová a průřezová kritéria a seznam prvků kritické infrastruktury.

Ministerstva a jiné ústřední správní úřady poskytují informace Ministerstvu vnitra, vytvářejí návrhy odvětvových kritérií, zpracovávají resortní programy ochrany kritické infrastruktury, navrhují subjekty kritické infrastruktury, jejichž provozovatelem je organizační složka státu a určují subjekty kritické infrastruktury, jejichž provozovatelem není organizační složka státu (Ministerstvo vnitra, 2010)

**Programy pro ochranu kritické infrastruktury**

Národní program v rámci příprav na implementaci Evropského programu na ochranu kritické infrastruktury do českých podmínek navrhuje několik konkrétních programů a oblastí, které je nutné projednat.

Nejdůležitějším programem je vypracování analýz, které jsou východiskem pro veškeré plánování a přípravu opatření ochrany kritické infrastruktury. Analýzy by měly být zaměřeny na možná ohrožení celostátně významných prvků kritické infrastruktury, zejména v oblasti energetiky, dopravě a komunikacích. Další oblastí pro provedení analýzy jsou vzájemné vazby mezi prvky kritické infrastruktury nebo i mezi různými odvětvími. Cílem bylo nalezení zranitelných míst ve vzájemných vazbách a posouzení možnosti jejich posílení.

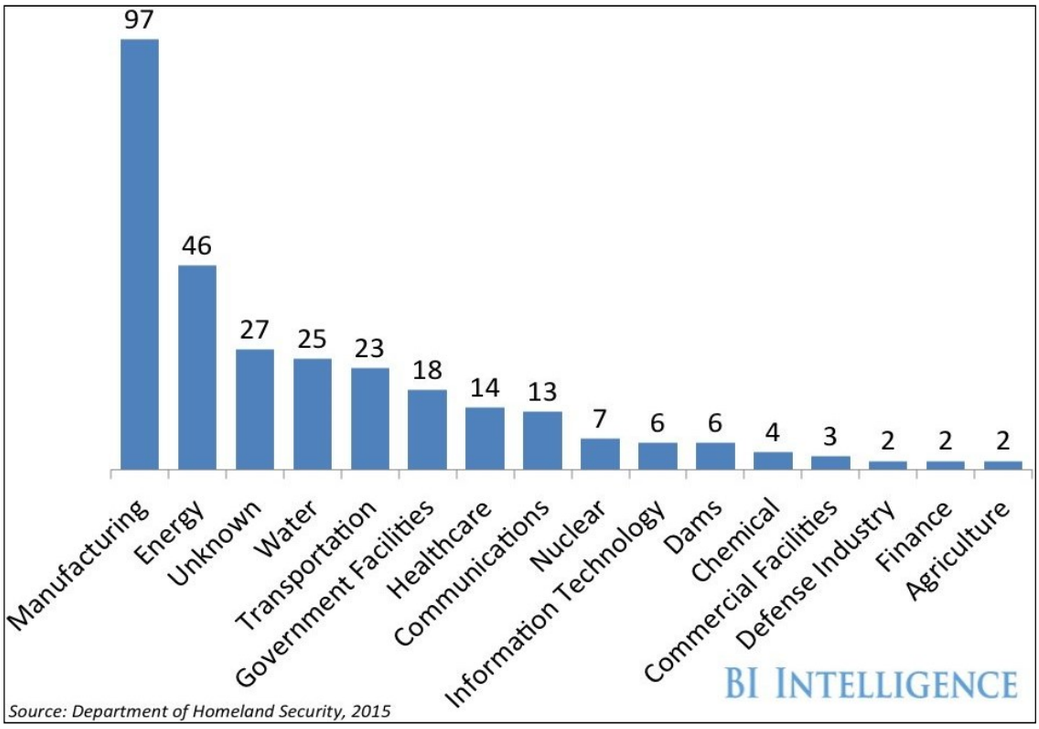
K projednání byla navržena zejména oblast plánování související s implementací problematiky kritické infrastruktury do právního řádu ČR a další související vnitřní předpisy a normy pro prvky kritické infrastruktury. Projednávaly se otázky související s úpravou metodiky zpracování krizových plánů, plánů krizové připravenost a dalších interních bezpečnostních plánů a v neposlední řadě plány zabezpečení kontinuity činnosti subjektu kritické infrastruktury. (Ministerstvo vnitra, 2010)

# 4 KYBERNETICKÁ BEZPEČNOST

Kybernetická bezpečnost se s narůstající závislostí prakticky celé společnosti na technologiích stává jednou z klíčových otázek zajištění bezpečnosti státu. Spolu s rozšířením digitálních technologií do téměř všech oblastí funkce společnosti a státu a jejich vzrůstající komplexností a propojeností se objevují nové hrozby a rizika včetně možnosti závažného domino efektu. Např. vyřazení elektrické rozvodné sítě kyberútokem může mít, v závislosti na době výpadku, za následek snížení efektivnosti záchranných a bezpečnostních sborů, narušení poskytování základních služeb obyvatelstvu, omezení zásobování pitnou vodou a potravinami, pozastavení činnosti průmyslu a s tím související ekonomické škody. Vzhledem k zasažení zdravotnictví může dojít i ke ztrátám na životech obyvatel. Jediný kyberútok může následně vyústit v protesty veřejnosti proti vládě, která mu nezabránila, případně nepostupovala podle představ veřejnosti a dojít k jejímu svržení, případně výraznému ovlivnění blízkých voleb. I dočasné vyřazení energetické sítě může být použito k paralyzování určité oblasti, například v kombinaci s „klasickým“ teroristickým útokem může výrazně zvýšit následky útoku. Reálným příkladem efektivnosti útoku na elektrickou rozvodnou síť je útok na ukrajinskou elektrickou rozvodnou síť údajně realizovaný údajně ruskými hackery, kteří 23. prosince 2015 na 6 hodin zastavili dodávky elektrické energie pro až 700 000 lidí (Groll, 2016).

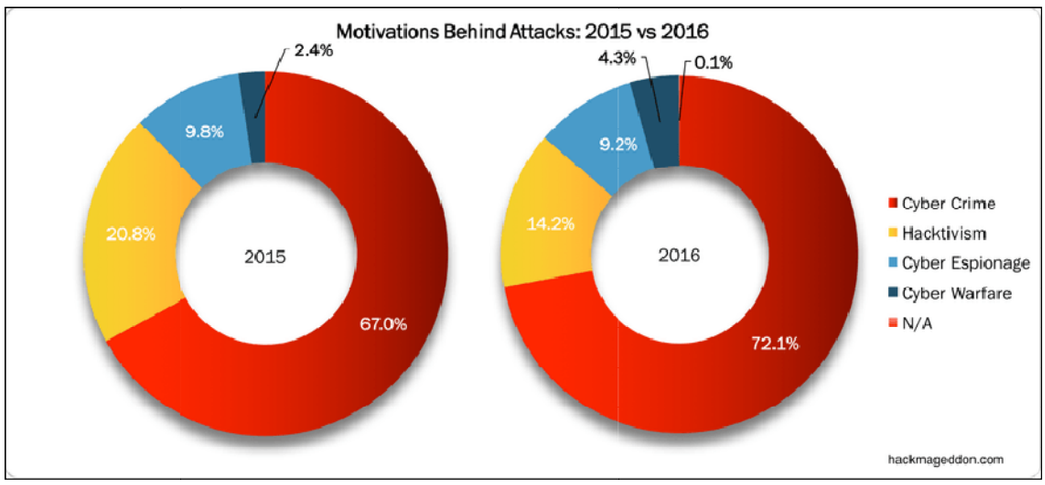
Kybernetický útok může též mít za cíl přímé ohrožení života a zdraví obyvatel. Tento typ útoku, tzv. kyber-fyzický, jak jej nazývají Marina Krotofil (bezpečnostní konzultant Evropské sítě pro kybernetickou bezpečnost a Jason Larsen (bezpečnostní konzultant v IOActive), způsobí prostřednictvím kybernetického útoku fyzické poškození objektu, které může mít různé bezpečnostní následky. Nejznámějším, ovšem ne jediným, příkladem tohoto typu útoku je použití červu Stuxnet, který závažně poškodil Íránské centrifugy na obohacování uranu (Root.cz, 2014). Jak ale prokázali ve své studii Marina Krotofil a Jason Larsen, velice zranitelná je i chemická továrna. V rámci výzkumu vytvořili nástroj, který umožňuje napadnout simulovanou chemickou továrnu. Následky útoku mohou být kromě získání provozních informací i přímé poškození chemických reaktorů nebo zásobníků vedoucí k možnému uvolnění chemických látek do ovzduší. Tento výzkum měl ukázat, jakým způsobem je možné chemickou továrnu ohrozit a v rámci simulovaného útoku naučit bezpečnostní techniky kybernetický útok rozpoznat. (NetworkWorld.com, 2015)

Možnosti napadení prvku kritické infrastruktury se neomezují pouze na chemický průmysl a energetické sítě. Podle statistiky amerického Ministerstva národní bezpečnosti se v roce 2015 uskutečnilo 295 kybernetických útoků na prvky kritické infrastruktury Spojených států a to v 16 různých odvětvích kritické infrastruktury.




*Graf 2 - Kybernetické útoky na sektory kritické infrastruktury v USA; zdroj: Ministerstvo národní bezpečnosti Spojených států amerických; 2015*

Z grafu 3 je patrné, že nejčastějším útokem se stávaly výrobní podniky. Domnívám se, že se za tímto faktem skrývá průmyslová špionáž. Vysoký je i počet útoků na sektor energetiky. V roce 2015 má část útoků na svědomí pravděpodobně stejná skupina hackerů, kteří zaútočili na ukrajinskou elektrickou rozvodnou síť. Je možné, že některé z těchto útoků (nezpůsobily výpadek) byly testem před uskutečněním hlavního útoku v Ukrajině. (Groll, 2016) Útokům se ale nevyhnuly ani jaderná zařízení, přehrady nebo chemická kritická infrastruktura. Statistika ovšem nezmiňuje motivaci na pozadí útoků ani jejich záměr či následky, tudíž v celkových číslech nejsou rozlišeny snahy o získání tajných informací nebo záměrné snahy o poškození kritické infrastruktury.




*Graf 3 - Motivace kybernetických útoků; zdroj: Hackmageddon.com, 2017*

Podle globálních statistik kybernetických útoků pravidelně uveřejňovaných serverem Hackmageddon.com je zcela dominantním motivem útoků kybernetická kriminalita, což v tomto případě obvykle znamená snaha získat finanční prostředky nelegálním způsobem. Kybernetická kriminalita tedy ze své podstaty není primární hrozbou pro prvky kritické infrastruktury. Výjimku ovšem může tvořit ransomware. Tento škodlivý kód zablokuje přístup do infikovaného počítače a jeho tvůrci zpravidla požadují zaplacení výkupného.

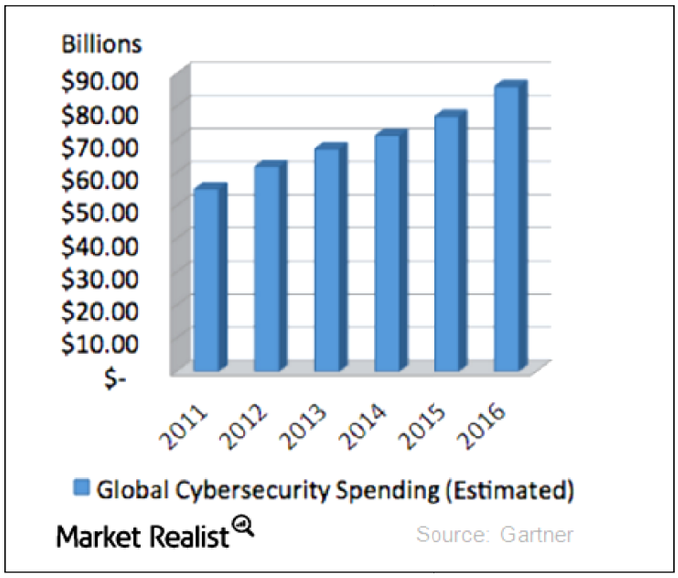
Domnívám se, že z hlediska bezpečnosti kritické infrastruktury představuje největší nebezpečí kybernetická špionáž a především útoky spadající do kybernetické války. Kybernetickou špionáží lze získat informace o prvku kritické infrastruktury, které mohou být využity při fyzickém napadení a útoky v rámci kybernetické války cílí na odstavení nebo poškození kritické infrastruktury.

Nejen pro prvky kritické infrastruktury představuje značné riziko velké rozšíření počítačů a dalších chytrých zařízení, která díky vývoji mají stále větší výpočetní výkon. Odhaduje se, že počet těchto zařízení se v současnosti pohybuje kolem 4 miliard (Statista.com, 2017) a značná část z nich nemusí být dostatečně zabezpečena. Toho lze zneužít a společný výpočetní výkon útočníkem kontrolovaných zařízení použít k efektivnímu napadení vysoce zabezpečených počítačových infrastruktur.

Pro plánování a vytváření bezpečnostních opatření v oblasti počítačových technologií se uplatňují obdobné postupy a principy napříč všemi oblastmi využívajícími počítače (od

státních organizací přes vojenská zařízení po komerční firmy nebo i, samozřejmě se sníženými nároky na bezpečnost, domácí uživatele). V první řadě je nutné si uvědomit, že celková bezpečnost je na takové úrovni, jak je silný nejslabší článek v bezpečnostních opatřeních a zároveň počítat s tím, že nepřekonatelné zabezpečení neexistuje.

Pro zajištění efektivní úrovně zabezpečení počítačových sítí a technologií se musí k této problematice přistupovat komplexně. Nelze se spoléhat pouze na hardwarová či softwarová opatření, ale, dalo by se říci především, by se měla věnovat pozornost koncovým uživatelům zabezpečených technologií. Při návrhu komplexního bezpečnostního systému se řeší opatření související s uživateli, bezpečnost konkrétních počítačů nebo jiných síťových prvků, bezpečnost vnitřní sítě a zabezpečení internetové komunikace. (Mead, 2016)




*Graf 4 - Odhadované finanční prostředky vynaložené na kybernetickou bezpečnost; zdroj: Gartner, 2016*

Vzhledem k dynamice virtuálního prostoru se musí obranná opatření pružně přizpůsobovat novým hrozbám, které neustále přibývají. Veškerá opatření k zajištění počítačové bezpečnosti jsou tudíž velice nákladná. Odhadované celosvětové finanční prostředky vynaložené na zajištění kybernetické bezpečnosti v roce 2016 se pohybují kolem 2,2 biliónu Kč.

# 5 METODY ZAJIŠTĚNÍ BEZPEČNOSTI

Pro zabezpečení objektu a areálu se používají běžné komerční metody objektové bezpečnosti. Principiálně se jedná o zabránění vniknutí do areálu, kontrolu a povolování vstupu určeným osobám, omezení pohybu osob v areálu a stanovení přístupových práv zaměstnancům. Vzhledem k závislosti technických prostředků střežení na informačních technologiích a možnosti kybernetického útoku je nezbytné počítat i s kybernetickou bezpečností a v neposlední řadě je nutné zabezpečit zásobování elektrickou energií. Metody ochrany objektů se obvykle rozdělují na mechanické, fyzické, technické a režimové.

## 5.1 Mechanická ochrana

Zabezpečení objektu pomocí mechanických prostředků spočívá v instalaci mechanických bezpečnostních prvků, které fyzicky zamezují neoprávněnému vniknutí do chráněné oblasti nebo zabraňují odcizení důležitých dokumentů, předmětů atd., případně takovéto počínání výrazně ztěžují a časově prodlužují. Spolu s fyzickou ochranou se jedná o nejstarší formu ochrany. Během dlouhého vývoje mechanických prostředků ochrany došlo k jejich výraznému vylepšení a technického zdokonalení, ovšem spolu s jejich vývojem docházelo též k vývoji technik a prostředků pro jejich překonání. (Uhlář, 2009) Obecně platí, že každá mechanická ochrana se sama o sobě nechá určitým způsobem překonat, někdy i velice snadno a rychle, což ovšem platí i pro ostatní formy zabezpečení objektu. Z tohoto důvodu se zpravidla nepoužívá pouze jedna forma zabezpečení, ale kombinace (nejlépe) všech variant přizpůsobených pro potřeby konkrétního objektu s ohledem na daný rozpočet, přičemž mechanická ochrana tvoří základní pilíř objektové bezpečnosti. (Ivanka, 2010) Mach (2012) rozděluje mechanickou ochranu objektu a areálu do čtyř kategorií podle místa uplatňování opatření, a to na obvodovou ochranu, plášťovou ochranu, prostorovou ochranu a předmětovou ochranu. V tomto rozdělení se postupuje od vnější hranice areálu (obvodová ochrana) až k samotným cenným předmětům v objektu (předmětová ochrana).

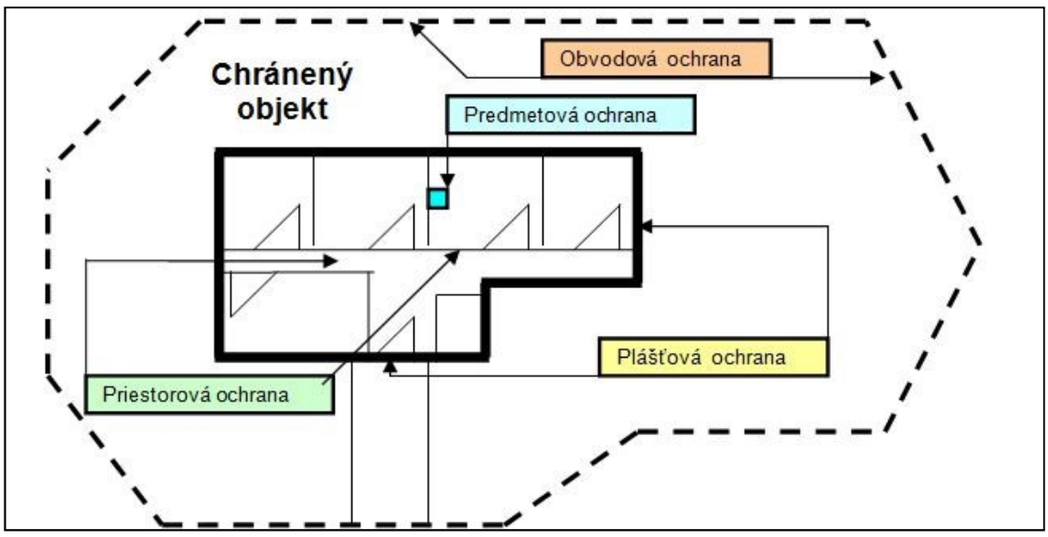
Předmětem obvodové ochrany je zajištění bezpečnosti v okolí objektu, respektive ochrana hranice jeho areálu, obvodu. Základní prostředky obvodové ochrany jsou ploty nebo zdi a jejich mechanické zabezpečení, např. žiletkovým drátem. Pro ochranu vjezdů se používají

brány, závory, retardéry, zastavovací pásy a vstup pro zaměstnance a další osoby se chrání turnikety, bezpečnostními branky atd.

Při posunu z hranice areálu k samotnému objektu se dostáváme do kategorie plášťové ochrany. Plášť v tomto případě představuje vnější stěny objektu včetně oken, dveří a dalších otvorů. Plášťová ochrana tedy zabraňuje (ztěžuje) vniknutí narušitele do vnitřních prostor objektu. Prvky plášťové ochrany jsou mříže, bezpečnostní dveře, rolety, bezpečnostní folie a skla atd. Při stanovování plášťové ochrany je však nezbytné počítat i s bezpečností samotných zdí, střech, případně i podzemních prostor.

Uvnitř objektu se uplatňuje prostorová ochrana, která je tvořen bezpečnostními prvky již v samotném vnitřním prostoru objektu. Poté, co pachatel vnikl do objektu, prvky prostorové ochrany by mu měly zabránit (ztížit) pokračovat dále od místa vniknutí. Bezpečnostní prvky jsou podobné jako v případě plášťové ochrany, jedná se o vnitřní bezpečnostní dveře, zabezpečení vnitřních oken, průlezů atd., pouze přizpůsobené pro vnitřní použití (minimalizace omezení pohybu oprávněných osob, splnění požárních předpisů aj.).

Pokud by se pachatel dostal k předmětu (nebo do blízkosti předmětu), který by chtěl odcizit nebo jinak zneužít, uplatní se opatření předmětové ochrany. Již z názvu vyplývá, že tento okruh využití mechanických prostředků slouží k ochraně předmětů v objektu před odcizením, zkopírováním nebo zničením. Hlavním prostředkem mechanické ochrany jsou trezory a úschovné prostory, případně sem lze zařadit další prvky chránící před odnesením předmětů, jako je uchycení předmětů ke zdi nebo k jinému pevnému bodu či zabezpečení počítačových dat.




*Obrázek 3 - Zóny mechanické ochrany objektu; zdroj: Mach, 2012*

## 5.2 Fyzická ochrana

Fyzická ochrana (ostraha) objektu spočívá ve využití živé síly, lidí, ke střežení objektu. Fyzická ochrana objektu je důležitou součástí komplexu všech metod ochrany, neboť jako jediná je schopna přímého zásahu k odvrácení nebezpečí. Lidi lze využít k ochraně objektu přímo (provádí aktivní střežení, např. formou pochůzek po areálu) nebo k obsluze a doplnění ostatních metod ochrany (např. obsluha kamerových systémů). Fyzická ochrana je též nedílnou součástí režimových opatření, neboť lidé jsou nezbytní ke kontrole osob na vstupech. Fyzickou ochranu lze rozdělit podle času, kdy probíhá střežení a podle způsobu střežení.

**Časové hledisko**

V závislosti na druhu střeženého objektu či areálu a potřebám zadavatele střežení se určuje doba, ve kterou mají být bezpečnostní opatření realizována. Pokud je zvýšené riziko narušení bezpečnosti s možností vážných následků, obvykle se přistupuje ke kontinuálnímu střežení. Úroveň ochrany (počet lidí vykonávajících střežení, četnost pochůzek…) se může v průběhu dne lišit, ale objekt je střežen 24 hodin denně.

Častým případem je provádění střežení po skončení pracovní doby zaměstnanců, obvykle v noci. Objekt je střežen v době, kdy se v něm nenachází zaměstnanci, tedy v době zvýšeného rizika vstupu nepovolaných osob, a končí se začátkem denního (případně

nočního) provozu objektu. Běžný je i způsob ochrany pouze během pracovní doby, kdy po skončení pracovní doby a odchodu zaměstnanců zadavatele ochrany končí i fyzická ochrana objektu. Tento typ ochrany se v průmyslových objektech nepoužívá příliš často, ale využití nachází při potřebě kontroly zákazníků, případně zaměstnanců, např. v nákupních centrech či jiných obchodech.

Ochrana objektu, areálu nebo převozu cenných věcí může být pouze dočasná, tzv. nárazová. Nárazová fyzická ochrana se provádí v závislosti na potřebách zadavatele. Jedná se o krátkodobou ochranu (několik hodin až dní), která se provádí při zvláštních událostech, jako je přeprava cenných materiálů, peněz atd. nebo v případě krátkodobého zvýšení rizika narušení bezpečnosti.

**Způsob střežení**

Podle způsobu střežení objektu a areálu se ostraha může rozdělit na několik typů. Celoplošná ostraha objektu nemá stanovena pevná stanoviště, ale zaměstnanci střežící objekt provádí pochůzky v celém areálu. Pochůzky by měly procházet všemi rizikovými oblastmi v objektu a areálu, ale jejich doba a trasa by neměla být stále stejná, aby nebylo možné zjistit pravidla pohybu ostrahy a toho využít. Pro pochůzky lze též využít psovoda s cvičeným služebním psem. Pokud se fyzická ochrana zaměřuje především na ochranu perimetru, případně vnější hranice objektu, jedná se o obvodovou ochranu. Využívají se též většinou pochůzky zaměstnanců ostrahy, ale omezují se pouze na hranice areálu nebo objektu. Kontrolují se mechanické bariéry (ploty, zdi, mříže atd.), jestli nejsou poškozeny a případné vizuální potvrzení vniknutí do areálu nebo objektu.

Způsob zajištění ochrany prováděný pracovníky bezpečnosti na kontrolních stanovištích u vchodů a vjezdů se označuje jako propustková fyzická ochrana. Provádí se kontrola vstupujících osob (vozidel) a jejich oprávnění ke vstupu (vjezdu). Kontroluje se též obsah zavazadel, vnitřního prostoru vozidel aj. z důvodu neoprávněného vynášení majetku nebo naopak vnášení nebezpečných předmětů a prostředků. Propustková fyzická ochrana je zpravidla součástí režimové ochrany. (Lucký, 2007)

Jestliže objekt či areál není přímo fyzicky střežen bezpečnostními pracovníky, avšak pro případ narušení bezpečnosti střeženého objektu nebo areálu jsou vyčleněni pracovníci,

hovoří se o zásahovém typu fyzické ochrany. V tomto případě jsou „zásahové jednotky“ bezpečnostní agentury nebo provozovatele objektu dislokovány na jednom nebo více určených míst. Mohou se nacházet na stanovištích přímo v areálu střeženého objektu, nebo v externím objektu bezpečnostní agentury. Tento typ se používá v kombinaci s technickou ochranou, v případě signálu o narušení střeženého prostoru vyjedou bezpečnostní jednotky k zásahu. Jedná se o velmi rozšířený druh fyzické ochrany zejména u menších komerčních subjektů nebo i u domácností, chat a chalup.

Zvláštní typ je tzv. doprovodná ochrana. Tento typ fyzické ochrany spočívá v zajištění ochrany převážených cenností, peněz, nebo jiného důležitého obsahu. Zaměstnanci přiřazení jako doprovod cenného nákladu fyzicky dohlíží na bezpečnost převozu, ať se jedná o dopravu po silnicích, vodě nebo leteckou přepravu. Oproti ostatním typům fyzické ochrany se odlišuje místem, kde je ochrana realizována. Nejedná se o zajišťování ochrany objektu a jeho areálu, ale pouze důležitých předmětů či jiných věcí zpravidla zcela mimo prostory zadavatele ochrany.

Dále je možné fyzickou ochranu dělit podle způsobu zajištění na smluvní (zajišťovaná externí firmou), vlastní (zajišťovaná provozovatelem objektu) a kombinovanou. Podle rozsahu vybavení se fyzická ochrana dělí na ozbrojenou (střelná zbraň nebo jiné prostředky osobní obrany) a neozbrojenou. (Lucký, 2007)

## 5.3 Technická ochrana

Systém technické ochrany objektu využívá mechanické (viz samostatná podkapitola) a elektronické systémy, které jsou obsahem této podkapitoly. Prostředky technické ochrany umožňují nepřetržité monitorování a ochranu objektu a areálu. Elektronické systémy představují vysokou počáteční investici, ale jejich provoz je relativně levný, na rozdíl od fyzické ochrany, kdy platy zaměstnanců jsou z v dlouhodobém horizontu výrazně vyšší než náklady na provoz elektronických systémů střežení. Přesto nelze (pokud je cílem maximálně efektivní ochrana objektu) technickou ochranu provozovat bez kombinace s fyzickou ochranou. Existuje velký počet různých druhů technických prostředků střežení, důležité je ovšem zvolit adekvátní kombinaci metod a typů ochrany.

**Kamerové dohledové systémy**

Základním prvkem elektronického střežení objektu a areálu jsou kamerové dohledové systémy, tzv. CCTV (Closed Circuit Television – uzavřený televizní okruh). Zajišťují nepřetržité monitorování vybraných oblastí, přičemž se může jednat o pevné kamery s předem nastaveným úhlem snímání, nebo otočné kamery, které v určitých intervalech nebo na základě manuálního řízení mění snímanou oblast. Přenášený obraz z kamerových systémů může být neustále sledován obsluhou, nebo je díky nim možné identifikovat a usvědčit pachatele. Zároveň kamery působí jako preventivní opatření, odrazují případné narušitele bezpečnosti.

Z hlediska použitých technologií se kamery rozlišují na analogové a digitální a kabelové a bezdrátové. Ačkoliv se u spotřebitelských produktů často přechází na bezdrátové technologie, u bezpečnostních kamer je důležitá především spolehlivost, a ta je vyšší u kabelových systémů. Bezdrátové kamery mohou trpět výpadky signálu, nebo je lze cíleně rušit. Kamery mohou být dále vybaveny dalšími technickými prvky, jako je systém nočního vidění nebo přisvětlování. Existují také speciální termokamery zaznamenávající tepelnou stopu.

U kamer je důležitá celková kvalita obrazu (kombinace rozlišení, clony, kvality snímacího čipu, softwarového zpracování obrazu…) a ohnisková vzdálenost, která determinuje zorný úhel kamery, případně velikost přiblížení. (Matchett, 2003)

**Elektronická zabezpečovací signalizace**

Systémy elektronické zabezpečovací signalizace jsou souborem detektorů, rozvodů a vyhodnocovacích procesorů, které stanoveným způsobem upozorňují na narušení střežené oblasti. Podle způsobu získávání dat je lze rozlišit na aktivní a pasivní. (Brabec, 2001)

Aktivní detektory pracují na principu aktivní emise elektromagnetického záření. V případě, že narušitel vstoupí do vysílaného záření, dojde k jeho odrazu zpět do detektoru, který následně narušení bezpečnosti vyhodnotí a určeným způsobem o tomto narušení informuje. Druhá varianta aktivních detektorů spočívá v přerušení emitovaného paprsku

mezi vysílačem a přijímačem, čímž dojde ke spuštění poplachu. Mezi aktivní detektory patří elektronické závory nebo detektory pohybu.

Pasivní detektory vyhodnocují změnu sledovaných hodnot. Tato změna je vytvořena narušitelem. Může se jednat o seismické detektory zaznamenávající otřesy, infračervené detektory snímající teplo nebo jednoduché detektory otevření oken či dveří, tříštění skla atd. (Homrighaus, 2006)

**Pult centralizované ochrany**

Pult centralizované ochrany je centrální stanoviště řízení bezpečnosti. Svým způsobem se jedná o zmenšené operační středisko složek IZS přizpůsobené potřebám ochraně objektu. Na toto středisko jsou napojeny všechny elektronické zabezpečovací systémy a z jednoho místa je možné je ovládat a kontrolovat jejich hlášení. Operátor pultu centralizované ochrany má přehled o zabezpečení celého střeženého areálu a objektu, možné je i sledovat pohyb hlídek a případně upravovat jejich trasu. Operátor také může pomocí pultu přímo kontaktovat Policii ČR a majitele/provozovatele střeženého objektu nebo areálu.

Hlavní výhoda pultu centralizované ochrany je svedení všech elektronických bezpečnostních systémů na jedno místo a možnost jejich snadného ovládání z jednoho místa pomocí standardizovaného softwaru, což zároveň snižuje nároky na počet pracovníků obsluhy. Tato centralizace ovšem také představuje bezpečnostní riziko, zejména pro případ výpadku dodávek elektrické energie. V takovém případě by došlo ke ztrátě veškerého elektronického zabezpečení, proto je nezbytné zajistit spolehlivé nouzové zásobování elektřinou. (Homrighaus, 2006)

## 5.4 Režimová ochrana

Režimová ochrana je kombinací bezpečnostních a organizačně-administrativních opatření. Cílem je vytvoření jednoznačných směrnic pro pohyb osob v objektu včetně mechanismu kontroly dodržování směrnic, ověřování oprávnění osob ke vstupu do objektu a pro pohyb v různých zónách zabezpečení. Z hlediska zaměření se rozlišuje na vnitřní a vnější, přičemž vnitřní režimová ochrana je zaměřena vůči zaměstnancům objektu a vnější je cílena na kontrolu a omezení vstupu cizích lidí. (Uhlář, 2009)

**Vnější režimová ochrana**

Základním principem vnější režimové ochrany je identifikace a kontrola vstupujících osob. Vstup je následně povolen pouze zaměstnancům a dalším osobám, které mají dočasně povolen vstup. Kontrola zaměstnanců běžně probíhá formou zaměstnanecké karty a elektronického turniketu, ale cizí osoby musí mít vstup předem povolený. Je nutná jejich identifikace na základě např. čísla občanského průkazu a jejich kontrola pomocí např. detekčních rámů. (Brabec, 2001)

Pro vozidla platí podobné podmínky jako pro osoby. Automobily či jiná vozidla zaměstnanců jsou identifikovatelná pomocí státních poznávacích značek a pro posádku platí stejné podmínky jako pro ostatní zaměstnance. V případě potřeby mohou být vozidla ještě fyzicky zkontrolovány z hlediska převáženého nákladu. Pro vozidla návštěv lze využít také identifikaci na základě předem sdělené SPZ a osoby musí být opět kontrolovány obdobně, jako kdyby přišly bez vozidla. Vozidlo cizí příchozí osoby může představovat zvýšenou bezpečnostní hrozbu, proto by měl být jeho obsah zkontrolován.

**Vnitřní režimová ochrana**

Objekt může být členěn do více částí s různou úrovní zabezpečení a ostrahy. Stejně tak zaměstnanci získávají určitou úroveň bezpečnostních povolení v závislosti na jejich pracovní pozici a s tím související potřebě přístupu. Zaměstnanci mohou vstupovat pouze do míst, kam je to nezbytné. Pro omezení přístupu lze použít zámky na dveřích odemykatelné pomocí zaměstnaneckých karet, ale hrozí zneužití odcizení nebo ztracené karty, případně i vypůjčené. U vysoce zabezpečených objektů se proto (navíc) používají biometrické prostředky, jako čtečky otisků prstů nebo skenery oční sítnice.

Omezení pohybu a jeho monitoring souvisí s omezením přístupu. V areálu nebo i samotném objektu mohou být stanoveny bezpečností zóny, kam je zakázaný nebo velmi omezený vstup. K omezení pohybu lze použít prostředky mechanické ochrany. Monitoring se používá z preventivních důvodů, pokud se osoba nebo vozidlo pohybuje směrem nebo již v zóně se zákazem vstupu, lze využít fyzické ochrany objektu k zásahu ještě před samotným ohrožením objektu. Zároveň je na základě monitorovaného objektu naopak zpětně určit pachatele, pokud selhaly ostatní prvky zabezpečení objektu. (Ščurek a Maršálek, 2014)

# 6 CÍLE PRÁCE

Hlavním cílem teoretické části diplomové práce je zpracovat nástin přístupu k ochraně kritické infrastruktury v České republice a na úrovni Evropské unie a popsat možné způsoby střežení a zajištění bezpečnosti objektu a areálu.

Cílem praktické části je zpracovat návrh bezpečnostních opatření určených ke střežení a ochraně prvku kritické infrastruktury a na základě analýzy rizik navrhnout možnosti rychlého navýšení úrovně zabezpečení pro případ zvýšeného bezpečnostního rizika pro prvek kritické infrastruktury.

**Cíle práce:**

- Zpracovat nástin metod střežení objektu a areálu
- Vytvořit modelový prvek kritické infrastruktury
- Vytvořit návrh sytému zabezpečení modelového prvku kritické infrastruktury
- Analyzovat hrozby pro modelový prvek kritické infrastruktury
- Navrhnout způsob rychlého navýšení úrovně zabezpečení modelového prvku kritické infrastruktury

# 7 METODIKA

## 7.1 Stanovení typového prvku kritické infrastruktury

Pro potřeby této diplomové práce byl vytvořen typový prvek kritické infrastruktury spadající do oblasti energetiky, konkrétně rafinérie s kapacitou atmosférické destilace 750 000 tun za rok. Prvky bezpečnostního systému jsou navrženy na základě systému zabezpečení reálné ropné rafinerie s objemem atmosférické destilace 3,3 milionu tun ročně.

## 7.2 Analýza rizik

Analýza rizik pro prvek kritické infrastruktury je zpracována s využitím softwarového nástroje RISKAN. Vzhledem k zaměření diplomové práce je analýza rizik směřována především na rizika spojená s fyzickým narušením bezpečnosti objektu. Analýza zahrnuje možné body vniknutí do objektu a cíle úmyslného narušení bezpečnosti.

## 7.3 SWOT analýza zabezpečení prvku kritické infrastruktury

Navržené dlouhodobé zabezpečení prvku kritické infrastruktury je pro případ zvýšení rizika narušení bezpečnosti analyzováno s využitím SWOT analýzy. Analýza je předpokladem pro efektivní zvýšení úrovně zabezpečení. Pro navržené metody bezprostředního navýšení zabezpečení je též zpracována SWOT analýza.

## 7.4 Návrh systému zabezpečení a střežení

Navrhovaná bezpečnostní opatření a prvky systému zabezpečení a střežení prvku kritické infrastruktury jsou zpracovány na podkladě zabezpečení obdobného prvku kritické infrastruktury a analýzy rizik. Při návrhu systému zabezpečení a střežení se vychází ze současného technologického pokroku bezpečnostních prostředků s přihlédnutím k ekonomickým faktorům ovlivňujícím ochranu (nejen) prvku kritické infrastruktury. Navrhovaná bezpečnostní opatření pro běžný stav vychází z obdobných systémů zabezpečení, což umožňuje poukázat na reálné silné a slabé stránky.

## 7.5 Návrh způsobu navýšení úrovně zabezpečení prvku kritické infrastruktury

Navrhovaná opatření pro zvýšení zabezpečení prvku kritické infrastruktury reflektují hrozby identifikované ve SWOT analýze. S využitím silných stránek zabezpečení prvku kritické infrastruktury a příležitostí pro navýšení úrovně zabezpečení jsou navrženy opatření střežení a zabezpečení prvku kritické infrastruktury, která mohou být aplikována v relativně krátké době. Předpokladem navržených opatření je jejich krátkodobé uplatnění, a to především z důvodu finanční nákladnosti a organizačních opatření, která částečně zasahují do běžného provozu prvku kritické infrastruktury.

# 8 MODELOVÝ PRVEK KRITICKÉ INFRASTRUKTURY

Jako modelový prvek kritické infrastruktury, pro který jsou v následujících kapitolách zpracována bezpečnostní opatření a prvky systému zabezpečení, je zvolena ropná rafinerie splňující podmínku zařazení mezi prvky kritické infrastruktury podle nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury. Jedná se tedy o rafinérii s roční kapacitou atmosférické destilace přesahující 500 000 tun.

*Tabulka 2 - Provozní parametry modelové ropné rafinerie; zdroj: vlastní*

| Provozní parametry modelové ropné rafinerie | |
|---|---|
| **Kapacita atmosférické destilace** | 750 000 tun/rok |
| **Počet primárních zásobníků uhlovodíků** | 6 (4 + 2) |
| **Objem zásobníků ropných produktů** | 4x 25 000 $m^3$ + 2x 50 000 $m^3$ |
| **Způsob zásobování rafinerie ropou** | Ropovod IKL a ropovod Družba |
| **Dopravní obslužnost** | Silniční a železniční doprava |
| **Počet zaměstnanců** | 150 |

Typová rafinerie je zásobována ropovodem IKL i ropovodem Družba. Pro ropné produkty se v areálu rafinerie nachází celkem 6 hlavních nadzemních zásobníků s celkovou kapacitou 200 000 $m^3$, které jsou v konfiguraci 4 nadzemních zásobníků o objemu 25 000 $m^3$ a 2 nadzemních zásobníků s objemem 50 000 $m^3$. Provoz rafinerie zajišťuje 150 zaměstnanců.

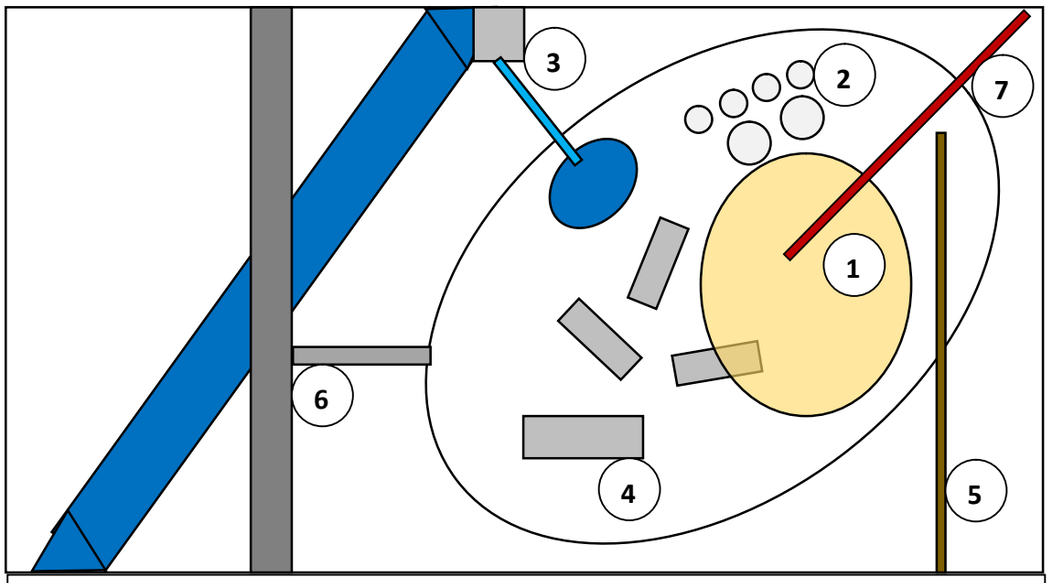
Dopravní obslužnost typové rafinerie obstarává silniční doprava a též napojení na železniční dopravní síť. Do areálu rafinerie je možné zajíždět vlakovými soupravami, pro které je připravena přečerpávací stanice. Vzhledem k velikosti areálu je možné vlakové soupravy odstavit uvnitř střeženého pásma za mechanickými bariérami zabezpečující perimetr areálu.

*Tabulka 3 - Specifikace areálu modelové ropné rafinerie; zdroj: vlastní*

| Specifikace areálu modelové ropné rafinerie | |
|---|---|
| **Rozloha areálu** | 1,44 $km^2$ |
| **Obvod areálu** | 4,5 km |
| **Počet budov** | 4 |
| **Počet osobních vstupů/výstupů** | 2/2 |
| **Počet vjezdů silničních vozidel** | 2 |
| **Počet výjezdů silničních vozidel** | 2 |
| **Počet vjezdů drážních vozidel** | 1 |

Kvůli prostorové náročnosti zpracování ropy je areál rafinerie poměrně rozlehlý. Areál rafinerie zabírá 1,44 $km^2$ a obvod je 4,5 km. Z bezpečnostního hlediska rozlehlý areál představuje určité riziko. Pro zajištění dostatečné úrovně zabezpečení je nutná investice do velkého množství technických prostředků střežení a současně je nutný adekvátní počet bezpečnostních zaměstnanců. Poměrně dlouhé vzdálenosti mezi jednotlivými částmi areálu též prodlužují reakční dobu na detekované narušení bezpečnosti. Větší počet možných cílů narušení bezpečnosti rovněž vyžaduje zvýšený počet zaměstnanců střežících klíčové body. Zásobování elektrickou energií zajišťuje vlastní elektrárna v areálu rafinerie.

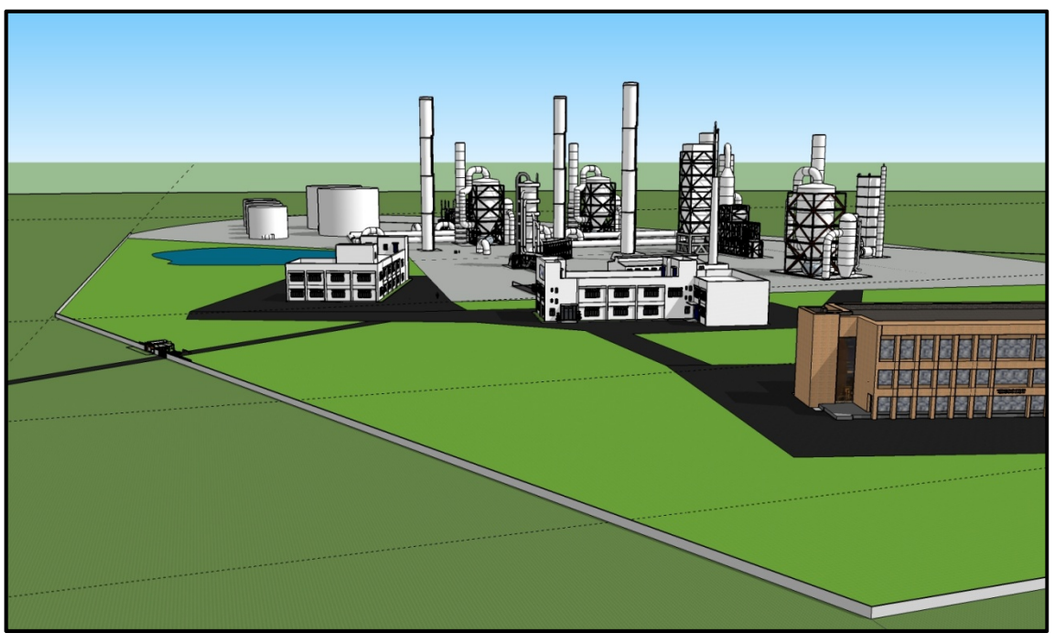
Zaměstnanci rafinerie, případně jiné oprávněné osoby, mohou do objektu vstupovat jedním ze dvou vstupů. Vstupy pro osoby jsou shodné s výstupy. Pro zaměstnance nebo jiné osoby přijíždějící do areálu rafinerie osobním automobilem je vyhrazen samostatný vjezd určený pro osobní automobily, které mohou být odstaveny na vnitřním parkovišti za administrativní budovou. Nákladní automobily vjíždí do areálu samostatným vjezdem. Vyhrazení samostatných vjezdů osobních a nákladních automobilů a výjezdu je realizováno z důvodu zvýšení přehlednosti a bezpečnosti dopravy po areálu a v neposlední řadě z důvodu zvýšení bezpečnosti.




| | | |
|---|---|---|
| 1 – Oblast výrobních technologií | 4 – Administrativní budova | 7 – Produktovod |
| 2 – Zásobníky uhlovodíků | 5 – Železnice | 8 – Elektrárna |
| 3 – Budova vodárny | 6 – Silnice | |

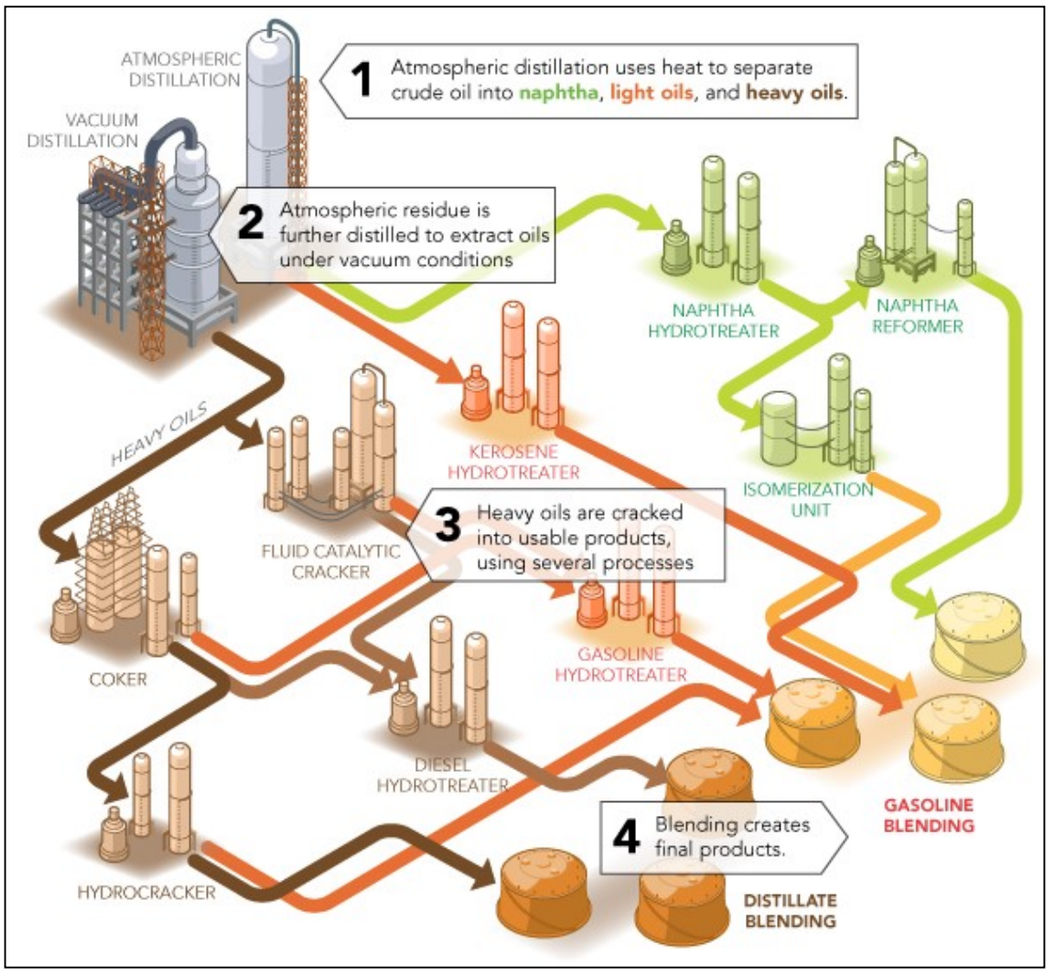
*Obrázek 4 – Ilustrační schéma modelové ropné rafinerie; zdroj: vlastní*

Vlakové soupravy mohou do areálu zajíždět jedním vjezdem, který současně funguje jako výjezd. Možnost odstavení vlakové soupravy po dobu přečerpávání uvnitř areálu eliminuje rizika vyplývající z nutnosti nechat otevřený vjezd.



*Obrázek 5 – Ilustrační model ropné rafinerie; zdroj: vlastní*

Areál ropné rafinerie lze rozdělit na technologickou část, ve které probíhá vlastní rafinace ropy a část s administrativními budovami. Technická a technologická zařízení rafinerie se nacházejí v severní části rafinerie. Vzhledem k posloupnosti technologických procesů (viz následující obrázek) a možnému dominovému efektu je bezpečnost celého technologického procesu pro provoz rafinerie naprosto klíčová. Narušení prakticky libovolného prvku může vyřadit z provozu celou rafinerii.




*Obrázek 6 - Schéma ropné rafinerie; zdroj: free-stock-illustration.com*

Kromě výše uvedených vjezdů silničních vozidel se v areálu nachází dalších 5 vjezdů, které nejsou za běžné činnosti rafinerie používány. Vjezdy slouží primárně pro případ nehody nebo havárie rafinerie, kdy by mohly být využity Hasičských záchranným sborem ČR, za situace, kdy došlo k napadení ropné rafinerie též Policií ČR. Všechny vjezdy jsou uzavřeny ocelovými bránami, které jsou vybaveny detektorem odemčení, který je napojen na pult centralizované ochrany.

# 9 NÁVRH ZABEZPEČENÍ PRVKU KRITICKÉ INFRASTRUKTURY

Navrhovaná opatření využívají prvky bezpečnosti používané v obdobných objektech a areálech. Způsob organizace bezpečnostních opatření a použité technické prvky zabezpečení představují optimální systém ochrany prvku kritické infrastruktury. Reflektující finanční nákladnost pořízení technických prostředků a dlouhodobé náklady spojené s nutností využití odpovídajícího počtu bezpečnostních pracovníků. Nejedná se tudíž o vytvoření maximálně dosažitelného zabezpečení objektu a areálu prvku kritické infrastruktury, neboť taková bezpečnostní opatření a technické prostředky by byly z finančního hlediska (dlouhodobě) nerealizovatelné.

## 9.1 Ochrana perimetru

Prvky zabezpečení perimetru jsou určeny k zabránění, nebo alespoň detekci vniknutí neoprávněných osob do areálu rafinerie. Spadá sem obvodové zabezpečení celého areálu a ochrana vstupů a vjezdů.

*Tabulka 4 – Návrh prvků ochrany perimetru; zdroj: vlastní*

| Návrh prvků ochrany perimetru | |
|---|---|
| **Prvek** | **Množství (ks/m)** |
| **CCTV kamera** | 16 |
| **Kamerový stožár** | 10 |
| **Žiletkový drát** | 4 400 m |
| **Betonová zeď** | 4 200 m |
| **Systém elektronického oplocení** | 4 400 m |

Základním prvkem ochrany perimetru je vybudování dostatečné technické zábrany vstupu do areálu, v tomto případě se jedná o technické opatření ve formě betonové zdi. Zeď je vybudována z betonových dílů o rozměrech 2 m x 0,5 m do výše 2 metrů. Na zdi jsou

instalovány v metrových rozestupech držáky žiletkového drátu, který je umístěn po celém obvodu areálu včetně bran.

Technické prostředky střežení obsahují kamerový dohledový systém a systém elektronického oplocení. Jednotlivé kamery jsou umístěny na kamerových stožárech o výšce 5 metrů. Ve výše uvedené tabulce je zahrnut pouze počet kamer, které jsou přímo zaměřeny na hranici areálu. Na kamerových stožárech jsou současně umístěny kamery snímající vnitřní prostor, které jsou započítány do prvků zabezpečení areálu objektu. Instalované kamery jsou vybaveny zoomem a jejich montáž umožňuje omezený pohyb manuálně řízený operátorem. Každá kamera současně zahrnuje detektor pohybu, který výrazně zvyšuje přehlednost výstupů kamer na dispečerském stanovišti. Při detekci pohybu je zobrazeno upozornění přímo v obraze z dané kamery. Tím může obsluha věnovat zvýšenou pozornost dané oblasti.

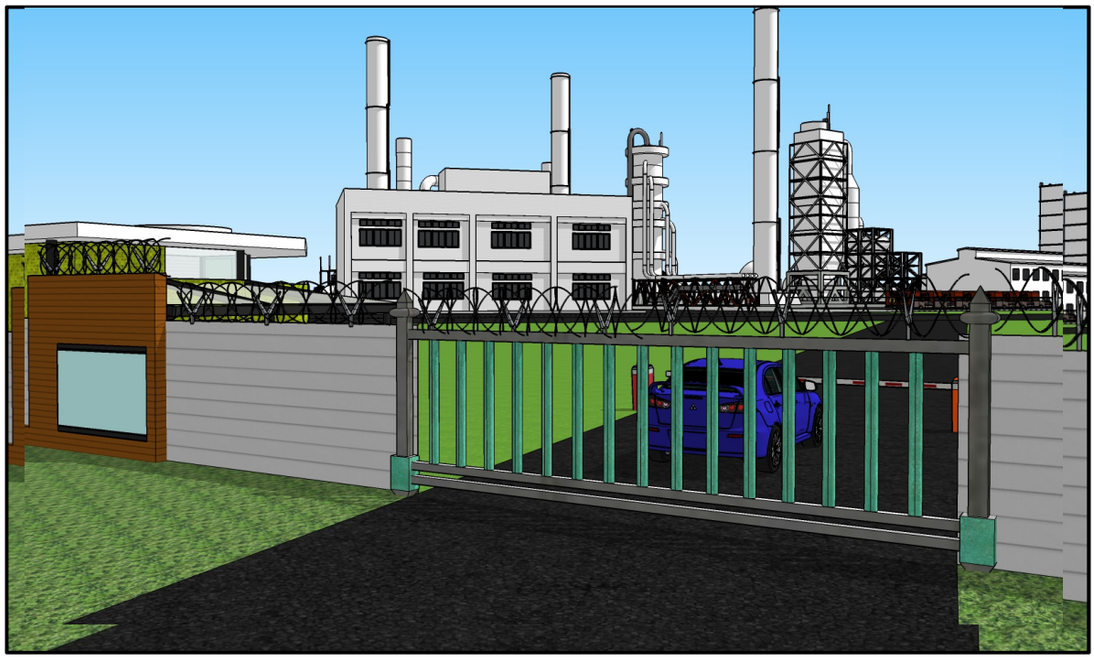
Systém elektronického oplocení ve spojení s žiletkovým drátem detekuje pokusy o překonání mechanické bariéry vstupu. Podstatou činnosti jsou čidla, která detekují pokus o vniknutí do areálu na principu zaznamenání zvýšeného tlaku a tahu na žiletkový drát. Systém elektronického oplocení je vybaven řídícím systémem, který umožňuje přesnou identifikaci místa narušení bezpečnosti.

*Tabulka 5 – Návrh prvků ochrany vstupů do areálu; zdroj: vlastní*

| **Návrh prvků ochrany vstupů/výstupů** | |
|---|---|
| **Prvek** | **Množství (ks)** |
| **CCTV kamera** | 8 |
| **Posuvná brána** | 5 |
| **Závora** | 4 |
| **Elektronická závora** | 4 |
| **Detektor pohybu** | 5 |
| **Turniket** | 4 |

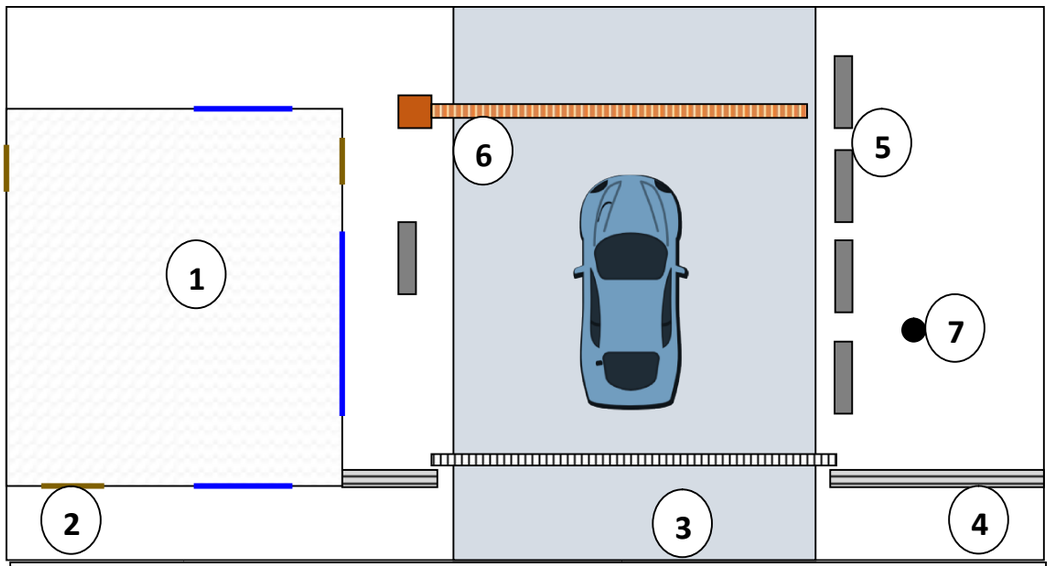
| | |
|---|---|
| **Systém osvětlení** | 3 |
| **Bezpečnostní dveře** | 2 |

Vstupy (shodují se i s výstupy) do areálu jsou realizovány prostřednictvím dvou vrátnic. Dveře vedoucí vně areálu jsou vybaveny bezpečnostními prvky. Pracovníci vstupují do areálu a opouští jej turniketem (v obou vrátnicích jsou umístěny 2), který je vybaven čtečkou zaměstnaneckých karet. Na pohyb osob dohlíží bezpečnostní pracovník. Osoby s povolením vstupu do areálu (např. předem domluvené návštěvy) na vrátnici získají kartu návštěvníka a jsou osobně doprovázeny do cíle jejich cesty.



*Obrázek 7 - Ilustrační model zabezpečení vjezdu; zdroj: vlastní*

Vjezdy jsou mimo pracovní dobu uzavřeny posuvnou bránou s instalovaným prvkem elektronické závory. Funkce elektronické závory spočívá ve vysílání paprsku záření, který je v případě pokusu o přelezení brány přerušen, čímž je detekováno vniknutí do areálu. Během pracovní doby je vstupní brána otevřena, ale vjezd blokuje ve vzdálenosti 7 metrů od brány závora.




| | | |
|---|---|---|
| 1 - Vrátnice | 4 – Zeď | 7 – Stožár kamerového systému |
| 2 - Vstup osob | 5 – Mechanické zábrany | |
| 3 – Brána vjezdu | 6 – Závora vjezdu | |

*Obrázek 8 – Schéma modelového vjezdu do areálu; zdroj: vlastní*

Zaměstnanec může otevřít závoru zaměstnaneckou kartou, ostatní osoby po kontrole získat oprávnění od pracovníka bezpečnosti. Železniční vjezd se otevírá pouze v době příjezdu (odjezdu) předem ohlášených vlakových souprav. Vstupy a vjezdy jsou doplněny systémem dálkově ovládaného nočního osvětlení a detektorů pohybu, které jsou aktivní mimo denní pracovní dobu ropné rafinerie.

## 9.2 Ochrana areálu

Prvky ochran areálu jsou určeny k detekci pohybu neoprávněných osob. Pro eliminaci rizika plynoucího z narušitele je v každém případě nutné využít opatření fyzické ochrany (bezpečnostní pracovníky). Pro pohyb osob nejsou ve většině areálu instalovány mechanické prostředky.

*Tabulka 6 – Návrh prvků ochrany areálu; zdroj: vlastní*

| Návrh prvků ochrany areálu | |
|---|---|
| **Prvek** | **Množství (ks)** |
| **CCTV kamera** | 50 |
| **Kamerový stožár** | 20 |
| **Detektor pohybu** | 200 |
| **Systém osvětlení** | 30 |

Hlavním prvkem zabezpečení areálu jsou CCTV kamery doplněné samostatnými detektory pohybu a systémem nočního osvětlení nepřehledných míst a rizikových bodů (např. přečerpávací stanice nebo ventily zásobníků ropných produktů). Kamery jsou instalovány na 5 metrů vysoké kamerové sloupy, čímž je zajištěno efektivní pokrytí větší oblasti, neboť je možné využívat zoomu kamery. Vzhledem k velikosti střežené oblasti ale kamerový systém nepokrývá celou plochu areálu. Z tohoto důvodu je kamerový systém doplněn sítí samostatných detektorů pohybu, jejichž lokace je zanesena ve virtuální mapě areálu. Při detekci pohybu je obsluha pultu centralizované ochrany přesně upozorněna na pohyb v konkrétní oblasti a lze využít vzdálené ovládání natáčení kamer.

## 9.3 Objektová ochrana

Nejširší škála technických prostředků zabezpečení je využita při ochraně vnitřních prostor budov. Všechny budovy se nachází v blízkosti hlavního stanoviště bezpečnostní sekce, proto je systém technického zabezpečení vnitřních prostor objektu koncipován k jednoznačné identifikaci místa vstupu a pohybu narušitele. Vzhledem k instalovaným bezpečnostním dveřím a okenním mřížím v kombinaci s kamerami a detektory pohybu a výše uvedenou ochranou perimetru a areálu by však hrozba narušitele měla být eliminována ještě před vniknutím do objektu.

*Tabulka 7 – Návrh prvků ochrany objektu; zdroj: vlastní*

| Návrh prvků ochrany objektu | |
|---|---|
| **Prvek** | **Množství (ks)** |
| **CCTV kamera** | 19 |
| **Detektor pohybu** | 50 |
| **Detektor otřesů** | 18 |
| **Detektor tříštění skla** | 80 |
| **Laserová závora** | 9 |
| **Systém osvětlení vchodu** | 10 |
| **Bezpečnostní dveře** | 13 |
| **Okenní mříž** | 40 |

Mechanické bariéry vstupu do objektu tvoří okenní mříže a bezpečnostní dveře. Bezpečnostními dveřmi jsou vybaveny všechny vstupy do budov a dále vstup do centrálního řízení technologických procesů ropné rafinerie, bezpečnostní centrály a serverové místnosti. Vchody jsou dále vybaveny systémem osvětlení reagujícím na pohyb s možností vzdáleného zapnutí. Okenní mříže jsou nainstalovány na oknech v přízemním patře budov. Okna v přízemí a v prvním patře jsou dále vybavena detektory tříštění skla.

K detekci pohybu narušitele uvnitř objektu je využit systém detektorů pohybu v kombinaci s detektory otřesů a, v přístupových oblastech k důležitému vybavení (např. servery) a řídícím místnostem (bezpečnost, technologie výroby), systém laserových závor.

## 9.4 Předmětová ochrana

Prvky této úrovně zabezpečení slouží k ochraně jednotlivých předmětů nacházejících se v chráněném objektu. Patří sem systémy mechanického zabránění odcizení předmětu a technické prvky informující o pohybu předmětu.

*Tabulka 8 – Návrh prvků předmětové ochrany; zdroj: vlastní*

| Návrh prvků předmětové ochrany | |
|---|---|
| **Prvek** | **Množství (ks)** |
| **Velký vestavěný trezor** | 2 |
| **Vestavěná bezpečnostní schránka** | 5 |
| **Mechanický zámek počítače** | 30 |
| **Elektronický lokátor** | 10 |

V administrativní budově rafinerie se nachází dva vestavěné trezory určené k ukládání klíčové dokumentace a jiných zvlášť cenných předmětů a materiálů. Především pro ukládání další důležité dokumentace jsou určeny bezpečnostní schránky, kterých je celkem pět a jsou též zabudovány do zdí budov, aby bylo zabráněno jejich fyzickému odnesení.

K zabránění odcizení počítačů jsou použity mechanické zámky. Jedná se o jednoduchý bezpečnostní prostředek, kdy je principem upevnění počítačové skříně k jinému pevnému předmětu, např. radiátoru. Menší předměty, jako např. laptopy, mohou být vybaveny elektronickým lokátorem. Tento systém spustí alarm při vzdálení předmětu od řídícího prvku a může být použit i mimo objekt, např. při služebních cestách managementu rafinerie.

## 9.5 Fyzické střežení objektu a areálu

Systém fyzického zabezpečení je zcela nenahraditelný technickými nebo mechanickými prostředky ochrany. Bezpečnostní pracovníci dohlíží na technické prvky zabezpečení, zajišťují fyzickou ochranu vstupů a vjezdů do areálu, provádí fyzické pochůzky po areálu a jsou připraveni zakročit proti případnému narušiteli. Přítomnost členů ostrahy současně preventivně působí k odstrašení případného narušitele.

*Tabulka 9 – Návrh systému fyzického střežení areálu a objektů; zdroj: vlastní*

| Návrh systému fyzického střežení areálu a objektů | |
|---|---|
| **Prvek bezpečnosti** | **Množství (ks) / počet zaměstnanců** |
| **Pult centralizované ochrany** | 1 ks |
| **Obsluha pultu centralizované ochrany** | 2 zaměstnanci |
| **Řízení systému zabezpečení** | 1 zaměstnanec |
| **Kontrola vstupu/odchodu osob** | 2 zaměstnanci |
| **Kontrola vjezdu/výjezdu vozidel** | 2 zaměstnanci |
| **Pohotovostní jednotka** | 3 zaměstnanci |
| **Pochůzky po areálu** | 5 zaměstnanců |
| **Ředitel bezpečnostní sekce** | 1 zaměstnanec |
| **Celkový počet zaměstnanců bezpečnosti** | **46** |

Ústředním bodem celého systému zabezpečení je pult centralizované ochrany, jehož obsluhu trvale zajišťují dva bezpečnostní pracovníci. Z pultu centralizované ochrany je možné vzdáleně ovládat kamerový systém a systém osvětlení a jsou do něj svedeny výstupy ze všech instalovaných bezpečnostních systémů, jejichž pozice je zanesena do mapy, což usnadňuje lokalizaci narušitele. Kromě obsluhy pultu centralizované ochrany se v daných prostorách nachází kancelář ředitele bezpečnostní sekce a vedoucího bezpečnostního pracovníka směny, který je zodpovědný za činnost a konkrétní opatření ochrany ropné rafinerie. V sídle bezpečnostní sekce se dále nachází pohotovostní jednotka skládající se ze třech pracovníků, kteří jsou v případě narušení bezpečnosti okamžitě vysláni do míst výskytu pachatele.

Pro kontrolu a ochranu každého ze vstupů a vjezdů a výjezdů je přiřazen vždy jeden bezpečnostní pracovník, celkem 4 zaměstnanci. Jejich úkolem je dohlížet na využívání turniketů zaměstnanci a provádět ověření a kontrolu dalších osob a jejich vozidel, které mají dočasné povolení vstupu (vjezdu) do areálu.

Poslední skupina bezpečnostních zaměstnanců provádí nepravidelné pochůzky po areálu rafinerie s cílem kontroly technických a mechanických prvků zabezpečení (např. poškození zdi, oken, nefunkčnost detektoru atd.) a případnou detekci narušitelů. Jedná se o pět pracovníků, jejichž pochůzky jsou plánovány se zahrnutím oblastí s výrobními, skladovacími či jinými technologiemi a čtyřech budov nacházejících se v areálu. Dále probíhá kontrola zabezpečení perimetru. Pochůzky nejsou náhodné, jejich trasa je předem naplánována, ale současně nejsou ve vztahu k jiným dnům shodné, aby nebylo možné vysledovat pohyb strážných.

Pracovní činnost zaměstnanců v oblasti bezpečnost probíhá na dvě směny. Všichni zaměstnanci (kromě ředitele) se pravidelně střídají po 12 hodinách. V každém okamžiku je tedy v areálu alespoň 15 bezpečnostních pracovníků. Celkový počet bezpečnostních zaměstnanců je 46 (ředitel + 3 x 15 zaměstnanců).

*Tabulka 10 – Návrh a výstroje a výbavy pracovníků ostrahy; zdroj: vlastní*

| **Návrh výstroje a výbavy bezpečnostních pracovníků** | |
|---|---|
| **Prvek bezpečnosti** | **Množství (ks)** |
| **Stejnokroj** | 46 |
| **Boty** | 46 |
| **Vysílačka** | 50 |
| **Obranný sprej** | 100 |
| **Taktická vesta** | 50 |
| **Taktické rukavice** | 100 |
| **Svítilna** | 50 |
| **Paralyzér** | 50 |

Standardní výstroj pracovníka fyzické ostrahy zahrnuje stejnokroj a taktickou vestu pro umístění příslušenství, dva páry taktických rukavic (letní a zimní varianta) přizpůsobených k ovládání zbraně a s protiprořezovou ochranou a pár bot s vyjímatelnou zimní vložkou.

Pracovníci ostrahy jsou vyzbrojeni obranným sprejem a paralyzérem. Dále jsou pracovníci vybaveni vysílačkou a ocelovou vodotěsnou svítilnou.

Paralyzér, svítilna, vesta, rukavice, obranný sprej a vysílačka jsou pořízeny ve zvýšeném počtu pro možnost okamžité výměny.

## 9.6 Odhad finančních nákladů

Při odhadu finančních nákladů instalace technických a mechanických prvků zabezpečení jsou zvoleny ceny komerčně dostupných prvků zabezpečení. Do ceny prvků zabezpečení nejsou započítány náklady za instalaci a zapojení prvku. Vzhledem k velkému množství instalovaných prostředků zabezpečení by pravděpodobně bylo možné dosáhnout výhodnějších cen. Jejich výše je ale závislá na konkrétním dodavateli, vyjednávání a dalších faktorech (např. předchozí zakázky), proto je v kalkulaci počítáno s jednotkovými cenami pro soukromé osoby.

*Tabulka 11 – Odhad ceny technických prvků zabezpečení; zdroj: vlastní s využitím komerčních cen technických prvků zabezpečení*

| Odhad ceny technických prvků zabezpečení | | | |
|---|---|---|---|
| **Prvek** | **Množství** | **Cena za kus/metr** | **Cena celkem** |
| **CCTV kamera** | 85 ks | 8 000 Kč | 680 000 Kč |
| **Systém elektron. oplocení** | 4 400 m | 2 000 Kč | 8 800 000 Kč |
| **Kamerový stožár** | 30 ks | 6 500 Kč | 195 000 Kč |
| **Žiletkový drát** | 4 400 m | 42 Kč | 184 800 Kč |
| **Držák žiletkového drátu** | 440 | 120 Kč | 52 800 Kč |
| **Betonová zeď** | 4 200 m | 1 300 Kč | 5 460 000 Kč |
| **Bezpečnostní dveře** | 15 ks | 30 000 Kč | 450 000 Kč |
| **Posuvná brána** | 5 ks | 60 000 Kč | 300 000 Kč |

| | | | |
|---|---|---|---|
| **Závora** | 4 ks | 100 000 Kč | 400 000 Kč |
| **Detektor pohybu** | 255 ks | 300 Kč | 76 500 Kč |
| **Laserová závora** | 10 ks | 2 500 Kč | 25 000 Kč |
| **Turniket** | 4 ks | 120 000 Kč | 480 000 Kč |
| **Systém osvětlení** | 42 ks | 5 000 Kč | 210 000 Kč |
| **Detektor otřesů** | 15 ks | 400 Kč | 6 000 Kč |
| **Detektor tříštění skla** | 80 ks | 300 Kč | 24 000 Kč |
| **Okenní mříž** | 40 ks | 8 000 Kč | 320 000 Kč |
| **Velký vestavěný trezor** | 2 | 40 000 Kč | 80 000 Kč |
| **Vestavěná bezpeč. schránka** | 5 | 12 000 Kč | 60 000 Kč |
| **Mechanický zámek počítače** | 30 ks | 150 Kč | 4 500 Kč |
| **Elektronický lokátor** | 10 ks | 1 000 Kč | 10 000 Kč |
| **Elektronická závora** | 4 ks | 5 000 Kč | 20 000 Kč |
| **Pult centralizované ochrany** | 1 ks | 7 000 000 Kč | 7 000 000 Kč |
| **Celkem** | | **24 838 600 Kč** | |

Celková částka na instalaci prvků zabezpečení dosahuje 24 838 600 Kč. Nejvyšší podíl na ní mají pult centralizované ochrany, výstavba betonové zdi a systém elektronického oplocení. Náklady na tyto tři prvky zabezpečení přesahují 21 000 000 Kč.

Naopak náklady na senzory jsou poměrně nízké. Náklady na pořízení celé sítě detektorů pohybu činí 76 500 Kč a senzory použité ke střežení vnitřních prostor budov mimo

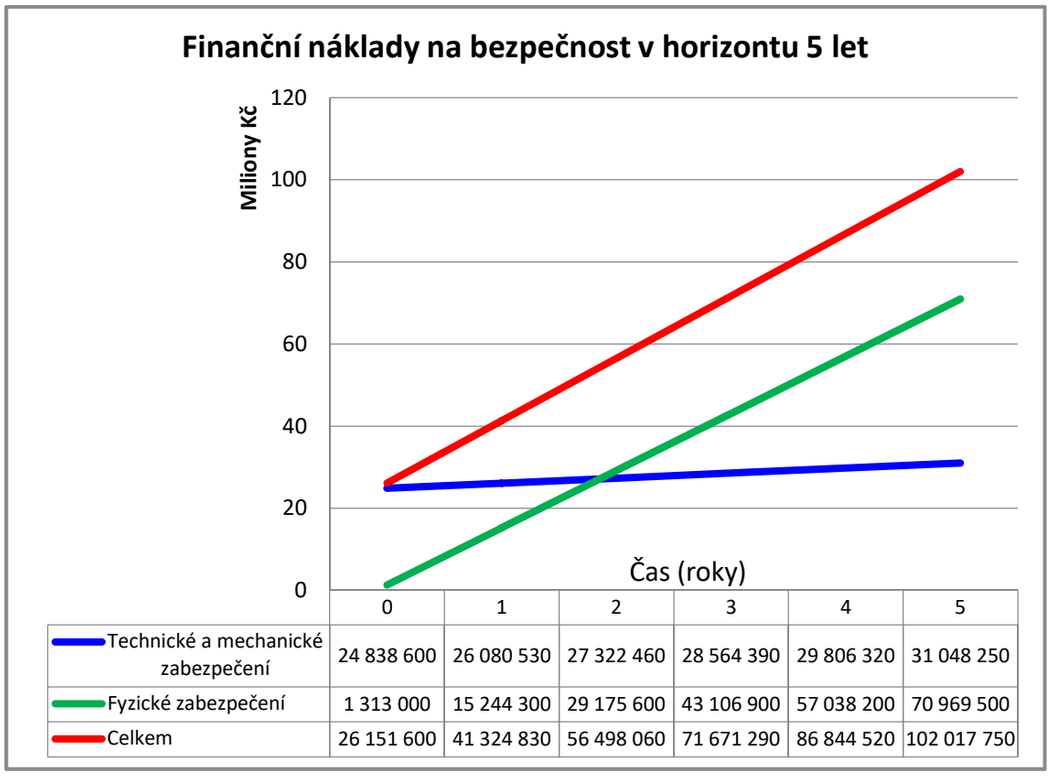
detektory pohybu (laserové závory, detektory tříštění skla, detektory otřesů) vyžadují částku 55 000 Kč.

*Tabulka 12 - Odhad ceny výstroje a výzbroje bezpečnostních pracovníků; zdroj: vlastní s využitím komerčních cen*

| Odhad ceny výstroje a výzbroje bezpečnostních pracovníků | | | |
|---|---|---|---|
| **Výzbroj/výstroj** | **Množství** | **Cena za kus** | **Cena celkem** |
| **Stejnokroj** | 46 | 10 000 Kč | 460 000 Kč |
| **Boty** | 46 | 3 000 Kč | 138 000 Kč |
| **Vysílačka** | 50 | 5 000 Kč | 250 000 Kč |
| **Obranný sprej** | 100 | 300 Kč | 30 000 Kč |
| **Taktická vesta** | 50 | 3 000 Kč | 150 000 Kč |
| **Taktické rukavice** | 100 | 1 000 Kč | 100 000 Kč |
| **Svítilna** | 50 | 7 00 Kč | 35 000 Kč |
| **Paralyzér** | 50 | 3 000 Kč | 150 000 Kč |
| **Celkem** | | **1 313 000 Kč** | |

Počáteční finanční náklady na pořízení výstroje a výzbroje pracovníků zajišťujících bezpečnost prvku kritické infrastruktury jsou 1 313 000 Kč. Do této ceny ovšem nejsou započítány náklady na nutnost výcviku.

Náklady na zajištění fyzického střežení jsou kalkulovány pouze jako součet měsíčních mezd zaměstnanců a náklady na pořízení výstroje a výzbroje. Nejsou zde započítány náklady na školení pracovníků. Při výpočtu je použita průměrná měsíční mzda bezpečnostního pracovníka 25 000 Kč. Roční náklady na mzdy činí 13 800 000 Kč.




| | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| Technické a mechanické zabezpečení | 24 838 600 | 26 080 530 | 27 322 460 | 28 564 390 | 29 806 320 | 31 048 250 |
| Fyzické zabezpečení | 1 313 000 | 15 244 300 | 29 175 600 | 43 106 900 | 57 038 200 | 70 969 500 |
| Celkem | 26 151 600 | 41 324 830 | 56 498 060 | 71 671 290 | 86 844 520 | 102 017 750 |

*Graf 5 – Odhad finančních nákladů na bezpečnost během 5 let; zdroj: vlastní*

V odhadu nákladů na bezpečnost v pětiletém horizontu se počítá s nulovými čistými investicemi do výzbroje a výstroje bezpečnostních pracovníků a technických a mechanických bezpečnostních prvků a obnovovacími investicemi ve výši 5% vstupní investice do technických a mechanických prvků zabezpečení a 10% do výzbroje a výstroje bezpečnostních pracovníků. Během pěti let dosahují celkové náklady na ochranu prvku kritické infrastruktury 102 017 750 Kč, z toho 69 000 000 Kč jsou náklady na mzdy bezpečnostních zaměstnanců. Celkové náklady na fyzické zabezpečení jsou 70 962 500 Kč a více než 31 048 250 Kč jsou náklady na instalaci a provoz technických a mechanických prvků zabezpečení. V horizontu pěti let tedy náklady na fyzickou ochranu dosáhnou více než dvojnásobku nákladů na pořízení a provoz technických prvků střežení.

# 10 ANALÝZA SYSTÉMU ZABEZPEČENÍ

Bezpečnostní systém zpracovaný v předchozí kapitole je určen pro provoz rafinerie za běžné situace. Na zvýšené riziko ohrožení funkčnosti kritické infrastruktury plynoucí z nových nebo do té doby latentních hrozeb jsou v této kapitole navržena adekvátní opatření navýšení zabezpečení. Vzhledem k zaměření diplomové práce na ochranu prvku kritické infrastruktury před fyzickým narušením bezpečnosti nejsou uvažována rizika vyplývající z výskytu živelných pohrom, ekonomická rizika či ochrana před kybernetickými útoky.

## 10.1 Analýza rizik

Tato práce je psaná v době, kdy v Evropě došlo během několika posledních let ke spáchání vysokého počtu teroristických útoků. Jen od ledna 2016 do konce července téhož roku bylo v Evropě spácháno 12 teroristických útoků, které si vyžádaly více než 150 obětí na životech (Indianexpress.com, 2016). Všechny útoky byly spáchány islámskými radikály a cílem útoků byli výhradně civilisté, případně příslušníci ozbrojených sil a ozbrojených bezpečnostních sborů. Z tohoto ovšem nelze usuzovat, že se prvky kritické infrastruktury v budoucnu nestanou terčem závažného teroristického útoku. Jen ve Spojených státech se od roku 1970 do roku 2015 odehrálo 2055 teroristických útoků cílených na kritickou infrastrukturu (Miller, 2016). Nedávné teroristické útoky v Evropě též poukázaly na hrozbu použití nákladního automobilu jako zbraně.

Nové hrozby pro kritickou infrastrukturu vyplývají i z technologického rozvoje. Kromě kybernetické hrozby pro prakticky všechna odvětví kritické infrastruktury představují novou hrozbu též moderní technické prostředky. Klasickým příkladem jsou komerčně dostupné bezpilotní prostředky, které již teroristé využili k přímým útokům (E15.cz, 2016).

Následující analýza rizik pro modelovou ropnou rafinerii je zpracována v softwarovém analytickém nástroji RISKAN. V analýze jsou uvažovány hrozby pro překonání vnější ochrany, hrozby pro modelový prvek kritické infrastruktury a možné cíle útoku.

| HODNOTA AKTIVA | |
|---|---|
| 0 | žádná |
| 1 | velmi nízká |
| 2 | nízká |
| 3 | střední |
| 4 | vysoká |
| 5 | velmi vysoká |

| PRAVDĚPODOBNOST HROZBY | |
|---|---|
| 0 | žádná |
| 1 | zanedbatelná |
| 2 | nízká |
| 3 | střední |
| 4 | vysoká |
| 5 | velmi vysoká |
| 6 | jistá |

| ZRANITELNOST AKTIVA | |
|---|---|
| 0 | žádná |
| 1 | nízká |
| 2 | střední |
| 3 | vysoká |

| VÝSLEDNÉ RIZIKO | |
|---|---|
| Nízké | 0 - 29 |
| Střední | 30 - 59 |
| Vysoké | 60 - 90 |

*Obrázek 9 - Číselníky softwarového nástroje RISKAN; zdroj: Softwarový nástroj RISKAN*

Při kalkulaci byla stanovena hodnota aktiv v rozmezí 0 až 5 (žádná až velmi vysoká), zranitelnost aktiva v rozmezí 0 až 3 (žádná až vysoká) a pravděpodobnost hrozby 0 až 6 (žádná až jistá) a výsledné riziko nabývá hodnot 0 až 90, viz výše přiložený obrázek číselníků.

*Tabulka 13 - Aktiva systému vnějšího zabezpečení ropné rafinerie; zdroj: vlastní*

| Aktiva systému vnějšího zabezpečení ropné rafinerie | |
|---|---|
| **Aktivum** | **Hodnota** |
| **Mechanická ochrana perimetru** | 2 |
| **Vstupy** | 4 |
| **Vjezdy** | 5 |

Možná místa napadení ropné rafinerie z hlediska vnějšího zabezpečení představují vstupy, vjezdy a mechanická ochrana perimetru ve formě betonové zdi, která je navíc vybavena systémem elektronického oplocení. Nejvyšší hodnota je přisouzena vjezdům, které by v případě prolomení zabezpečení umožnily rychlý postup útočníků včetně pohybu po

areálu motorovými vozidly. Naopak betonová zeď představuje vysoký stupeň ochrany, jejíž překonání je poměrně složité a nečekaný, např. bombový, útok by si pravděpodobně nevyžádal oběti na životech.

*Tabulka 14 - Aktiva ropné rafinerie; zdroj: vlastní*

| Aktiva ropné rafinerie | |
|---|---|
| **Aktivum** | **Hodnota** |
| **Zásobníky uhlovodíků** | 5 |
| **Přečerpávací stanice** | 4 |
| **Vnitřní produktovody** | 4 |
| **Řízení výrobních technologií** | 4 |
| **Řízení systému zabezpečení** | 4 |
| **Elektrárna** | 3 |
| **Produktovod** | 4 |
| **Vodárna** | 4 |

Z vytipovaných aktiv ropné rafinerie, která by se mohla stát terčem útoku, se vně vlastního areálu rafinerie nachází objekt vodáren a produktovod. Obě aktiva jsou klíčové pro činnost rafinerie, z hlediska možných bezpečnostních opatření provozovatele jsou obtížně chránitelná, především produktovod.

V areálu rafinerie se nachází zásobníky uhlovodíků, které jsou maximálně rizikovým objektem, neboť jejich poškození následované případným požárem by kromě vyřazení rafinerie z provozu představovalo závažné následky i pro obyvatelstvo. Dalším uvažovaným cílem jsou produktovou uvnitř areálu a přečerpávací stanice. Jejich vyřazení by mělo kritické následky pro činnost ropné rafinerie a mohlo by dojít ke vzniku požáru tvořícího nebezpečné zplodiny hoření. Centrum řízení výrobních technologií a centrum řízení systému zabezpečení (pult centralizované ochrany) jsou dalšími možnými cíli útoku. Bez centrálního řízení rafinerie nemůže pokračovat v činnosti a vyřazení řízení bezpečnosti je závažné z hlediska dalšího následného útoku, případně pokračování útoku, neboť by

koordinace řízení bezpečnosti byla prakticky nemožná. Vyřazení elektrárny, která zásobuje elektrickou energií rafinerii, by pro činnost rafinerie ani systém zabezpečení nemělo představovat kritický problém, automaticky by došlo k napojení na dodávky elektrické energie z veřejné rozvodné sítě. Útok by si ovšem mohl vyžádat oběti pracovníků elektrárny a ostrahy.

*Tabulka 15 - Hrozby; zdroj: vlastní*

| Hrozby | |
|---|---|
| **Hrozba** | **Pravděpodobnost** |
| **Útok ozbrojené skupiny** | 4 |
| **Útok střelou s reaktivním pohonem** | 2 |
| **Bombový útok s pomocí dronu** | 3 |
| **Získání informací pomocí dronu** | 4 |
| **Proražení ochrany perimetru nákladním vozidlem** | 5 |
| **Bombový útok nákladním vozidlem** | 4 |
| **Vyzrazení citlivých informací zaměstnancem** | 5 |
| **Přímý útok zaměstnance** | 3 |

Ve výše uvedené tabulce jsou uvažované hrozby z oblasti fyzického narušení bezpečnosti prvku kritické infrastruktury. Nejvyšší pravděpodobnost je stanovena vyzrazení citlivých informací zaměstnancem (ať již záměrně nebo nezáměrně), které mohou být využity při útoku. Použití nákladního automobilu, jakožto specifické hrozbě pro vnější ochranu areálu, je též přiřazena velmi vysoká pravděpodobnost. Vysoká pravděpodobnost je určena u hrozeb použití nákladního automobilu k bombovému útoku, útoku ozbrojené skupiny a použití dronu k získání informací o struktuře areálu a případných bezpečnostních opatřeních. Z útoku organizované skupiny je, jako specifická hrozba, vyčleněn útok zaměstnance(ů), který má přiřazenu, stejně jako bombový útok s využitím dronu, střední

pravděpodobnost. Útok střelou s reaktivním pohonem by mělo velice závažné následky, ale pravděpodobnost jejího použití je nízká.

*Tabulka 16 - Analýza rizik v softwarovém nástroji RISKAN; zdroj: vlastní s využitím softwarového nástroje*

| RISKAN RIZIKOVÝ KALKULÁTOR T-SOFT | Aktiva | AKTIVA - CELKEM | Zabezpečení typové rafi | Mechanická ochrana per | Vjezdy | Vstupy | Objekty uvnitř areálu | Zásobníky uhlovodíků | Přečerpávací stanice | Vnitřní produktovody | Řízení výrobních technol | Řízení systému zabezpe | Elektrárna | Objekty vně areálu | Produktovod | Vodárna |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Hodnoty aktiv | 5 | 5 | 2 | 5 | 4 | 5 | 5 | 4 | 4 | 4 | 4 | 3 | 4 | 4 | 4 |
| Generátor grafů / Export do XML | | velmi vysoká | velmi vysoká | nízká | velmi vysoká | vysoká | velmi vysoká | velmi vysoká | vysoká | vysoká | vysoká | vysoká | střední | vysoká | vysoká | vysoká |
| Hrozby | Pravděpodobnost | | | | | | | | | | | | | | | |
| HROZBY - CELKEM | 5 velmi vysoká | 75 | 75 | 10 | 75 | 40 | 60 | 60 | 48 | 48 | 40 | 40 | 36 | 48 | 48 | 40 |
| Útok ozbrojené skupiny | 4 vysoká | 60 | 40 | 8 | 40 | 32 | 60 | 60 | 48 | 48 | 32 | 32 | 24 | 48 | 48 | 32 |
| Útok střelou s reaktivním pohonen | 2 nízká | 30 | 8 | 0 | 0 | 8 | 30 | 30 | 8 | 8 | 8 | 8 | 6 | 8 | 8 | 8 |
| Bombový útok s pomocí dronu | 3 střední | 45 | 12 | 0 | 0 | 12 | 45 | 45 | 36 | 36 | 0 | 0 | 18 | 24 | 24 | 24 |
| Získání informací pomocí dronu | 4 vysoká | 40 | 20 | 8 | 20 | 0 | 40 | 40 | 32 | 32 | 0 | 0 | 12 | 16 | 16 | 16 |
| Proražení ochrany perimetru nákla | 5 velmi vysoká | 75 | 75 | 10 | 75 | 20 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Bombový útok nákladním automob | 4 vysoká | 60 | 20 | 0 | 20 | 16 | 60 | 60 | 48 | 48 | 16 | 16 | 36 | 16 | 16 | 16 |
| Vyzrazení citlivých informací zamě | 5 velmi vysoká | 50 | 50 | 10 | 50 | 40 | 50 | 50 | 40 | 40 | 40 | 40 | 30 | 40 | 40 | 40 |
| Přímý útok zaměstnancem | 3 střední | 45 | 15 | 0 | 15 | 12 | 45 | 45 | 24 | 24 | 24 | 24 | 18 | 24 | 24 | 24 |

Ve výše uvedené tabulce jsou uvedena výsledná rizika pro jednotlivá aktiva ropné rafinerie včetně specifických aktiv vnější ochrany areálu.

Z hlediska možností vniknutí narušitelů bezpečnosti do areálu vychází jako nejpravděpodobnější vniknutí prostřednictvím vjezdů pro silniční vozidla. Mechanická ochranná bariéra vstupu na perimetru areálu, která je doplněna žiletkovým drátem a systémem elektronického oplocení, představuje dostatečnou ochranu, jejíž překonání by vyžadovalo delší čas a (nebo) dostatečné technické prostředky. Kontrola na osobních vstupech trvale přítomno obsluhou by útočníky mohla odradit. Za běžného provozu jsou bezpečnostní brány vjezdů otevřeny, což útočníkům umožňuje rychlé vniknutí do areálu. K vniknutí lze navíc použít vozidla umožňující rychlý pohyb po areálu a v tomto případě by k vniknutí do areálu byly téměř jistě využity vjezdy (proražení mechanické ochrany perimetru by bylo reálné, ale z hlediska útočníků značně neefektivní). Uzavření bran vjezdů

do značné míry omezí riziko osobního vniknutí narušitelů, ovšem nákladní automobil brána nemůže zastavit.

Specifická hrozba je únik citlivých informací. Přestože se nejedná o fyzické narušení bezpečnosti, úzce s ním souvisí, neboť díky úniku informací mohou útočníci získat přehled o bezpečnostních opatřeních, technických prostředcích střežení, činnosti fyzické ostrahy a možných cílích, což ve výsledku může rozhodnout o „úspěšnosti“ útoku. Podle rozsahu znalostí vnitřní organizace může tímto způsobem zaměstnanec ohrozit celou rafinerii včetně systému vnější ochrany areálu. Se získáním informací o vnitřní struktuře areálu, lokaci možných cílů, přístupových cest k cíli a částečně bezpečnostních opatřeních souvisí hrozba použití dronu se záznamovým zařízením.

Nejkritičtějším objektem v ropné rafinerii jsou nadzemní zásobníky uhlovodíků. Jejich poškození by mohlo mít zdravotní následky i na civilní obyvatelstvo, v závislosti na vzdušném proudění i v poměrně vzdálených lokalitách. Z tohoto důvodu lze předpokládat, že by se v případě napadení rafinerie stali cílem útoku právě zásobníky uhlovodíků.

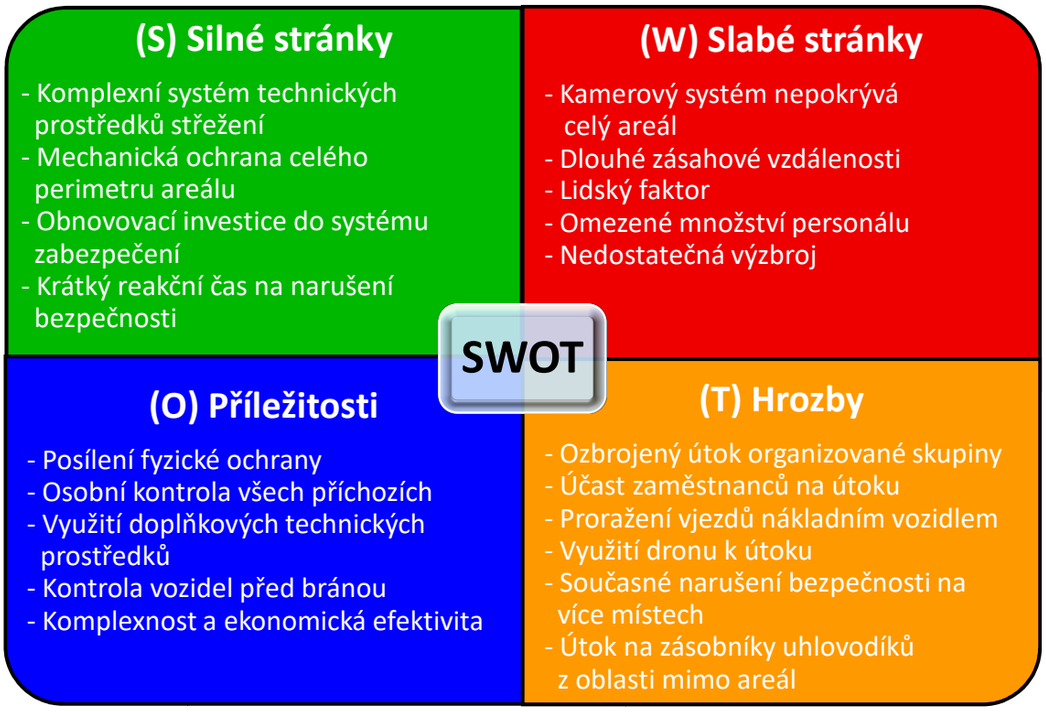
Největší riziko představuje útok ozbrojené skupiny na zásobníky uhlovodíků a útok nákladním automobilem naloženým výbušninami též na zásobníky uhlovodíků. Útok ozbrojené skupiny i nákladní automobil s výbušninami představuje též hrozbu pro ostatní klíčové prvky v areálu rafinerie, zde je riziko nižší především z důvodu existence lákavějšího cíle. Centra řízení bezpečnosti a řízení výrobních technologií jsou navíc proti útoku nákladním automobilem s výbušninami částečně chráněna svoji lokací v suterénu uvnitř budovy a jejich umístěná není z vnějšku zřejmé, což znesnadňuje útočníkovi lokaci cíle.

Hrozby, proti kterým (v současnosti) neexistuje reálná obrana, jsou použití dronu k bombovému útoku a použití střely s reakčním pohonem. Jednoznačně nejpravděpodobnější cíl použití střely jsou zásobníky uhlovodíků, které výrazně převyšují mechanickou ochranu perimetru. Střelu lze použít i k překonání ochrany perimetru nebo jiným cílům, ale zásobníky uhlovodíků se jeví jako dalece pravděpodobnější cíl, na který lze zaútočit i z poměrně velké vzdálenosti od rafinerie. Samotné použití střely s reaktivním pohonem k útoku je ale nízké. Větší pravděpodobnost má útok s využitím dronu k přepravě

výbušného zařízení na cíl. Komerčně běžně dostupné drony mají dostatečnou nosnost, jejich ovládání je jednoduché a v současnosti neexistuje žádná regulace jejich prodeje.

## 10.2 SWOT analýza systému zabezpečení modelového objektu

Pro zajištění možnosti včasného a efektivního zvýšení úrovně zabezpečení prvku kritické infrastruktury je nezbytná perfektní znalost aktuálního systému zabezpečení a to především jeho slabých stránek. Za tímto účelem je v této podkapitole zpracována SWOT analýza systému zabezpečení typové ropné rafinerie. Opatření pro zvýšení úrovně zabezpečení jsou zaměřena na eliminaci hrozeb a slabých míst v bezpečnosti a využívají silných stránek a příležitostí v možnostech zvýšení zabezpečení.




*Obrázek 10 - SWOT analýza zabezpečení typové ropné rafinerie; zdroj: vlastní*

**Silné stránky**

Areál prvku kritické infrastruktury je zabezpečen proti vniknutí nepovolaných osob kompletním systémem mechanických zábran vstupu. Na všech vstupech je trvale přítomen bezpečnostní personál a veškerá přijíždějící vozidla jsou zastavena elektronicky ovládanou závorou. Mimo obvyklou pracovní dobu jsou vjezdy do areálu uzavřeny posuvnou ocelovou

bránou s instalovaným žiletkovým drátem ve svrchní části. Brána železničního vjezdu se otevírá pouze při příjezdu nebo odjezdu železničních souprav, které jsou během přečerpávání ropných produktů uzavřeny v areálu objektu. Z tohoto hlediska není možné do areálu vniknout bez nutnosti překonání mechanických prostředků zabezpečení, které jsou díky pravidelným obnovovacím investicím udržovány v bezvadném stavu.

Další silnou stránkou systému ochrany modelové rafinerie je komplexní systém technických prostředků zabezpečení objektu a areálu. Celý perimetr je pokryt kamerovým systémem a ve vnitřních prostorech areálu jsou kamery doplněny sítí detektorů pohybu. Moderní prostředky zabezpečení jsou také použity uvnitř budov, kde jsou instalovány kromě kamer a detektorů pohybu také laserové závory, detektory tříštění skla a detektory otřesů. Výstupy ze všech technických prvků jsou svedeny na pult centralizované ochrany, díky čemuž je umožněno přehledné sledování činnosti velkého počtu technických prostředků. Stejně jako v případě mechanické ochrany je systém technických prostředků udržován v ideálním funkčním stavu a veškeré závady jsou v nejkratší možné době odstraňovány.

Díky možnosti okamžité a přesné lokalizace místa vniknutí narušitele do areálu a vytvořené pohotovostní jednotce, která je trvale připravena proti narušiteli zasáhnout, je reakční doba na narušení bezpečnosti minimalizována. S využitím systému zabezpečení vnitřního areálu, jenž je koncipován k u umožnění sledování pohybu, je možné zneškodnit pachatele ještě před dosažením jeho cílové lokace.

**Slabé stránky**

Většina slabých stránek bezpečnostního systému pramení z rozlehlosti areálu a limitovaných finančních prostředků vynakládaných na zabezpečení.

Kamerový systém je vytvořen k trvalému dohledu nad perimetrem a dále jsou instalovány kamerové body na klíčových místech areálu. Velikost areálu ovšem znemožňuje reálnou instalaci počtu kamer, které by nepřetržitě snímaly kompletní vnitřní pozemky prvku kritické infrastruktury. Pro kompletní pokrytí by bylo nutné vzhledem k nákladům neúměrně vysoký počet kamerových bodů, což by ovšem současně výrazně zvyšovalo nároky na obsluhu pultu centralizované ochrany a snižovalo přehlednost výstupů z kamer,

případně by bylo nutné úměrně navýšit počet bezpečnostních pracovníků dohlížející na výstupy kamer, což opět zvyšuje náklady.

S velikostí střežené oblasti také souvisí problém s dlouhými zásahovými vzdálenostmi. Stanoviště bezpečnostních zaměstnanců je v administrativní části areálu blízko vstupům a vjezdům do areálu, které jsou vyhodnoceny jako nejpravděpodobnější místo vniknutí narušitele. Do nejvzdálenější části areálu je ovšem zásahová vzdálenost pohotovostní jednotky téměř jeden kilometr. Pět bezpečnostních pracovníků pochůzky rovnoměrně po celém areálu a technický systém zabezpečení umožňuje okamžitou detekci narušení bezpečnosti, ovšem reakce na větší počet narušitelů by vyžadovala odpovídající množství zaměstnanců. Z tohoto hlediska je zásadní míra schopnosti narušitelů eliminovat mechanické zábrany vniknutí, které by měly poskytnout dostatečné množství času k adekvátní reakci na danou hrozbu.

Přestože jsou zaměstnanci v oblasti zajišťování bezpečnosti dostatečně proškoleni a vybaveni odpovídajícími technickými prostředky a jsou vycvičeni k jejich ovládán, do slabých stránek, prakticky jakéhokoliv systému s lidskou účastí, je nutné zařadit lidský faktor. Příkladem může být snížení pozornosti ostrahy vůči dlouholetým zaměstnancům, se kterými se pracovníci ostrahy znají a nepředpokládají od nich žádnou bezpečnostní hrozbu. Dále sem lze zařadit chybná interpretace výstupů z technických prostředků zabezpečení

Pracovníci ostrahy také nejsou za běžné situace vyzbrojeni střelnými zbraněmi. Důvodem je výskyt rizikových materiálů a technologií, které by mohly být použitím střelné zbraně poškozeny, čímž by mohlo dojít k havárii rafinerie. Vyzbrojení bezpečnostního personálu střelnou zbraní též klade na ostrahu zvýšené nároky.

**Příležitosti**

Z hlediska dočasného a rychlého navýšení zabezpečení prvku kritické infrastruktury lze využít zejména organizační úpravu bezpečnostních opatření a dočasné navýšení množství pracovníků zajišťujících ochranu prvku kritické infrastruktury a nasazení doplňkových technických prostředků.

Za běžné situace jsou bezpečnostní opatření nastavena na optimální poměr mezi zabezpečením prvku kritické infrastruktury vůči reálným hrozbám a možností efektivní realizace náplně předmětu činnosti daného prvku kritické infrastruktury, v tomto případě ropné rafinerie. Zvýšené riziko přímého ohrožení prvku kritické infrastruktury je reflektováno v adekvátním posílení bezpečnosti včetně možného dočasného zásahu do plynulosti provozu rafinerie.

Vzhledem k relativní časové náročnosti instalace nových stacionárních technických prostředků střežení a jejich následné implementace do stávajícího systému zabezpečení je vhodnější použít mobilní technické prostředky nezávislé na centrálním ovládání, které poslouží k vykrytí slabých míst. Možné je například nasazení bezpilotních prostředků vybavených dálkovým přenosem obrazu pro snímání areálu z ptačí perspektivy nebo dálkově ovládaných robotických systémů vybavených kamerami a dalšími detektory, např. pohybu nebo tepla.

Z organizačního hlediska lze aplikovat osobní kontroly každé vstupující a odcházející osoby a to včetně zaměstnanců. Kontrolu všech silničních vozidel vjíždějících do areálu je možné provádět před bránou, která se otevře až po prověření a kontrole vozidla oproti běžné kontrole vozidel prováděnou před závorou, která se nachází uvnitř areálu. Pro zajištění dostatečné rychlosti osobních kontrol a kontrol vozidel je nezbytné navýšení bezpečnostních pracovníků provádějících kontroly.

Navýšení bezpečnostního personálu se též odrazí ve zvýšeném počtu osob provádějících pochůzky po areálu. Kromě zvýšeného počtu hlídek lze uvažovat o provádění pochůzek v počtu dvou ozbrojených osob, případně nasazení psovoda. Dále je možná dočasná dislokace vyčleněné pohotovostní jednotky do další části areálu rafinerie, čímž dojde ke zkrácení zásahových vzdáleností a navýšení počtu pracovníků ostrahy v počátečních fázích narušení bezpečnosti.

Aplikace komplexního systému technického zabezpečení v kombinaci s komplementárním systémem fyzického zabezpečení kromě posílení zabezpečení umožňuje též dosahovat ekonomické úspory. Přestože je fyzická ochrana nenahraditelná, moderní technické prostředky (elektronické oplocení, detektory otřesů, laserové závory, autonomní systémy

atd.) umožňují optimalizaci počtu pracovníků ostrahy, což v dlouhodobém horizontu přináší značné úspory, které výrazně přesahují nákupní cenu technických prostředků.

**Hrozby**

Jako hrozba systému ochrany ropné rafinerie je identifikován útok dobře organizované a vyzbrojené skupiny, zapojení zaměstnanců do narušení bezpečnosti, využití těžkého nákladního vozidla k proražení ochrany perimetru, útok s využitím dronu a současné narušení bezpečnosti na několika místech.

Přestože je ostraha vybavena prostředky osobní obrany a vycvičena k jejich použití, dobře organizovaná a vyzbrojená (např. automatickými zbraněmi, výbušninami) skupina by mohla v případě jasného cíle a znalosti postupu ostrahu rychle přemoci. Hlavní problém představuje okamžité přečíslení obránců v konkrétní lokaci a rychlý postup. Hlavní parametr účinnosti obrany by představovala rychlost překonání zabezpečení perimetru, neboť čas na překonání mechanické zábrany umožňuje přesunutí ostrahy do místa útoku a též možný včasný příjezd jednotek Policie ČR.

Značnou hrozbou pro mechanickou ochranu perimetru je využití těžkého nákladního vozidla k proražení ochrany vjezdů do areálu. Ačkoliv je ocelová brána konstruována s ohledem na požadavky bezpečnosti, nebyla by schopna zastavit nákladní vozidlo. Tohoto faktu by bylo možné zneužít v kombinaci s výše uvedeným útokem organizované skupiny, nebo, pokud by bylo naloženo výbušninami, i samostatně.

V závislosti na množství útočníků by mohlo představovat velkou hrozbu současné narušení bezpečnosti na několika místech. Příkladem by mohl být ozbrojený útok větší skupiny, který by na sebe vázal většinu pracovníků ostrahy a následné vniknutí několika dalších osob na opačných stranách areálu. Na tuto hrozbu lze reagovat pouze zvýšeným počtem bezpečnostních zaměstnanců.

Ať už přímé narušení bezpečnosti ze strany zaměstnance nebo poskytnutí informací o prvku kritické infrastruktury, organizaci jeho zabezpečení nebo identifikaci možných cílů zaměstnancem představuje výraznou hrozbu pro bezpečnost. Jako opatření proti pronesení nebezpečných předmětů a materiálu do areálu lze aplikovat zvýšené kontroly

zaměstnanců. Jedinou ochranou proti předání vnitřních informací nepovolaným osobám je ovšem prověřování zaměstnanců před přijetím, systém autorizací zaměstnanců a dostatečná motivace zaměstnanců, která je odradí od nežádoucích akcí. Jedná se tedy, s výjimkou autorizací, o čistě preventivní opatření měkké povahy.

Další významnou hrozbou je využití bezpilotního prostředku k útoku. Komerčně dostupné drony mají v současné době dostatečnou nosnost k umístění výbušného zařízení, případně je lze použít k podrobnému zmapování vnitřních prostor areálu. Kromě toho je možné předem naprogramovat jejich trasu s využitím GPS, takže ani aktivní rušení vzdáleného ovládání není v tomto případě účinné. Proti využití bezpilotních prostředků bohužel zatím neexistuje reálně využitelná adekvátní obrana. Jedná se tedy o poměrně novou hrozbu, která zatím nebyla teroristickými organizacemi (s výjimkou bojišť na Blízkém východě) použita, ovšem zcela jistě je zde přítomná.

Výraznou hrozbou, proti které není areál ropné rafinerie nijak zabezpečen, a z principu útoku ani reálně být nemůže, je útok na zásobníky uhlovodíků z oblasti mimo areál. Pokud by byla například teroristická skupina vybavena střelami s reaktivním pohonem, případně jiným prostředkem dopravy výbušného zařízení na cíl, mohla by tato skupina uskutečnit přímý útok na zásobníky uhlovodíků, které představují jeden z velice rizikových bodů v ropné rafinerii. Vzhledem k výšce zásobníků, která výrazně přesahuje ochrannou zeď chránící perimetr, jediná reálná obrana před takovýmto útokem odhalení plánovaného útoku ještě před samotnou realizací. Neočekávaný útok není možné žádným způsobem zastavit.

# 11 NAVRHOVANÁ OPATŘENÍ KE ZVÝŠENÍ ÚROVNĚ ZABEZPEČENÍ

Tato kapitola pojednává o možných způsobech a opatřeních zvýšení zabezpečení prvku kritické infrastruktury v případě náhlého výskytu hrozeb pro daný prvek kritické infrastruktury. Opatření k posílení zabezpečení ropné rafinerie jsou zpracovány z pohledu provozovatele rafinerie, ovšem na základě smlouvy s Armádou České republiky lze při navyšování úrovně zabezpečení využít armádní síly a prostředky.

Zpracovaná opatření a metody navýšení bezpečnosti předpokládají nutnost bezprostřední reakce na výskyt nové nebo do té doby latentní hrozby. Proto jsou vypracována s ohledem na rychlost jejich integrace do trvalého systému zabezpečení. Vzhledem k zásahům do provozní činnosti ropné rafinerie a výraznému zvýšení finančních prostředků vynakládaných na bezpečnost jsou navrhovaná opatření dočasného charakteru.

Důvodů pro zvýšení bezpečnosti kritické infrastruktury, respektive konkrétní ropné rafinerie, je několik. Jedná se o teroristický útok na obdobnou infrastrukturu v zahraničí, teroristický útok v České republice, pohrůžka teroristickým útokem na území České republiky, vyhrožování útokem na obdobnou infrastrukturu (v ČR i v zahraničí), pohrůžka provozovateli ropné rafinerie a v neposlední řadě informace o možném útoku získané tajnými službami.

## 11.1 Navrhované metody navýšení úrovně zabezpečení

Reakce (nejen) v oblasti bezpečnosti prvku kritické infrastruktury na vyvstanuvší hrozbu musí být okamžitá a přinést reálné posílení zabezpečení. Mechanické prostředky zabezpečení perimetru a komplexní systém technického zabezpečení prvku kritické infrastruktury byly budovány v kontextu naléhavosti hrozby v dlouhém časovém úseku. V krátké době lze začlenit určité množství technických prvku (např. kamerových bodů) do stávajícího systému zabezpečení, ale např. změna konstrukce mechanických zábran nebo přestavba vjezdů do areálu nelze považovat za bezprostřední opatření k navýšení bezpečnosti. Hlavní metody umožňující okamžité zvýšení úrovně zabezpečení představují posílení fyzické ochrany objektu a úprava režimových opatření.

Východiskem pro realizaci všech bezpečnostních opatření je plán krizové připravenosti subjektu kritické infrastruktury, ve kterém jsou definovány hrozby pro prvek kritické infrastruktury a způsob zajištění jeho ochrany. Další významný interní dokument představuje plán reakce na hrozbu prvku kritické infrastruktury, který není definován zákonem, ale je zpracován např. v ropné rafinerii v Kralupech nad Vltavou.

Pro možnost účinné realizace níže uvedených opatření je nezbytné navýšení počtu pracovníků ostrahy. Bez dodatečného personálu by nebylo možné realizovat dodatečná opatření fyzické ochrany, zpřísnění režimových opatření by bylo možné pouze za cenu výrazného navýšení zdržení u vstupů a vjezdů a nově nakoupené technické prostředky též vyžadují lidskou obsluhu.

**Fyzická ochrana**

Navýšení počtu bezpečnostních pracovníků v první řadě umožňuje realizaci činností a opatření, která probíhají i za běžného režimu, ale s výrazně nižší četností a s menším počtem vyčleněných pracovníků a posílení ostrahy vytipovaných rizikových míst (vjezdy, vchody, produktovou, vodárny, zásobníky uhlovodíků, řízení výrobních technologií a bezpečnostního systému).

Za obvyklé situace nepravidelné pochůzky po areálu ropné rafinerie provádí pět pracovníků ostrahy. S výskytem akutních hrozeb pro funkčnost prvku kritické infrastruktury a s tím souvisejícím navýšením počtů bezpečnostních pracovníků je celkový počet přidělených zaměstnanců ostrahy dvojnásobně navýšen.

Kromě pochůzek po areálu jsou další bezpečnostní pracovníci přiřazeni k trvalé ostraze produktovodů, vodárny, zásobníků uhlovodíků a centra řízení provozu rafinerie a jejího zabezpečení. Produktovody vedoucí do rafinerie vedou i mimo areál rafinerie, tudíž je jejich ostraha problematická a jejich poškození by mělo fatální následky na činnost rafinerie. Z tohoto důvodu zaměstnanci bezpečnosti přidělení k jejich ochraně provádí kontrolu i mimo vlastní areál rafinerie. Stejně kritická pro provoz ropné rafinerie je vodárna dodávající vodu pro provoz výrobních technologií, a proto by se mohla stát cílem útoku. Centrum řízení provozu rafinerie a pult centralizované ochrany se nachází v administrativní budově. Cílem navýšení fyzické ochrany je v tomto případě ostraha všech vstupů do

objektu. Z hlediska následků útoku pro obyvatelstvo jsou nejkritičtějším místem zásobníky uhlovodíků, jejichž produkty hoření mohou zasáhnout hustě obydlené oblasti a jejich hašení je značně problematické.

V souvislosti s využíváním technických prostředků střežení pracovníci ostrahy ropné rafinerie pravidelně fyzicky kontrolují stav a činnost všech technických prostředků. Systém technického zabezpečení umožňuje vzdálenou indikaci stavu technického prostředku (v provozu / mimo provoz / detekce narušení bezpečnosti), ale technický prvek lze uvažovat částečné poškození (které může být snadno opravitelné) a akutní hrozbu ztráty funkčnosti nebo poruchu v řídící jednotce systému a nesprávnou indikaci stavu koncového prvku zabezpečení.

*Tabulka 17 - Počty pracovníků zajišťujících posílení fyzické ochrany; zdroj: vlastní*

| Počty pracovníků zajišťující posílení fyzické ochrany | |
|---|---|
| **Opatření** | **Navýšení počet pracovníků** |
| **Pochůzky po areálu** | 5 |
| **Ostraha produktovodů** | 2 |
| **Ostraha vodárny** | 3 |
| **Ostraha zásobníků uhlovodíků** | 4 |
| **Kontrola perimetru** | 3 |
| **Ochrana vstupů** | 4 |
| **Ochrana vjezdů** | 3 |
| **Celkem** | **24** |

**Režimová opatření**

Na vstupech a vjezdech do areálu jsou aplikována zpřísněná režimová opatření. Za tímto účelem je navýšen počet bezpečnostních pracovníků zajišťující ochranu vjezdů a vstupů viz výše uvedená tabulka.

Za běžné situace jsou v běžnou pracovní dobu rafinerie vstupní brány vjezdů silničních vozidel otevřeny a vozidla jsou zastavena elektronicky ovládanou závorou, kterou mohou zaměstnanci s povolením vjezdu otevřít pomocí zaměstnanecké karty. Při zvýšeném riziku útoku dojde k trvalému uzavření vjezdů pro všechna vozidla a všechna přijíždějící vozidla jsou kontrolována před vjezdovou bránou za perimetrem areálu. Současně lze uvažovat o zákazu vjezdu všech vozidel (včetně vozidel zaměstnanců), která nemají zvláštní povolení k vjezdu a jejichž přítomnost v areálu není z hlediska činnosti rafinerie nezbytná. U všech vozidel vjíždějících do areálu se provádí kontrola prostoru posádky a nákladního prostoru z důvodu minimalizace rizika propašování nebezpečných materiálů a předmětů do areálu.

Zpřísněná režimová opatření se též dotknou všech vstupujících osob. Povolení ke vstupu do areálu získají pouze osoby, jejichž vstup je důležitý z hlediska činnosti ropné rafinerie a náplň jejich návštěvy nelze realizovat jiným způsobem. Identifikační údaje osoby s povolením vstupu musí být předem nahlášeny včetně času příchodu a přibližné doby, kdy se v prostorách rafinerie zdrží. Na vstupech jsou poté vstupující osoby prověřeni pracovníkem bezpečnosti včetně kontroly zavazadel, na což jsou ještě před příchodem upozorněny. Kontrola zavazadel se týká též zaměstnanců rafinerie.

Všichni zaměstnanci disponují zaměstnaneckými čipovými kartami, které jim v rámci pohybu po areálu rafinerie umožňují přístup do objektů dle jejich zařazení. Z tohoto důvodu nejsou v této oblasti režimové ochrany zařazena dodatečná opatření.

**Technické prostředky**

K plnění mimořádných opatření jsou bezpečnostní pracovníci dovybaveni mobilními technickými prostředky.

Ke kontrole vstupujících osob jsou určeny ruční detektory kovů, kterými je vybavena ostraha vstupů do areálu. Pro použití v podmínkách snížené viditelnosti jsou pořízeny tři dalekohledy s úpravou pro noční vidění. Nejnákladnější nově pořízený technický prostředek představuje dron s doletem 7 km a výdrží cca 30 minut. Těchto parametrů a vestavěné kamery s bezdrátovým přenosem obrazu ve vysokém rozlišení lze využít při střežení celého perimetru a areálu objektu.

Výrazným přínosem pro zabezpečení prvku kritické infrastruktury v nočních hodinách jsou pokročilé systémy nočního vidění určené pro pracovníky ostrahy provádějící pochůzky po areálu. K detekci narušitele lze též využít mobilní termovize. Pro posílení ochrany a značné zvýšení mobility a modularity systému zabezpečení, především v blízké budoucnosti, je možné použít semiautonomní robotické prostředky. Zásadní problém těchto moderních prostředků střežení je velmi vysoká pořizovací cena, což je do značné míry činí pro provozovatele prvku kritické infrastruktury nedostupnými.

**Odhadované náklady na zvýšení úrovně zabezpečení**

Náklady na posílení zabezpečení modelového prvku kritické infrastruktury jsou 2 034 000 Kč za první měsíc, kdy bylo posíleno zabezpečení. Největší část tvoří náklady na fyzickou ochranu, kdy mzdy bezpečnostních pracovníků dosahují v součtu 1 800 000 Kč měsíčně (dvousměnný provoz) bez započítání nákladů na jejich vybavení. Pořízení dodatečných technických prvků střežení vychází na 234 000 Kč.

*Tabulka 18 - Odhad nákladů na krátkodobé zvýšení úrovně zabezpečen; zdroj: vlastní*

| Odhad nákladů na krátkodobé zvýšení úrovně zabezpečení | | | |
|---|---|---|---|
| **Výzbroj/výstroj** | **Množství** | **Cena za kus** | **Cena celkem** |
| **Ruční detektor kovů** | 10 | 4 000 Kč | 40 000 Kč |
| **Binokulární noční vidění** | 3 | 18 000 Kč | 54 000 Kč |
| **Dron** | 2 | 70 000 Kč | 140 000 Kč |
| **Fyzická ochrana** | **Počet** | **Měsíční mzda** | **Celková mzda za měsíc** |
| Pracovníci ostrahy | 72 | 25 000 Kč | 1 800 000 Kč |
| **Celkem** | | **2 034 000 Kč** | |

S prodlužující se dobou, kdy jsou uplatňována opatření k posílení ochrany prvku kritické infrastruktury, narůstají především náklady na fyzickou ochranu. Při dlouhodobém výskytu hrozeb pro funkčnost prvku kritické infrastruktury by se ovšem muselo přistoupit k dalším

opatřením, např. posílení mechanické ochrany perimetru (úprava vstupů a vjezdů, bariéry proti proražení vjezdu nákladními vozidly atd.).

## 11.2 SWOT analýza posílení zabezpečení

Následující SWOT analýza je zaměřena na výše uvedené opatření posílení ochrany modelového prvku kritické infrastruktury, která jsou aplikovatelná v krátkém časovém úseku, řádově dnech.


*Obrázek 11 - SWOT analýza zvýšené úrovně zabezpečení; zdroj: vlastní*

**Silné stránky**

Silné stránky posílení ochrany modelové ropné rafinerie vyplývají především z navýšení počtů pracovníků ostrahy. Dodatečné bezpečnostní pracovníky lze využít k navýšení fyzické ochrany a zpřísnění režimových opatření na vstupech a vjezdech do areálu.

V oblasti fyzické ochrany je navýšen počet bezpečnostních pracovníků, kteří provádí pochůzky po areálu rafinerie a zároveň jsou pracovníci ostrahy ve zvýšeném počtu nasazeni k trvalému střežení rizikových objektů v areálu rafinerie a v případě vodárny a produktovou

též částečně i mimo vlastní areál rafinerie. Díky tomu jsou nejrizikovější body pod trvalým fyzickým dohledem a ochranou.

Zpřísněná režimová opatření významně snižují riziko pronesení nebezpečných předmětů a materiálů do areálu rafinerie. Až na výjimky kompletní zákaz vjezdu vozidel do areálu minimalizuje riziko použití dopravního prostředku k přepravě např. výbušnin. Stejně jako v případě silničních vozidel je výrazně omezen vstup též osobám, jejichž návštěva není zcela nezbytná. Pro realizaci zpřísněných kontrol všech příchozích jsou pracovníci ostrahy nově vybaveni ručními detektory kovů.

Nové možnosti ostrahy areálu a perimetru přináší nasazení dronu s bezdrátovým přenosem obrazu z vestavěné kamery. Tyto bezpilotní prostředky jsou pořízeny ve dvou kusech z důvodu možnosti okamžitého nasazení i v případě, že jeden z nich je zrovna po nasazení a jeho baterie jsou dobíjeny. Snímání z ptačí perspektivy umožňuje rychlou detekci narušitele a rychlost v kombinaci s doletem dovoluje nasazení i mimo perimetr areálu a rychlé přelety.

**Slabé stránky**

Zásadní slabé stránky systému posílené bezpečnosti vyplývají z problematické, nebo v některých případech prakticky nereálné, obrany před specifickými hrozbami (viz dále uvedená kapitola „Hrozby“). Primární funkce rafinerie je zpracování ropy za účelem komerčního úspěchu provozovatele rafinerie. Z tohoto ohledu nelze pohlížet na rafinerii jako na objekt projektovaný pro případnou obranu před přímým napadením. Systém zabezpečování ochrany je navržen v souladu s běžnou činností rafinerie a opatření okamžité reakce na hrozbu k posílení zabezpečení z tohoto systému vychází a opírají se o něj.

S výše uvedeným souvisí fakt, že veškerá opatření musí respektovat finanční možnosti provozovatele s tím, že se neustále vyvažují náklady na ochranná opatření a možnosti investice finančních prostředků do jiných oblastí, které z ekonomického hlediska mohou dostávat přednost.

**Příležitosti**

V krátkém časovém horizontu bezprostřední reakce na výskyt hrozby není s ohledem na finanční nákladnost bezpečnostních opatření příliš dalších možností, jak zvýšit zabezpečení (nejen) prvku kritické infrastruktury. V závislosti na finančních možnostech provozovatele prvku kritické infrastruktury lze dále zvýšit počet pracovníků ostrahy a pořídit další technické prostředky ve větším množství (např. noktovizor pro každého člena ostrahy).

Z hlediska výrazného posílení fyzické ochrany se nabízí možnost efektivní spolupráce s Armádou ČR. Armáda disponuje vycvičenými profesionály vyzbrojenými automatickými zbraněmi a vybavenými moderními technickými prostředky, které lze využít při bezpečnostních opatřeních. Ke střežení prvku kritické infrastruktury lze též využít síly a prostředky Policie ČR.

Nové metody výcviku pracovníků ostrahy umožní zvýšit efektivitu zákroků proti narušitelům bezpečnosti. Ostraha může být cvičena v boji beze zbraně a v použití střelných zbraní, což souvisí s dovybavením pracovníků ostrahy krátkými střelnými zbraněmi. Dále se nabízí možnost výcviku v oblasti taktiky boje a koordinace zásahu ve vícečlenné jednotce.

Při dlouhodobém výskytu přímých hrozeb pro bezpečnost daného prvku kritické infrastruktury by bylo reálné posílit bezpečnost formou posílení mechanické ochrany vjezdů, zejména s ohledem na zastavení jedoucích nákladních vozidel a posílit systém technických prostředků.

**Hrozby**

Závažné hrozby pro bezpečnost prvku kritické infrastruktury představují použití nákladního automobilu, ozbrojený útok organizované skupiny, použití dronu, útok zpoza perimetru, účast zaměstnanců na útoku a v neposlední řadě též finanční nákladnost posílení ochrany.

Zaměstnanci, kteří by se pokusili do objektu propašovat nebezpečný materiál, by měli být odhaleni zpřísněnými kontrolami na vstupech. Problém ovšem představuje předání citlivých informací útočníkům, neboť z hlediska možných opatření tomuto narušení bezpečnosti prakticky nelze zabránit, výjimku tvoří zachycení předávání informací tajnými službami.

Další hrozbou je i přes zpřísněná bezpečnostní opatření napadení prvku kritické infrastruktury organizovanou skupinou útočníků, která je dobře vyzbrojena a má dostatečné informace o vnitřním uspořádání areálu a objektů, případně i informace o bezpečnostních opatřeních. To by umožnilo rychlý postup útočníků vedoucí k přečíslení ostrahy s možností její rychlé eliminace a následný útok na zvolený cíl v areálu (nebo i mimo areál, např. vodárna, produktovod).

Na možnost použití dronu k útoku není ani v delším časovém horizontu nalézt adekvátní obranu, stejně jako v případě útoku, především, na zásobníky uhlovodíků zpoza perimetru střelou s reakčním pohonem. Pokud se útočníci dostanou do palebné pozice, žádná obrana není realizovatelná a opatření realizovaná provozovatelem rafinerie též nelze aplikovat k zabránění dosažení palebného postavení.

Použití nákladního automobilu k překonání zabezpečení vjezdu je též významnou hrozbou, proti které v bezprostřední reakci na hrozbu pro prvek kritické infrastruktury není možné aplikovat dostatečnou ochranu. Bezpečnostní závory a brány vjezdu nemohou vydržet náraz naloženého nákladního automobilu a použití masivní mechanické překážky vjezdu není možné z důvodu nutnosti nezbytné dopravní obsluhy rafinerie. Během dostatečně dlouhé doby je ovšem možné doplnit ochranu vjezdu o specializované prvky mechanické ochrany, např. vyklápěcí bariéry vjezdu, které jsou konstruovány k zatavení (zničení) nákladních vozidel.

Dodatečná opatření k navýšení úrovně zabezpečení přináší navýšení nákladů bezpečnosti. Nárůst finančních výdajů může v závislosti na aktuální finanční situaci provozovatele prvku kritické infrastruktury představovat i existencionální hrozbu a v každém případě (negativně) ovlivňuje instalaci dalších prostředků střežení a posilování bezpečnosti.

# 12 PREZENTACE VÝSLEDKŮ

V souladu se stanovenými cíli práce byl v předchozích kapitolách vytvořen modelový prvek kritické infrastruktury z oblasti energetiky, ropná rafinerie s kapacitou atmosférické destilace 750 000 tun ročně, a vypracován systém jejího zabezpečení.

Na základě identifikovaných hrozeb a analýzy rizik v softwarovém nástroji RISKAN byl navržen systém komplexního zabezpečení rafinerie pro období bez výskytu přímých hrozeb pro modelovou ropnou rafinerii se zohledněním finančního faktoru bezpečnostních opatření. Ochrana modelového prvku kritické infrastruktury vychází ze systému zabezpečení obdobného prvku kritické infrastruktury. Následně byla navržena možná opatření pro okamžité navýšení úrovně zabezpečení v případě výskytu hrozby pro prvek kritické infrastruktury. K analyzování systému zabezpečení pro běžnou situaci a posílené ochrany modelového prvku kritické infrastruktury byla použita SWOT analýza.

Jádrem navrhovaného systému ochrany modelového prvku kritické infrastruktury je efektivní mechanická ochrana perimetru se systémem moderních technických prostředků střežení (systém elektronického oplocení, laserové závory, kamerový systém, detektory otřesů, pohybu a tříštění skla) doplněná režimovými opatřeními a systémem fyzické ochrany, která je pro zajišťování bezpečnosti nenahraditelná. Pro okamžité posílení zabezpečení lze především aplikovat posílení fyzické ochrany navýšením počtu pracovníků ostrahy a s tím související částečnou organizační úpravou a zpřísněním režimových opatření. V oblasti technických prostředků je navrženo dovybavení bezpečnostních zaměstnanců mobilními technickými prostředky (dalekohledy s úpravou pro noční vidění, drony vybavené kamerami, ruční detektory kovů). V závislosti na finančních možnostech provozovatele prvku kritické infrastruktury lze též uvažovat o nasazení robotických prostředků střežení, termovizí a dalších pokročilých systémů, jejich pořízení je ovšem finančně velmi nákladné.

Protiopatření vůči použití nákladního vozidla k útoku vyžadují implementaci mechanických prvků ochrany do struktury vjezdů do areálu, kterou lze realizovat v delším časovém horizontu. Ochranná opatření proti útoku dronem v současné době nejsou reálně proveditelná, zde je nutná legislativní úprava provozu dronů a technický pokrok ve vývoji

prostředků k jejich zneškodnění. Z problematiky ochrany prvku kritické infrastruktury vůči určitým hrozbám vyplývá nutnost vytváření ochranných zón a ochranných pásem v okolí prvku kritické infrastruktury, které by poskytly dodatečnou vrstvu ochrany.

## 12.1 Vyhodnocení cílů práce

První stanovený cíl spočíval ve vytvoření nástinu metod zajišťování objektové bezpečnosti. Tohoto cíle bylo dosaženo v kapitole 6, kde byly nastíněny způsoby realizace mechanické, technické a fyzické ochrany a režimových opatření.

Další cíl, vytvoření modelového prvku kritické infrastruktury, byl naplněn v kapitole 9. Vytvořena byla modelová ropná rafinerie o kapacitě atmosférické destilace 750 000 tun ročně.

V následující kapitole, číslo 10, byl vytvořen systém komplexního zabezpečení modelového prvku kritické infrastruktury. Podkladem byl způsob zabezpečení obdobných prvků kritické infrastruktury a aktuální přístup k objektové bezpečnosti. Systém zabezpečení využívá síť moderních technických prostředků střežení, fyzické ochrany a režimových opatření. V rámci komplexního systému zabezpečení jsou též zpracovány metody předmětové ochrany. Navržením systému zabezpečení byl splněn třetí cíl diplomové práce.

Čtvrtého cíle bylo dosaženo v kapitole 11, ve které byla zpracována analýza rizik modelového ropné rafinerie v softwarovém nástroji RISKAN. Největší riziko představuje použití nákladního automobilu k útoku a útok ozbrojené skupiny. Dále v této kapitole byla zpracována SWOT analýza systému zabezpečení modelového prvku kritické infrastruktury.

Na základě analýzy rizik a SWOT analýzy systému zabezpečení modelového prvku kritické infrastruktury byly v kapitole 12 navrženy možná opatření pro zvýšení úrovně zabezpečení. Jako okamžitá reakce na výskyt přímých hrozeb pro prvek kritické infrastruktury je navrženo posílení fyzické ochrany, zpřísnění režimových opatření a dovybavení pracovníků ostrahy mobilním technickými prostředky. Tímto byl splněn poslední cíl práce.

Na základě výše uvedeného lze konstatovat, že všechny stanovené cíle této diplomové práce byly naplněny.

# 13 DISKUZE

V této diplomové práci byla zpracována problematika ochrany kritické infrastruktury proti fyzickému narušení bezpečnosti. Oblast zajišťování bezpečnosti kritické infrastruktury je v rámci celé Evropské unie pokryta především Evropským programem na ochranu kritické infrastruktury, jehož prvky jsou implementovány na národní úrovni jednotlivých členských států Unie.

Během posledních let se v Evropě odehrálo velké množství teroristických útoků. Přestože se České republice zatím vyhnuly, nelze z toho usuzovat, že se tak bude dít i nadále. Jak uvádí J. Kyncl (2014), Česká republika se asi nestane primárním cílem teroristických organizací nebo jimi inspirovaných jednotlivců, ovšem vzhledem k zapojení do mezinárodního boje proti terorismu nelze hrozbu útoku na našem území podcenit. Současně není možné tvrdit, že by případný útok nebyl cílen na kritickou infrastrukturu z důvodu, že předchozí útoky byly zaměřeny na civilní obyvatelstvo a příslušníky ozbrojených sil a bezpečnostních sborů. Jen ve Spojených státech se od roku 1970 do roku 2015 odehrálo teroristických útoků, jejichž cílem byla kritická infrastruktury (Miller, 2016). Nutné je ovšem podotknout, že naprostá většina z nich se odehrála před rokem 2000, ale i jediný úspěšně realizovaný útok může napáchat obrovské škody. Následky narušení funkce jednoho prvku kritické infrastruktury mohou kaskádu dalších událostí, jejich analýza je komplikovaná vzhledem k propojení prakticky všech sektorů průmyslu, služeb i veřejné správy (Zio, 2016).

K ochraně kritické infrastruktury je nutné přistupovat komplexně, vzhledem k množství hrozeb a jejich dynamice se nelze zaměřit na vytvoření špičkové ochrany, která je účinná jen proti jedné nebo několika málo hrozbám (Zio E., Piccinelli R., Sansavini G. (2011). Pro účely návrhu bezpečnostních opatření a systému zabezpečení v praktické části práce byl vytvořen modelový prvek kritické infrastruktury, jehož předlohou byla ropná rafinerie zpracovávající přibližně 3,3 milionu tun ropy ročně. Návrh systému zabezpečení prakticky aplikuje obecné způsoby zajišťování objektové bezpečnosti zpracované v kapitole číslo 5. Navrhovaný systém zabezpečení reflektuje reálný systém zabezpečení obdobného prvku kritické infrastruktury včetně finanční stránky ochranných opatření se zapracováním moderních technických prostředků střežení.

Vytvořený modelový systém zabezpečení lze rozdělit na opatření k ochraně perimetru, zabezpečení areálu, systém fyzického střežení, režimová opatření, ochranu objektů uvnitř areálu a dále jsou uvedena možné způsoby předmětové ochrany. Ochrana perimetru primárně spočívá ve vybudované mechanické bariéře vniknutí ve formě betonové zdi s instalovaným žiletkovým drátem, který je ovšem součástí jednoho z nejmodernějších technických prostředků střežení – systému elektronického oplocení. Systém umožňuje identifikaci přesného místa pokusu o vniknutí do areálu, a jak uvádí Kyncl (2014), je velice odolný vůči možným způsobům narušení činnosti detektorů včetně elektromagnetického rušení. Ochrana perimetru je dále doplněna kamerovými stožáry umístěnými v rizikových místech a fyzickou kontrolou perimetru včetně kontroly funkčnosti technických prostředků. Vchody osob jsou zabezpečeny režimovými opatřeními umožňujícími vstup zaměstnanců na čipovou kartu a pro vstup ostatních osob je nutné předem získané oprávnění. Na efektivní realizaci režimových opatření dohlíží pracovníci ostrahy. Slabinu v systému zabezpečení představují vjezdy pro silniční vozidla. Během pracovní doby jsou za běžné situace bezpečnostní brány trvale otevřeny a vjezdu vozidla brání padací závora, která ovšem nepředstavuje žádnou skutečnou překážku, pokud by ji řidič vozidla chtěl prorazit. Proti neočekávanému útoku s využitím vozidla je vjezd prakticky nechráněn. Oblast organizačních opatření ovšem nelze pro dlouhodobé nasazení příliš vylepšit, neboť by tím vzhledem k vysokému počtu přijíždějících a odjíždějících nákladních vozidel došlo k výraznému zásahu do činnosti ropné rafinerie omezující její provoz.

Vzhledem k rozloze areálu je zde koncentrace prvků zabezpečení nižší. Zabezpečení je tvořeno kamerovým systémem, přičemž kamerové body se nachází v oblastech výrobních technologií, přístupových cestách v areálu, zásobníků uhlovodíků a dalších vytipovaných místech. Vyšší počet kamer by kromě vysokých nákladů též způsoboval, z důvodu příliš vysokého množství obrazů z kamer, zhoršení vyhodnocovací schopnosti obsluhy pultu centralizované ochrany, kam jsou výstupy kamer svedeny. Kamerový systém je dále doplněn sítí detektorů pohybu, které v případě detekce pohybu oznámí přesnou lokaci místa potenciálního narušení bezpečnosti. Technické prvky zabezpečení jsou posíleny fyzickou ochranou areálu, která je zde zcela nenahraditelná, protože systém technického zabezpečení pouze detekuje narušení bezpečnosti, ale pohyb narušitelů nijak nemůže zastavit ani zpomalit, s výjimkou preventivního odstrašení případných útočníků, kteří si budou vědomi nemožnosti nepozorovaného pohybu. Protože je areál modelové rafinerie

rozlehlý, projevuje se slabá stránka fyzické ochrany představovaná relativně nízkým počtem bezpečnostních pracovníků. Velký areál znamená dlouhé zásahové vzdálenosti, takže i přes okamžitou detekci vniknutí v závislosti na konkrétní lokaci může trvat nasazení dostatečného počtu pracovníků ostrahy poměrně dlouhou dobu. K posílení fyzické ochrany by mohla být použita např. další zásahová skupina ostrahy, která by byla dislokována na druhé straně areálu, než je první zásahová skupina. Další možnost zkvalitnění fyzické ochrany je aplikace výcviku bezpečnostních pracovníků v oblasti taktiky boje, koordinace nebo bojových umění a použití zbraně.

Ochrana budov v areálu spočívá v instalaci mechanických zábran vstupu ve formě okenních mříží ve spodních patrech a bezpečnostních dveří a dále technických prostředků jako jsou laserové závory, detektory pohybu, detektory otřesů a detektory tříštění skla. Z hlediska možného cíle útoku na ropnou rafinerii se ale lze domnívat, že pravděpodobný cíl bude mimo budovy v oblasti výrobních technologií a zásobníků uhlovodíků, případně produktovodů. Ochrana produktovodů je ovšem komplikovaná už jenom kvůli jejich lokaci mimo areál provozovatele prvku kritické infrastruktury.

Pro analýzu systému zabezpečení modelové ropné rafinerie byla využita SWOT analýza a dále byla zpracována analýza rizik v programu RISKAN. Největší identifikované riziko představuje útok ozbrojené skupiny a použití nákladního automobilu. Další významnou hrozbou je použití dronu k dopravě výbušného zařízení na cíl v areálu rafinerie.

Na základě analýzy rizik byly identifikovány jako výrazné bezpečnostní riziko vjezdy pro silniční vozidla, jak již bylo uvedeno výše. V případě výskytu akutních hrozeb pro prvek kritické infrastruktury a na to navazující nutnosti okamžitého zvýšení zabezpečení je jejich zabezpečení značně problematické. Uzavření vjezdových bran a kontrola vozidel před branami nejsou dostatečnými opatřeními k minimalizaci rizika, nákladní automobil bez větší potíží bránu prorazí. Jak ukázal německý crashtest betonových zátarasů, které byly instalovány jako reakce na teroristické útoky s využitím nákladních vozidel jako zbraně, ani ty nejsou příliš účinné (rt.com, 2017). Jediné řešení tedy představuje zabudování mechanických zdvižných zábran, které jsou přímo určeny k zastavení rozjetého naloženého nákladního vozidla. Toto opatření ale vyžaduje delší čas na realizaci a značné finanční prostředky, proto jej za bezprostřední opatření reakce na hrozbu nelze považovat.

Proti hrozbě použití dronu k útoku nelze v současné době aplikovat žádná efektivní ochranná opatření. Problematiku dronů by bylo vhodné právně ukotvit, neboť se na ně v současnosti nevztahuje žádný právně závazný dokument. Díky tomu by bylo například možné vytvoření bezletových zón pro drony nebo jiná opatření omezující jejich provoz v rizikových oblastech. Kromě toho je též nezbytné sledovat technický pokrok, kdy jsou v současné době vyvíjeny zbraně speciálně určené pro boj proti dronům, např. elektromagnetická „puška“ určená k jejich sestřelování, která je již ve fázi testování (Paganini, 2015).

Na základě výsledků práce lze konstatovat, že navýšení zabezpečení prvku kritické infrastruktury vlastními prostředky provozovatele je značně problematické. Na nové hrozby, ačkoliv nemusí být pro prvek kritické infrastruktury v daném momentě aktuální, je nutné se připravovat dlouhodobě a dynamicky reagovat na proměny bezpečnostní situace. Vytvoření systému zabezpečení prvku kritické infrastruktury, který je schopen efektivně čelit většině reálných hrozeb, představuje výzvu, ke které je nutné se postavit čelem. K problematice je nutné přistupovat komplexně, od legislativního procesu umožňujícího ve výsledku tvorbu ochranných pásem či získávání dotací na zabezpečení, přes aplikaci moderních prostředků a přístupů střežení a spolupráci mezi provozovatelem prvku kritické infrastruktury s policií a armádou po mezinárodní, ideálně globální, spolupráci a výměnu informací a zkušeností s ochranou kritické infrastruktury.

# 14 ZÁVĚR

Cílem praktické části této diplomové práce bylo vytvořit modelový prvek kritické infrastruktury, zpracovat systém zabezpečení modelového prvku kritické infrastruktury pro běžný stav bez výskytu přímých hrozeb a na základě analýzy rizik a SWOT analýzy navrhnout opatření pro okamžité zvýšení úrovně zabezpečení.

Navrhovaný komplexní systém zabezpečení zpracovaný pro modelový prvek kritické infrastruktury reflektuje finanční aspekty ochrany objektu a je založen na reálném systému ochrany obdobného prvku kritické infrastruktury – ropné rafinerie. Systém zabezpečení navržený v následující kapitole reflektuje nutnost zajištění ochrany prvku kritické infrastruktury v kontextu reálných finančních možností a bez výrazných zásahů do optimálního provozu ropné rafinerie. Základem je síť moderních technických prostředků střežení doplněných systémem fyzické ochrany. Fyzická ochrana představuje z finančního hlediska oblast, u které se dá očekávat snaha provozovatele prvku kritické infrastruktury o úspory. Podle odhadu nákladů zpracovaných v této práci se ukazuje, že během pěti let dosáhly náklady na fyzickou ochranu objektu více než dvojnásobku nákladů na pořízení a provoz technických prostředků střežení. Nutné je ovšem zdůraznit, že fyzická ostraha je zcela nenahraditelná, nízký počet bezpečnostních pracovníků může představovat bezpečnostní riziko.

Analýza rizik při zvýšeném ohrožení prvku kritické infrastruktury byla zpracována v softwarovém nástroji RISKAN. Dále byla použita SWOT analýza zabezpečení prvku kritické infrastruktury. Na základě analýz byly identifikovány jako nejvýznamnější hrozby použití nákladního automobilu k překonání mechanických bariér vstupu, útok ozbrojené skupiny, podíl zaměstnanců na útoku, využití dronu a použití nákladního automobilu naloženého výbušninami. Nejkritičtější bod systému ochrany prvku kritické infrastruktury byly identifikovány vjezdy pro silniční vozidla.

Navrhovaná opatření zvýšení úrovně zabezpečení spočívají v dočasném navýšení zaměstnanců ostrahy, použití dodatečných mobilních technických prostředků zabezpečení a úpravě organizace bezpečnostních opatření při zajišťování ochrany perimetru. Do budoucna je ovšem nezbytné zohlednit nové hrozby jako jsou drony, proti kterým zatím

není efektivní obrana. Současně je doporučeno navýšit připravenost prvku kritické infrastruktury čelit hrozbám formou zabudování mechanické ochrany odolné vůči nákladním automobilům, vytvořením ochranných pásem a legislativní úpravou provozu dronů. Jedná se ovšem o opatření vyžadujících delší čas na realizaci.

# 15 ZDROJE

[1] 2016 Cyber Attacks Statistics. Hackmageddon.com [online]. 2017 [cit. 2017-04-24]. Dostupné z: http://www.hackmageddon.com/2017/01/19/2016-cyber-attacks-statistics/

[2] ARADAU, Claudia. Security That Matters: Critical Infrastructure and Objects of Protection. *Security Dialogue* [online]. 2010, **41**(5), 491-514 [cit. 2017-02-19]. DOI: 10.1177/0967010610382687. ISSN 0967-0106. Dostupné z: http://journals.sagepub.com/doi/10.1177/0967010610382687

[3] BRABEC, František. *Bezpečnost pro firmu, úřad, občana*. Praha: Public History, 2001. ISBN 80-86445-04-6.

[4] BROWN Kathi Ann a foreword by John A. MCCARTHY. *Critical Path: A Brief History of Critical Infrastructure Protection in the United States*. Fairfax, Va: Spectrum Pub. Group, 2006. ISBN 9780913969069.

[5] CABRERA, Ed. Protecting Critical Infrastructure From Cyberattack. *Risk Management* [online]. 2016 [cit. 2017-04-24]. Dostupné z: http://www.rmmagazine.com/2016/10/03/protecting-critical-infrastructure-from-cyberattack/

[6] Can concrete barriers protect against truck attacks? Germans stage crash test to find out (VIDEO). *RT.com* [online]. 2017 [cit. 2017-05-13]. Dostupné z: https://www.rt.com/news/384461-truck-attacks-concrete-test/

[7] COLLINS, Danny a MARK HODGE. TWO YEARS OF TERROR How Europe became a continent in crisis after hundreds of victims were killed in 24 terror attacks: Killing of Catholic priest on church's altar is the latest in a growing list of sickening atrocities. *The Sun* [online]. [cit. 2017-04-09]. Dostupné z: https://www.thesun.co.uk/news/1506287/how-europe-became-a-continent-in-crisis-after-395-victims-were-killed-in-23-terror-attacks-over-24-months/

[8] Cyber-physical attacks: Hacking a chemical plant. *NetworkWorld.com* [online]. 2015 [cit. 2017-04-23]. Dostupné z: http://www.networkworld.com/article/2968432/microsoft-subnet/cyber-physical-attacks-hacking-a-chemical-plant.html

[9] DE BRUIJNE, Mark a Michel VAN EETEN. Systems that Should Have Failed: Critical Infrastructure Protection in an Institutionally Fragmented Environment. *Journal of Contingencies and Crisis Management* [online]. 2007, **15**(1), 18-29 [cit. 2017-02-19]. DOI: 10.1111/j.1468-5973.2007.00501.x. ISSN 0966-0879. Dostupné z: http://doi.wiley.com/10.1111/j.1468-5973.2007.00501.x

[10] Evropský program na ochranu kritické infrastruktury (European Programme for Critical Infrastructure Protection). *Hasičský záchranný sbor České republiky* [online]. Nedatováno [cit. 2017-04-22]. Dostupné z: http://www.hzscr.cz/clanek/evropsky-program-na-ochranu-kriticke-infrastruktury-european-programme-for-critical-infrastructure-protection.aspx

[11] EUR-Lex - l33260 - EN: Evropský program na ochranu kritické infrastruktury. *EUR-Lex* [online]. 2010 [cit. 2017-02-17]. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=URISERV%3Al33260

[12] FREUDENRICH, Craig. How Oil Refining Works. *SCIENCE: HOW STUFF WORKS* [online]. nedatováno [cit. 2017-04-29]. Dostupné z: http://science.howstuffworks.com/environmental/energy/oil-refining.htm

[13] GROLL, ELIAS. Did Russia Knock Out Ukraine's Power Grid? *Foreign Policy* [online]. 2016 [cit. 2017-04-23]. Dostupné z: http://foreignpolicy.com/2016/01/08/did-russia-knock-out-ukraines-power-grid/

[14] HOMRIGHAUS, Henry L. *A primer on electronic security for schools, universities, & institutions*. Bloomington, Ind.: AuthorHouse, c2006. ISBN 1420876635.

[15] IVANKA, Ján. *Mechanické zábranné systémy*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2010. ISBN 978-80-7318-910-5.

[16] JOHN, Miloslav. *Československé letectvo v roce 1938*. Praha: Baroko & Fox, 1996. ISBN 8085642212.

[17] *Komplexní strategie ČR k řešení problematiky kritické infrastruktury (2010)*

[18] KOVAŘÍK, J., *Kritická infrastruktura a ochrana obyvatelstva*, In: Ochrana obyvatel, 2007, Ochrana kritické infrastruktury, s. 145-152, ISBN: 80-86634-51-5

[19] Kritická infrastruktura. *Hasičský záchranný sbor České republiky* [online]. 2017 [cit. 2017-02-17]. Dostupné z: http://www.hzscr.cz/clanek/web-krizove-rizeni-a-cnp-kriticka-infrastruktura-kriticka-infrastruktura.aspx

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

[21] KYNCL, Jaromír. *Bezpečnost objektu ve světle moderních technologií*. Praha: Komora podniků komerční bezpečnosti České republiky, 2014. ISBN 978-80-260-7115-0.

[22] LAUCKÝ, Vladimír. *Technologie komerční bezpečnosti II*. Vyd. 2. Zlín: Univerzita Tomáše Bati ve Zlíně, 2007. ISBN 978-80-7318-631-9.

[23] LAZARI, Alessandro. *European critical infrastructure protection*. 2014. Firenze: Springer. ISBN 9783319074962.

[24] List of terrorist attacks that have struck Europe in 2016: A list of deadly terror attacks carried out in European countries since January this year. *Indianexpress.com* [online]. 2016 [cit. 2017-05-11]. Dostupné z: http://indianexpress.com/article/world/world-news/

[25] MACAULAY, Tyson. *Critical Infrastructure Understanding Its Component Parts, Vulnerabilities, Operating Risks, and Interdependencies*. Hoboken: Taylor & Francis, 2008. ISBN 9781420068368.

[26] MACH, Vlastimil. Zisťovanie prielomovej odolnosti mechanických zábranných prostriedkov obvodovej a predmetovej ochrany. *Security Revue: International magazine for security engineering* [online]. 2012 [cit. 2017-02-26]. Dostupné z: http://www.securityrevue.com/article/2012/10/zistovanie-prielomovej-odolnosti-mechanickych-zabrannych-prostriedkov-obvodovej-a-predmetovej-ochrany/

[27] MARTELLINI, Maurizio. *Cyber Security Deterrence and IT Protection for Critical Infrastructures*. Cham: Springer, 2013. ISBN 9783319022796.

[28] MATCHETT, Alan R. *CCTV for security professionals*. Boston: Butterworth-Heinemann, c2003. ISBN 0750673036.

[29] MEAD, Nancy R. Cyber Security Engineering: A Practical Approach For Systems And Software Assurance. ISBN 9780134189802.

[30] MILLER, Erin. *Terrorist Attacks Targeting Critical Infrastructure in the United States, 1970-2015: Report to the Office of Intelligence and Analysis, U.S. Department of Homeland Security*. Maryland: National Consortium for the Study of Terrorism and Responses to Terrorism: A Department of Homeland Security Science and Technology Center of Excellence, 2016.

[31] MINÁŘ, Alexander. Kritická infrastruktura EU a ČR. 2012. Dotupné z: http://pvvc.cz/ckfinder/userfiles/files/Prezentace%20%20.ppt

[32] Ministerstvo vnitra. *Národní program ochrany kritické infrastruktury (2010)*. 2010.

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

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

[35] *Návrh ROZHODNUTÍ RADY o výstražné informační síti kritické infrastruktury (CIWIN): KOM(2008) 676 v konečném znění 2008/0200 (CNS)*

[36] Number of smartphone users worldwide from 2014 to 2020 (in billions). *Statista.com* [online]. 2017 [cit. 2017-04-24]. Dostupné z: https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

[37] Ochrana kritické infrastruktury. *Vzdělávání členů SH ČSM* [online]. 2014 [cit. 2017-03-02]. Dostupné z: https://www.vzdelavani-dh.cz/publicCourse?id=59&head=121&subhead=298

[38] *Pracovní dokument komise o novém přístupu k Evropskému programu na ochranu kritické infrastruktury (EPCIP) Budování bezpečnější Evropské kritické infrastruktury: SWD(2013) 318 v konečném znění*. In: . Brusel: Rada EU, 2013.

[39] PROCHÁZKOVÁ, Dana. *Bezpečnost kritické infrastruktury*. Praha: České vysoké učení technické v Praze, 2012. ISBN 978-80-01-05103-0.

[40] První "letecký" útok IS: Teroristé k útoku v Iráku použili dron. *E15.cz* [online]. 2016 [cit. 2017-05-11]. Dostupné z: http://zpravy.e15.cz/zahranicni/udalosti/prvni-letecky-utok-is-teroriste-k-utoku-v-iraku-pouzili-dron-1323786

[41] Příchod hackerů: příběh Stuxnetu. *Root.cz* [online]. 2014 [cit. 2017-04-23]. Dostupné z: https://www.root.cz/clanky/prichod-hackeru-pribeh-stuxnetu/

[42] ROSINOVÁ, Marika. Postup určování prvků kritické infrastruktury. *Časopis 112* [online]. 2012, **XI**(10/2012) [cit. 2017-02-17]. Dostupné z: http://www.hzscr.cz/clanek/informacni-servis-casopis-112-2012-casopis-112-rocnik-xi-cislo-10-2012.aspx?q=Y2hudW09NQ%3D%3D

[43] *Sdělení komise ze dne 12. prosince 2006 o Evropském programu na ochranu kritické infrastruktury: KOM(2006) 786 v konečném znění*. In: *Úřední věstník C 126*. 2006.

[44] *Ochrana kritické infrastruktury při boji proti terorismu: KOM(2004) 702 v konečném znění*. In: . Brusel: Komise evropských společenství, 2004.

[45] PAGANINI, Pierluigi. DroneDefender, electromagnetic gun that shoot down drones. *Securityaffairs.co* [online]. 2015 [cit. 2017-05-13]. Dostupné z: http://securityaffairs.co/wordpress/41138/security/dronedefender-electromagnetic-gun.html

[46] ŠČUREK, Radomír a Daniel MARŠÁLEK. *Režimová a administrativní ochrana civilního letiště*. Brno: Akademické nakladatelství CERM, 2014. ISBN 978-80-7204-882-

[47] ŠENOVSKÝ, Michail, Vilém ADAMEC a Pavel ŠENOVSKÝ. *Ochrana kritické infrastruktury*. V Ostravě: Sdružení požárního a bezpečnostního inženýrství, 2007. Spektrum (Sdružení požárního a bezpečnostního inženýrství). ISBN 978-80-7385-025-8.

[48] ŠTĚTINA, Jiří. *Zdravotnictví a integrovaný záchranný systém při hromadných neštěstích a katastrofách*. Praha: Grada, 2014. ISBN 9788024745787.

[49] UHLÁŘ, Jan. *Technická ochrana objektů*. 2. vyd. Praha: Policejní akademie České republiky v Praze, 2009. ISBN 978-80-7251-312-3.

[50] *Usnesením vlády České republiky ze dne 14. prosince 2011 č. 934*

[51] Výstražná informační síť kritické infrastruktury (CIWIN). *Hasičský záchranný sbor České republiky* [online]. 2017 [cit. 2017-02-15]. Dostupné z: http://www.hzscr.cz/clanek/vystrazna-informacni-sit-kriticke-infrastruktury-ciwin.aspx

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

[53] *Zelená kniha o evropském programu na ochranu kritické infrastruktury: KOM(2005) 576 v konečném znění*. In: . Brusel: Komise evropských společenství, 2005.

[54] ZIO, Enrico. Challenges in the vulnerability and risk analysis of critical infrastructures. *Reliability Engineering & System Safety*. 2016, (152), 137–150. ISSN 0951-8320.

[55] Zio E, Piccinelli R, Sansavini G (2011) An all-hazard approach for the vulnerability analysis of critical infrastructures. In: Proceedings of the European Safety and Reliability Conference: 2451–2458

[56] ZIO, Enrico. Challenges in the vulnerability and risk analysis of critical infrastructures. *Reliability Engineering & System Safety*. 2016, (152), 137–150. ISSN 0951-8320.

# 16 SEZNAM POUŽITÝCH OBRÁZKŮ

# 17 SEZNAMU POUŽITÝCH TABULEK

# 18 SEZNAM POUŽITÝCH GRAFŮ