**ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE**

**Fakulta biomedicínského inženýrství**
**Katedra zdravotnických oborů a ochrany obyvatelstva**

# Ochrana utajovaných informací u podnikatelských subjektů

# Protection of Classified Information of Business Entities

Diplomová práce

Studijní program: Ochrana obyvatelstva
Studijní obor: Civilní nouzové plánování

Vedoucí práce: Ing. Ivan Koleňák

**Bc. Daniela Žáčková**

**Kladno, květen 2019**

ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

# ZADÁNÍ DIPLOMOVÉ PRÁCE

## I. OSOBNÍ A STUDIJNÍ ÚDAJE

| | | | | | |
|---|---|---|---|---|---|
| Příjmení: | **Žáčková** | Jméno: | **Daniela** | Osobní číslo: | **474909** |
| Fakulta: | **Fakulta biomedicínského inženýrství** | | | | |
| Garantující katedra: | **Katedra zdravotnických oborů a ochrany obyvatelstva** | | | | |
| Studijní program: | **Ochrana obyvatelstva** | | | | |
| Studijní obor: | **Civilní nouzové plánování** | | | | |

## II. ÚDAJE K DIPLOMOVÉ PRÁCI

Název diplomové práce:

**Ochrana utajovaných informací u podnikatelských subjektů**

Název diplomové práce anglicky:

**Protection of Classified Information of Business Entities**

Pokyny pro vypracování:

Předmětem diplomové práce bude analýza a komparace systému vlastní ochrany utajovaných informací u vybraných právnických osob z odlišných oblastí podnikání (energetika, informatika a doprava), v rámci jejichž činnosti je požadován přístup k utajovaným informacím stupně utajení „důvěrné" a vyšší. V teoretické části bude obecně popsán bezpečnostní systém ČR a dále současný stav problematiky ochrany utajovaných informací s důrazem na právnické osoby, včetně popisu systému ochrany těchto informací, který je souhrnně zpracován v dokumentaci jednotlivých právnických osob, a jehož narušením může být způsobena újma zájmům ČR. V praktické části bude provedena SWOT analýza systému ochrany utajovaných informací u vybraných podnikatelských subjektů z odlišných oblastí podnikání, s důrazem na jednotlivá ohrožení utajovaných informací a z nich vyplývající rizika v daných odvětvích. Výsledky analýzy budou komparativně posouzeny a dále budou na jejich základě stanoveny návrhy dalších opatření k zajištění ochrany utajovaných informací v souladu se splňováním podmínek nutných pro vydání osvědčení podnikatele.

Seznam doporučené literatury:

[1] MUSIL, Rudolf, Ochrana utajovaných skutečností, Praha: EUROUNION,s.r.o., 2001, ISBN 8085858932
[2] VILÁŠEK, Josef a FUS, Jan, Krizové řízení v ČR na počátku 21. století, ed. 1., Praha: Kalolinum, 2013, 266 s., ISBN 978-80-246-2170-8
[3] BALABÁN, Miloš a PERNICA, Bohuslav a kol., Bezpečnostní systém ČR: problémy a výzvy, Praha: Karolinum, 2015, ISBN 9788024631509

Jméno a příjmení vedoucí(ho) diplomové práce:

**Ing. Ivan Koleňák**

Jméno a příjmení konzultanta(ky) diplomové práce:

Datum zadání diplomové práce: **01.10.2018**
Platnost zadání diplomové práce: **18.09.2020**

| | |
|---|---|
| prof. MUDr. Leoš Navrátil, CSc., MBA, dr.h.c. | prof. MUDr. Ivan Dylevský, DrSc. |
| podpis vedoucí(ho) katedry | podpis děkana(ky) |

## Prohlášení

Prohlašuji, že jsem diplomovou práci s názvem Ochrana utajovaných informací u podnikatelských subjektů vypracovala 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 Praze dne 25.03.2019

……
podpis

## Poděkování

Mé poděkování patří zejména vedoucímu diplomové práce, panu Ing. Ivanu Koleňákovi, a to za jeho trpělivost, přínosné rady a konstruktivní připomínky při tvorbě diplomové práce. Současně bych tímto způsobem ráda poděkovala odborným konzultantům z Národního bezpečnostního úřadu, a to za umožnění realizace praktické části této práce a za odborné připomínky při jejím zpracování. V neposlední řadě patří poděkování mé rodině, jejíž členové byli po celou dobu vypracování diplomové práce velkou morální oporou.

## Abstrakt

Diplomová práce je zaměřena na systém ochrany utajovaných informací u podnikatelských subjektů, v rámci jejichž činnosti je požadován přístup k utajovaným informacím. Uvedená problematika úzce souvisí s problematikou bezpečnosti České republiky. Předmětem zkoumání je systém vlastní ochrany utajovaných informací u vybraných právnických osob z odlišných oblastí podnikání (energetika, informatika a doprava).

Teoretická část je zaměřena na obecný popis bezpečnostního systému České republiky, vztah krizového řízení a utajovaných informací, bezpečnost informací a její řízení a dále na současný stav problematiky ochrany utajovaných informací s důrazem na právnické osoby, včetně popisu systému ochrany těchto informací, jehož narušením může být způsobena újma zájmům České republiky. Uvedené součásti vycházejí z platných právních předpisů pro jednotlivé oblasti.

Praktická část diplomové práce je zaměřena na analýzu systému ochrany utajovaných informací u vybraných subjektů z odlišných oblastí podnikání, s důrazem na jednotlivá ohrožení utajovaných informací v daných odvětvích.

Cílem diplomové práce je posouzení výsledků výše popsané analýzy a současně návrh dalších možných opatření k zajištění ochrany utajovaných informací v souladu se splňováním podmínek nutných pro vydání osvědčení podnikatele.



## Klíčová slova

Bezpečnost; krizové řízení; informace; utajované informace; ochrana utajovaných informací.

## Abstract

The Master Thesis is focused on the system of protection of classified information for business entities whose activity requires access to classified information. The topic is closely related to the security of the Czech Republic. The subject of investigation is the system of protection of classified information in selected legal entities from different areas of business (energetics, informatics, and transport).

The theoretical part focuses on the general description of the security system of the Czech Republic, the relationship between crisis management and classified information, the security of information and its management, as well as on the state of the art of protecting classified information with emphasis on legal entities including a description of the system of protection of such information the violation of which may cause damage to the interests of the Czech Republic. These parts are based on the applicable legislation for individual areas.

The practical part of the Master Thesis is focused on the analysis of the system of protection of classified information in selected entities from different areas of business, with an emphasis on individual threats to classified information in sectors concerned.

The aim of the Master Thesis is to evaluate the results of the analysis described above and at the same time to propose other possible measures to ensure the protection of classified information in compliance with the conditions necessary for the issuance of a certificate of entrepreneur.

## Key words

Safety; crisis management; information; classified information; protection of classified information.

# Obsah

# 1 Úvod

Informace jsou v současné době často skloňovaným pojmem v mnoha významech. Lidské poznání se ve své podstatě zakládá převážně na získaných informacích, které jsou dále zpracovávány. Relevantní informace jsou ceněným aktivem, a to jak pro jednotlivce, tak pro firmy a státní aparát jako komplex. Tyto relevantní informace mohou mít z hlediska svého obsahu různý charakter a v souvislosti s tímto podléhají určitému druhu zabezpečení např. pro případ, že by došlo k mimořádné události nebo krizové situaci, v jejímž důsledku by mohly být uvedené hodnoty ohroženy.

V prostředí jednotlivých společností může být motivem zajištění informací nejen pravděpodobnost vzniku mimořádné události nebo krizové situace, ale zejména zajištění konkurenceschopnosti, udržení vlastního know-how a v neposlední řadě dodržování postupů v rámci legislativních pravidel. Za jednu z konkurenčních výhod lze považovat skutečnost, že daný subjekt má možnost se přímo či subdodavatelsky podílet na veřejné zakázce, u níž je striktně stanovený požadavek zadavatele pro přístup k utajovaným informacím (dále jen „UI“) stupně utajení Důvěrné a vyšší. Pro to, aby se tento subjekt mohl v rámci uvedené veřejné zakázky realizovat, musí být držitelem tzv. osvědčení podnikatele, které na základě výsledků prováděného bezpečnostního řízení vydává Národní bezpečnostní úřad (dále jen „NBÚ“). Jestliže se daná společnost rozhodne tuto „konkurenční výhodu“ získat, musí mj. být schopna zajistit ochranu UI, a to nejen v rámci bezpečnostního řízení, ale následně po celou dobu držitelství osvědčení podnikatele. V souvislosti s výše uvedeným zpracovává podnikatel souhrnný dokument s názvem bezpečnostní dokumentace, ve kterém stanoví systém ochrany UI, a který je průběžně aktualizován. Na základě tohoto dokumentu dále systém ochrany UI podnikatel realizuje. Celý systém na základě všech zjištěných skutečností ověřuje NBÚ.

Jelikož ochrana UI přímo souvisí se zajištěním bezpečnosti České republiky (dále jen „ČR“), je v teoretické části diplomové práce věnován prostor i obecnému popisu bezpečnostního systému ČR a zároveň vztahu ochrany UI a krizového řízení, včetně opory v právním řádu ČR.

Problematika ochrany UI je velmi rozsáhlá a při její detailní analýze by byly z hlediska rozsahu překročeny zejména kapacitní požadavky na diplomovou práci. Z tohoto důvodu

je praktická část diplomové práce zaměřena na analýzu vlastního systému ochrany UI u vybraných podnikatelských subjektů. Výběr tématu diplomové práce byl ovlivněn zejména tím, že jsem zaměstnancem výše uvedeného úřadu, konkrétně odboru průmyslové bezpečnosti a náplní mé práce je mj. provádění bezpečnostního řízení u právnických osob. Důvodem byl dále zejména fakt, že výzkum obdobného charakteru nebyl dle mých informací do současnosti proveden a je pro mne, zaměstnance výše uvedeného úřadu, dalším přínosem.

# 2 Současný stav

Prostor, ve kterém žijeme, je otevřený systém, který se neustále vyvíjí. Tento prostor je možno nazvat jako lidský systém a neustále v něm probíhají procesy, děje, jevy a různé události. Projevy zmíněných skutků, které mohou za určitých okolností poškodit člověka nebo jeho zájmy, se nazývají pohromy. Člověk se snaží tyto děje, jevy a události zmapovat a zhodnotit tak, aby mohl dále lidstvu zajistit bezpečný prostor, k čemuž používá tzv. řízení neboli management. [1]

V uvedeném otevřeném systému stále vzrůstá význam informací. Práce s informacemi je v současné době velmi důležitá, a z tohoto důvodu je nutno zajistit kvalitní řízení. Důraz na efektivnost při práci s informacemi je způsoben zejména tlakem konkurenčního prostředí, které si vynucuje změnu chování podnikatelů, firem soukromých i polostátních, ale také složek bezpečnostního systému státu. U všech jmenovaných tvoří informace aktivum firmy, resp. organizace. Informace představují hodnotu, která vzrůstá s možným obohacením o další atributy. Pokud se firmě, resp. organizaci podaří pracovat s informacemi efektivněji, získá značnou konkurenční výhodu. Pro všechna aktiva subjektů, a v důsledku tedy i pro informace, platí, že se musí stát objektem bezpečnosti. [2] Výše uvedené subjekty se při své činnosti mohou setkávat s různými druhy informací. Podle typu informací, které se ve společnosti vyskytují, musí být u disponujících subjektů nastavena jednotlivá bezpečnostní opatření.

Aby bylo možno ztotožnit si bezpečnost UI, je potřeba si definovat pojmy týkající se bezpečnostního systému, krizového řízení a v neposlední řadě i jednotlivé typy informací, které následně se zajištěním vlastní ochrany UI přímo souvisí.

## 2.1 Bezpečnostní systém

Obecně je bezpečnostní systém vnímán jako systém řízení bezpečnosti. Hlavním úkolem bezpečnostního systému každého státu je zajištění požadované bezpečnostní situace, a to zejména s ohledem na zajištění ochrany svých bezpečnostních zájmů. [1]

### 2.1.1 Bezpečnost a bezpečnostní systém České republiky

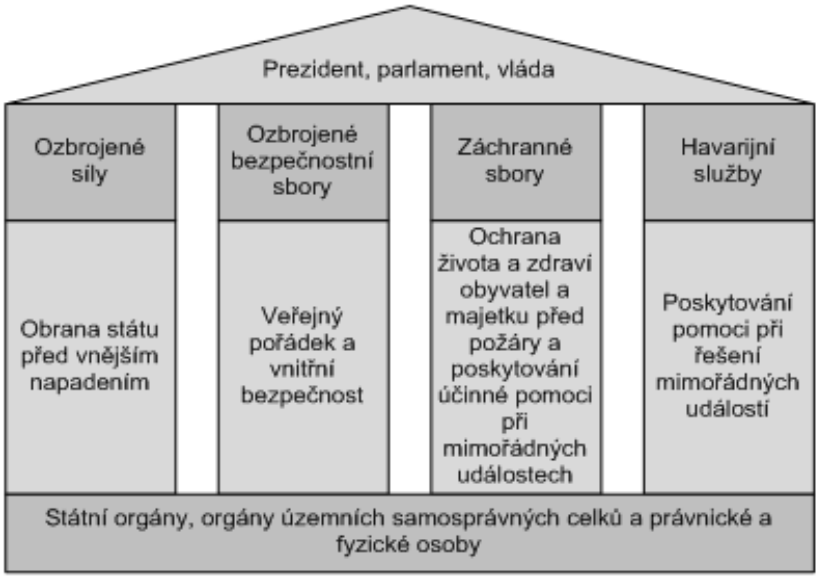
Bezpečnost je výrazem, který se používá v obecné mluvě a současně i ve specifických odvětvích. [3] Svým obsahem se jedná o subjektivní pojem. To, co připadá bezpečné jedné individualitě, nemusí jiné k pocitu bezpečí již postačovat.

Český ekvivalent vychází z latinského výrazu securus, který znamená bezstarostný, klidný, nemající starosti. V návaznosti na různá pojetí lze ve vztahu k jakémukoli subjektu vymezit pojem bezpečnost jako stav, kdy jsou na nejnižší míru eliminovány hrozby pro individuální objekt a tento objekt je současně ochoten spolupracovat při eliminaci možných hrozeb. Uvedené vyvození pojmu bezpečnosti lze tedy dále použít k odvození charakteristiky vnitřní i vnější bezpečnosti státu. Vnitřní bezpečnost je označována za vícevýznamový výraz pro procesy a opatření, jejímž cílem je zajistit takové poměry, v nichž bude důsledně respektován právní pořádek. [4] Nelze však zcela oddělit bezpečnost vnitřní od bezpečnosti vnější. Pro zajišťování vnitřní a vnější bezpečnosti musí každé státní zřízení analyzovat své bezpečnostní prostředí, jehož definování je klíčové pro určení východisek bezpečnostní politiky státu. [3]

V bezpečnostním prostředí, které je tvořeno prostorem vně státních hranic, se odehrávají procesy, které mohou mít významný vliv na bezpečnost státu, a proto jeho důsledná analýza je základním kamenem pro vybudování kvalitní bezpečnostní politiky. Toto prostředí prochází v současnosti různými změnami. Charakteristickým ukazatelem současného prostředí je zejména skutečnost, že i konflikty odehrávající se mimo území Evropy mohou přímo ovlivnit bezpečnost ČR. Analýzou bezpečnostního prostředí, ve kterém se ČR nachází, bylo identifikováno, resp. aktualizováno 11 hrozeb. Mezi nejvýznamnější faktor zvyšující v současné době pravděpodobnost vzniku hrozby patří zejména zhoršující se bezpečnostní situace v zemích sousedících s členskými státy NATO a Evropské unie (dále jen EU“). [5] Specifické parametry má poté v případě útoku kybernetický prostor. Pokud jde o kybernetické hrozby je současně nutno uvést, že hranice státu je v těchto případech doslovně stírána. S uvedeným se lze ztotožnit i na základě konstatování vyplývajícího z předchozího výzkumu, a to že konflikty v budoucnu mohou být konfliktem informatiky a budou uskutečněny v prostředí elektroniky, robotizace a umělé inteligence. V návaznosti na uvedené lze proto hrozbu kybernetického útoku řadit mezi hrozby s nejvyšší pravděpodobností. [6]

Bezpečnostní systém státu je obecně definován jako *institucionální nástroj pro tvorbu a realizaci bezpečnostní politiky. Je tvořen příslušnými prvky zákonodárné, výkonné a soudní moci, územní samosprávy, právnickými a fyzickými osobami, které mají odpovědnost za zajištění bezpečnosti státu.* [7]

Bezpečnostní systém ČR, resp. propojení zákonodárné, výkonné a soudní moci a územní samosprávy spolu s právnickými a fyzickými osobami, je tedy úzce spojen s bezpečnostní politikou státu, kterou tvoří několik základních složek. Mezi tyto složky patří zahraniční politika v oblasti bezpečnosti státu, obranná politika, politika v oblasti vnitřní bezpečnosti, hospodářská politika v oblasti bezpečnosti státu a politika veřejné informovanosti v oblasti bezpečnosti státu. [1] Strukturu bezpečnostního systému ČR znázorňuje obrázek 1.




*Obrázek 1 Bezpečnostní systém ČR [8]*

Základním dokumentem bezpečnostní politiky ČR je Bezpečnostní strategie České republiky, v aktualizovaném znění z roku 2015, která definuje východiska bezpečnostní politiky ČR, bezpečnostní zájmy ČR, bezpečnostní prostředí a strategii prosazování bezpečnostních zájmů ČR. [5]

### 2.1.2 Bezpečnostní zájmy

Národní zájmy jsou z obecného hlediska těžce definovatelné. Můžeme je však považovat, v určitém časovém intervalu, za stálé zaměření státu vzniklé na základě stavů ve vnitropolitické a zahraničněpolitické situaci. Toto zaměření dává zastupitelům státu podnět ke stanovení pro stát důležitých cílů a zároveň etickou povinnost k jejich dosažení. [3]

Bezpečnostní zájmy ČR jsou rozděleny na zájmy životní, strategické a další významné zájmy. Uvedené skupiny jsou řazeny podle stupně důležitosti, z čehož i z logiky věci vyplývá, že zajištění životních zájmů je prioritou státu. [5] *Životním zájmem je zajištění suverenity, územní celistvosti a politické nezávislosti ČR, zachování všech náležitostí demokratického právního státu včetně záruky a ochrany základních lidských práv a svobod obyvatel. Ochrana životních zájmů státu a jeho občanů je základní povinností vlády i všech orgánů veřejné moci.* [5] Rozdělení bezpečnostních zájmů je zobrazeno na obrázku 2.


*Obrázek 2 Bezpečnostní zájmy ČR [5]*

Za životní zájmy lze označit ty národní zájmy, které jsou nutné k zajištění existence státu, a to zejména k zajištění územní celistvosti a státní suverenity. Linie mezi životními a strategickými zájmy je v oblasti bezpečnostní politiky těžko určitelná. Strategické zájmy jsou v rámci bezpečnostní politiky stanoveny jako zájmy, jejichž obhajoba s pozitivním výsledkem tvoří podmínky pro dosažení cílů bezpečnostní politiky. [3]

### 2.1.3 Legislativní rámec k zajištění bezpečnosti ČR

Výchozím zdrojem k vytváření a uplatňování bezpečnostní strategie je ústavní pořádek ČR, zejména Ústava ČR, Listina základních práv a svobod a ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky, v platném znění. [5] Součástí právního rámce jsou také další spojenecké a mezinárodní závazky vycházející z členství ČR v mezinárodních aliancích (NATO, EU, OSN a OBSE). [5] Členství v NATO a EU je pro ČR strategicky a politicky důležité, státu tak zabezpečuje a posiluje stabilitu bezpečnostního systému. [9]

S právními předpisy, které dávají legislativní rámec pro uplatňování bezpečnostní politiky státu úzce souvisí i dokumenty nelegislativního charakteru, mezi které, kromě již zmíněné Bezpečnostní strategie České republiky, dále patří např. Obranná strategie České republiky, Analýza hrozeb pro Českou republiku, Audit národní bezpečnosti, Akční plán k Auditu národní bezpečnosti, Koncepce ochrany obyvatelstva do roku 2020 s výhledem do roku 2030, Bílá kniha o obraně, Nová strategická koncepce NATO a Evropská bezpečnostní strategie.

Jak již z výše uvedeného vyplývá, bezpečnostní systém ČR je složen z celé řady prvků rozdělených do dvou úrovní řízení, a to ústřední a územní. Ústřední úroveň tvoří prezident republiky, Parlament ČR, Bezpečnostní rada státu (dále jen „BRS“) včetně jejích stálých pracovních orgánů, ministerstva a jiné ústřední správní úřady. Územní úroveň tvoří orgány krajů, orgány obcí s rozšířenou působností (dále jen „ORP“) a orgány obcí a další správní úřady s územní působností.

Současně de iure dle výše uvedeného ústavního zákona č. 110/1998 *bezpečnost ČR zajišťují ozbrojené síly, ozbrojené bezpečnostní sbory, záchranné sbory a havarijní služby. Státní orgány, orgány samosprávných celků a právnické a fyzické osoby jsou povinny se na zajišťování bezpečnosti podílet*. [10] Z pohledu prostředí, ve kterém jednotlivé složky

bezpečnost zajišťují lze uvést, že vnitřní bezpečnost zajišťují Policie ČR, Ministerstvo vnitra ČR, Ministerstvo financí ČR, Celní správa, zpravodajská služba a v neposlední řadě Hasičský záchranný sbor ČR. Pro zajištění vnitřní bezpečnosti má významnou roli také spolupráce s občany a sdruženími působícími v oblasti bezpečnosti. Individuální bezpečnost je výsadou zejména soukromých bezpečnostních služeb, které zajišťují ochranu osob a majetku. [11] Vnější bezpečnost je v gesci Ministerstva zahraničních věcí ČR, Ministerstva obrany ČR a také zpravodajských služeb. [12]

Jak z výše uvedeného vyplývá, primárním úkolem bezpečnostní politiky státu je ochrana bezpečnostních zájmů ČR. Tato politika je založena na proaktivním přístupu a dle bezpečnostní strategie ČR *usiluje proto o včasnou detekci hrozeb, jejich kvalitní analýzu a přijímání aktivních opatření.* [5] Jestliže organizace disponuje v rámci své činnosti UI dle zákonné klasifikace, může být jejím vyzrazením nebo zneužitím způsobena újma zájmu ČR nebo to může být pro zájem nevýhodné. [13] Vzhledem k výše uvedené skutečnosti je důležité či zcela nezbytné realizovat v organizaci bezpečnostní politiku, ve které je nutno nastavit pravidla, interní předpisy a zvyklosti určující způsoby, pomocí kterých budou v dané organizaci předmětné informace, a v konečném důsledku i bezpečnostní zájmy ČR, dostatečně chráněny.

## 2.2 Definice a rozdělení informací

Informace pochází z latinského slova informare, což znamená dodávat tvar, podobu, formovat, tvořit, zobrazovat a představovat si. Základem informace jsou data, která zobrazují stavy, vlastnosti objektů nebo probíhající procesy. V sociálních a informačních vědách je uváděna tzv. obecná definice informace, podle které se jedná o správně vytvořená, smysluplná a pravdivá data. [14] Informace jsou tedy data použitá v určitém kontextu. [15] Informace je ve svém důsledku součástí tzv. informačního procesu a dává význam přisuzovaný datům. Další interpretací informací a aplikací lidské zkušenosti jsou informace přetvořeny ve znalosti. [16]

Každá organizace pracuje s množstvím různorodých informací. Z pohledu výskytu informací v dané společnosti lze informace dělit na veřejné, neveřejné a ostatní, u kterých je určitým způsobem potřebná regulace. [2]

### 2.2.1 Veřejné a neveřejné informace

Za veřejné informace se považují informace, které jsou přístupné pro čtení zpravidla komukoli. Informace neveřejné jsou dostupné pouze omezenému okruhu osob a ve své podstatě jsou opakem informací veřejných. [17] Z hlediska ochrany se na ně nevztahují žádné právní normy. Tyto informace mohou mít zejména provozní nebo organizační charakter. [2]

### 2.2.2 Ostatní informace

Ostatní informace lze dále rozdělit podle způsobu, jakým je práce s nimi regulována. V návaznosti na uvedené rozdělení tvoří skupinu ostatních informací informace citlivé, informace utajované a tzv. zvláštní skutečnosti. [2]

#### A) Citlivé informace

Citlivé informace dále členíme na důvěrné a přísně důvěrné, na rozdíl od UI, které se dělí na Vyhrazené, Důvěrné, Tajné a Přísně tajné. Obě kategorie jsou díky těmto podskupinám v laické praxi lehce zaměnitelné. Z hlediska významu a obsahu jsou však naprosto rozdílné. V prvním případě si lze pod citlivými informacemi důvěrného charakteru představit osobní údaje, obchodní tajemství a informace smluvní strany.

Definice pojmu osobní údaj je zakotvena v zákoně č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů, a zní: *„jakákoliv informace týkající se určeného nebo určitelného subjektu údajů“.* [18] Ochrana osobních údajů vyplývá z uvedeného zákona a nově z Nařízení (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

Obchodním tajemstvím se rozumí: *„konkurenčně významné, určitelné, ocenitelné a v příslušných obchodních kruzích běžně nedostupné skutečnosti, které souvisejí se*

*závodem a jejichž vlastník zajišťuje ve svém zájmu odpovídajícím způsobem jejich utajení“.* [19] Před platností nového občanského zákoníku, který nabyl účinnosti dne 1. 1. 2014, upravoval pojem obchodní tajemství obchodní zákoník, který byl ke stejnému dni zrušen. Informace smluvní strany jsou, jak už z názvosloví vyplývá, takové informace, jejichž nutnost ochrany vyplývá ze smluvních vztahů. [2]

S osobními údaji, obchodním tajemstvím a informacemi smluvní strany úzce souvisí citlivé informace s charakterem přísně důvěrným. Tyto informace se vyznačují obsahem prvků obchodního tajemství a jejich ohrožení může vést k poškození strategických a prioritních zájmů firmy, resp. organizace. [2]

### B) Utajované informace

Pojem utajovaná informace je v praxi používán v různém smyslu. Jediná a závazná definice tohoto pojmu je však ve smyslu zákona č. 412/2005, o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. Uvedený zákon uvádí, že UI je: *„informace v jakékoliv podobě zaznamenaná na jakémkoliv nosiči označená v souladu s tímto zákonem, jejíž vyzrazení nebo zneužití může způsobit újmu zájmům České republiky nebo může být pro tento zájem nevýhodné, a která je uvedena v seznamu utajovaných informací“.* [13] Pro určení charakteru a dále stupně utajení je potřeba, aby informace splňovala znaky uvedené v předmětném zákoně. Zajištění ochrany UI vychází striktně z uvedeného zákona a příslušných prováděcích právních předpisů.

### C) Zvláštní skutečnosti

Zvláštní skutečnosti představují informace z oblasti krizového řízení. V podstatě se jedná o informace přísně důvěrné, které mají vztah k výkonu státní správy při přípravě na řešení a při řešení krizových situací naturogenního či antropogenního původu. [20] Samotný pojem je definován v zákoně č. 240/2000 Sb., zákon o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů, který uvádí, že: *„zvláštními skutečnostmi se rozumí údaje z oblasti krizového řízení, které by v případě zneužití mohly vést k znemožnění nebo omezení činnosti orgánu krizového řízení, ohrožení života a zdraví osob, majetku, životního prostředí nebo podnikatelského zájmu právnické*

*osoby nebo fyzické osoby vykonávající podnikatelskou nebo jinou obdobnou činnost podle zvláštních právních předpisů, pokud tyto údaje nejsou utajovanými informacemi“*. [21] Uvedené informace jsou chráněné tímto zákonem a dále nařízením vlády č. 462/2000 Sb., k provedení některých ustanovení krizového zákona.

Jestliže by daná informace byla v režimu obchodního tajemství a současně by nebylo vyloučeno, že je dle svého charakteru informací utajovanou, uplatnily by se na ni opatření podle předpisů, které upravují oblast informací utajovaných, neboť zde z podstaty věci platí priorita vyššího zájmu. [22]

## 2.3 Krizové řízení a utajované informace

V obecném pojetí vyjadřuje pojem krize situaci, při které dochází ke zvratu událostí či změně tzv. normálního stavu, za který je považováno fungování určitého systému. Při tomto je zřejmé narušení, resp. ohrožení chráněných hodnot, zájmů či statků. [3]

Z hlediska původu vzniku můžeme dělit hrozby na naturogenní a antropogenní. Hrozby naturogenního charakteru lze dále dělit na abiotické a biotické. Nebezpečí antropogenního původu dále dělíme na technogenní, sociogenní a ekonomické. Na základě určitých definovaných hrozeb lze v důsledku důvodně očekávat vznik krizové situace. [23]

V ČR je pojem krizová situace definován jako *„mimořádná událost podle zákona o integrovaném záchranném systému, narušení kritické infrastruktury nebo jiné nebezpečí, při nichž je vyhlášen stav nebezpečí, nouzový stav nebo stav ohrožení státu“*. [21]

Jinou definici pojmu krizová situace uvádí např. PhDr. Ivo Hlaváč v publikaci Česká bezpečnostní terminologie, a to jako: „*mimořádnou událost, při níž jsou bezprostředně ohroženy demokratické zájmy státu, svrchovanost a územní celistvost státu, chod hospodářství, systém státní správy a soudnictví, zdraví a život velkého počtu osob, majetek ve velkém rozsahu, životní prostředí nebo plnění mezinárodních závazků ke společné obraně“*. [3] Obecně tedy lze říci, že pokud mimořádná událost nabyde takových

rozměrů, že běžná činnost správních úřadů, orgánů krajů a obcí, složek integrovaného záchranného systému (dále jen „IZS“) nebo subjektů kritické infrastruktury nevede k odvrácení vzniklého ohrožení, je nutno k řešení této události vyhlásit krizový stav.

Pojem krizový stav je zakotven v právním systému ČR a základním kritériem pro jeho vyhlášení je druh mimořádné události, rozsah postižení a velikost postiženého území. Jestliže se jedná o krizovou situaci, která nesouvisí se zajišťováním obrany ČR před vnějším napadením, lze vyhlásit stav nebezpečí, nouzový stav a stav ohrožení státu. Jedná-li se o krizové situace, které naopak se zajišťováním obrany ČR před vnějším napadením souvisejí, lze vyhlásit stav ohrožení státu nebo válečný stav. [23]

K mimořádným událostem dochází každý den, a to v širokém spektru oblastí a v různém rozsahu. V praxi není vždy jednoduché předem odhadnout jakého rozsahu bude daná mimořádná událost nabývat a zda se při svém vývoji překlene do situace krizové.

Možné hrozby se mohou současně mezi sebou provazovat a jejich dopady na chráněné zájmy společnosti se tak mohou vzájemně navyšovat. S ohledem na neustále rostoucí počet přírodních a člověkem způsobených mimořádných událostí a závažnost jejich následků je důležité přistupovat k činnostem zaměřeným na eliminaci vlivu těchto jevů. Z výsledků splněného úkolu zadaného v Koncepci ochrany obyvatelstva do roku 2020 s výhledem do roku 2030, který se týkal zpracování Analýzy hrozeb pro ČR, bylo identifikováno celkem 72 typů nebezpečí, z toho 22 s nepřijatelným rizikem. Nepřijatelné riziko je nutno považovat na všech stupních veřejné správy za riziko s nejvyšší prioritu. Opatření vedoucí k eliminaci těchto rizik spadají do oblasti přípravy na řešení krizových situací a zahrnují především krizové plánování, jelikož některé hrozby v podmínkách ČR již nastaly, některé však dosud nenastaly. [23] Přehled typů nebezpečí s nepřijatelným rizikem je uveden v tabulce 1.

*Tabulka 1 Typy nebezpečí s nepřijatelným rizikem [23]*

| KATEGORIE NEBEZPEČÍ | | TYPY NEBEZPEČÍ S NEPŘIJATELNÝM RIZIKEM | GESCE* |
|---|---|---|---|
| naturogenní | Abiotické | Dlouhodobé sucho | **MŽP**, MZe, MV |
| | | Extrémně vysoké teploty | **MŽP** |
| | | Přívalová povodeň | **MŽP**, MV, MZe |
| | | Vydatné srážky | **MŽP**, MV |
| | | Extrémní vítr | **MŽP**, MV |
| | | Povodeň | **MŽP**, MV, MZe |
| | Biotické | Epidemie – hromadné nákazy osob | **MZ** |
| | | Epifytie – hromadné nákazy polních kultur | **MZe** |
| | | Epizootie – hromadné nákazy zvířat | **MZe** |
| antropogenní | Technogenní | Narušení dodávek potravin velkého rozsahu | **MZe**, MPO |
| | | Narušení funkčnosti významných systémů elektronických komunikací | **ČTÚ**, MPO |
| | | Narušení bezpečnosti informací kritické informační infrastruktury** | **NBÚ**, MV |
| | | Zvláštní povodeň | **MZe**, MV, MŽP |
| | | Únik nebezpečné chemické látky ze stacionárního zařízení | **MŽP**, MV, SÚJB |
| | | Narušení dodávek pitné vody velkého rozsahu | **MZe** |
| | | Narušení dodávek plynu velkého rozsahu | **MPO**, MV |
| | | Narušení dodávek ropy a ropných produktů velkého rozsahu | **SSHR**, MPO |
| | | Radiační havárie | **SÚJB**, MV |
| | | Narušení dodávek elektrické energie velkého rozsahu | **MPO**, MV |
| | Sociogenní | Migrační vlny velkého rozsahu | **MV**, MZV |
| | | Narušování zákonnosti velkého rozsahu (včetně terorismu) | **MV** |
| | Ekonomické | Narušení finančního a devizového hospodářství státu velkého rozsahu | **MF**, ČNB |

* Tučně jsou uvedena gesční ministerstva a jiné ústřední správní úřady a Česká národní banka (dále jen „ČNB“).

** Zařazení typu nebezpečí do kategorie nebezpečí s nepřijatelným rizikem vychází ze skutečnosti, že zákonné podmínky předpokládají pro tyto situace vyhlášení krizového stavu.

V návaznosti na výše uvedené skutečnosti můžeme uvést, že krizovou situaci je vždy nutno řešit, a to i v prekrizovém období, resp. v období běžném, nekrizovém.

Z tohoto důvodu je v právním systému státu zakotvena definice krizového řízení, která vystihuje ucelený proces od přípravy na krizovou situaci až po její řešení.

Krizovým řízením je určen *„souhrn řídících činností orgánů krizového řízení zaměřených na analýzu a vyhodnocení bezpečnostních rizik a plánování, organizování, realizaci a kontrolu činností prováděných v souvislosti s přípravou na krizové situace a jejich řešením, nebo ochranou kritické infrastruktury“*. [21] Uvedené činnosti zajišťují tzv. orgány krizového řízení, kterými jsou vláda, ministerstva a jiné správní úřady, ČNB, orgány kraje a ostatní orgány s působností na území kraje, orgány ORP a orgány obce. [1] Mezi ostatní orgány s územní působností řadíme bezpečnostní rady neboli poradní orgány zřizovatelů (vlády, kraje, ORP) pro řešení otázek bezpečnosti a přípravu na krizové situace a dále krizové štáby, které jsou pracovními orgány zřizovatelů pro řešení krizových situací. [23]

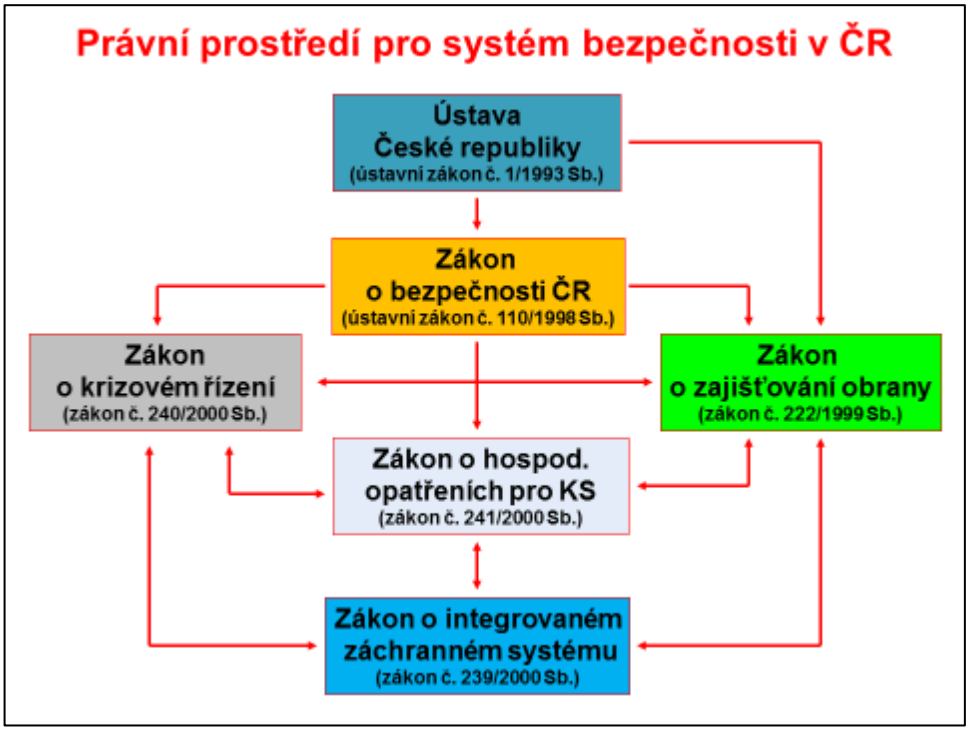
Ve vztahu k výše uvedeným identifikovaným hrozbám byly příslušnými (gesčními) ministerstvy a jinými ústředními správními úřady vypracovány typové plány, které stanoví pro konkrétní druh krizové situace doporučené typové postupy, zásady a opatření pro jejich řešení. Tyto typové plány jsou dále rozpracovány v územních krizových plánech (krizový plán kraje, krizový plán ORP) a to v operativní části krizového plánu, v návaznosti na konkrétní hrozící krizové situace, identifikované pro dané území příslušnými orgány krizového řízení.

Základní povinností státu je *„zajištění svrchovanosti a územní celistvosti České republiky, ochrana jejích demokratických základů a ochrana životů, zdraví a majetkových hodnot“*. [10] K tomu, aby stát mohl dostát litery zákona, usiluje v rámci své bezpečnostní politiky, jak je již výše uvedeno, o včasnou detekci hrozeb na základě diferenčních indicií, o kvalitní analýzu těchto zjištění a současně o přijetí adekvátních opatření. V obecném měřítku lze říci, že v rámci havarijního plánování a krizového řízení, resp. v souvislosti s přípravou na možný výskyt mimořádné události, je cílem příslušných orgánů taktéž ochrana života, zdraví a majetku. Z pohledu majetkového lze jako na vlastníka UI pohlížet jednak na stát, resp. veřejnou správu, tak na soukromé subjekty. A v tomto případě je nutno nahlížet na ochranu UI jako na ochranu aktiva daného subjektu a pro její zajištění je nezbytné provést včasnou detekci hrozeb a z nich vyplývajících rizik a opatření k jejich eliminaci. Zajištění ochrany UI je však nutno chápat

jako komplexní záležitost, jelikož jak vyplývá již z podstaty a charakteru UI, při mimořádné události, v jejímž důsledku by došlo ke ztrátě UI, nevznikne jejímu vlastníkovi pouze škoda „na majetku“, ale současně by mohlo dojít k ohrožení zájmu chráněného zákonem neboli k ohrožení základního stavebního kamene státu.

### 2.3.1 Právní předpisy v oblasti krizového řízení

Oblast krizového řízení je zakotvena v právním řádu ČR od roku 2000. Základním právním předpisem je zákon č. 240/2000 Sb., o krizovém řízení a změně některých zákonů (krizový zákon), ve znění pozdějších předpisů, který mj. definuje výše jmenované pojmy (krizová situace, krizové řízení, krizový stav a další) a úzce souvisí s dalšími právními předpisy z oblasti bezpečnosti. Propojení těchto předpisů je znázorněno na obrázku 3.




*Obrázek 3 Právní prostředí pro systém bezpečnosti ČR [24]*

Ke krizovému zákonu byly vydány 4 prováděcí předpisy, kterými jsou:

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

- nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, ve znění nařízení vlády č. 315/2014 Sb.;
- vyhláška č. 75/2001 Sb., kterou se stanoví báňsko-technické podmínky pro zřizování, využití a ochranu důlních děl vybraných pro využití při krizových situacích pro uplatňování preventivních, technických a bezpečnostních opatření a provádění kontrol;
- vyhláška č. 281/2001 Sb., kterou se provádí § 9 odst. 3 písm. a) zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění vyhlášky č. 237/2003 Sb.

Oblast krizového řízení je dále spjata s dalšími předpisy spadajícími do konkrétního oblastí činnosti. Kromě právních předpisů uvedených na obrázku 3 se jedná o následující normy:

- **zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti**, ve znění pozdějších předpisů;
- **zákon č. 181/2014 Sb., o kybernetické bezpečnosti**, ve znění pozdějších předpisů;
- zákon č. 254/2001 Sb., o vodách a o změně některých zákonů (vodní zákon), ve znění pozdějších předpisů;
- zákon č. 133/1985 Sb., o požární ochraně, ve znění pozdějších předpisů;
- zákon č. 12/2002 Sb., o státní pomoci při obnově území, ve znění pozdějších předpisů;
- zákon č. 458/2000 Sb., energetický zákon, ve znění pozdějších předpisů;
- zákon č. 320/2015 Sb., o hasičském záchranném sboru České republiky a o změně některých zákonů (zákon o hasičském záchranném sboru);
- zákon č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů;
- zákon č. 374/2011 Sb., o zdravotnické záchranné službě, ve znění pozdějších předpisů;
- zákon č. 224/2015 Sb., o prevenci závažných havárií, ve znění pozdějších předpisů;
- zákon č. 97/1993 Sb., o působnosti Správy státních hmotných rezerv, ve znění pozdějších předpisů;

- zákon č. 553/1991 Sb., o obecní policii, ve znění pozdějších předpisů;
- zákon č. 258/2000 Sb., o ochraně veřejného zdraví a o změně některých souvisejících zákonů, ve znění pozdějších předpisů;
- zákon č. 166/1999 Sb., o veterinární péči a o změně některých souvisejících zákonů, ve znění pozdějších předpisů;
- zákon č. 263/2016 Sb., atomový zákon;
- zákon č. 350/2011 Sb., o chemických látkách a chemických směsích (chemický zákon), ve znění pozdějších předpisů;
- zákon č. 189/1999 Sb., o nouzových zásobách ropy, o řešení stavů ropné nouze a o změně některých souvisejících zákonů (zákon o nouzových zásobách ropy), ve znění pozdějších předpisů;
- zákon č. 219/1999 Sb., o ozbrojených silách České republiky, ve znění pozdějších předpisů;
- zákon č. 585/2004 Sb., o branné povinnosti a jejím zajišťování (branný zákon), ve znění pozdějších předpisů. [25]

Legislativní rámec v oblasti krizového řízení dále obsahuje soubor prováděcích právních předpisů (nařízení a vyhlášky), které výše uvedené zákony tzv. uvádějí do života. Tato nařízení a vyhlášky jsou zařazena ve Sbírce zákonů ČR.

### 2.3.2 Ostatní dokumenty v oblasti krizového řízení

V oblasti krizového řízení mají významnou úlohu i další dokumenty, které nejsou zařazeny do právního systému ČR. Tyto dokumenty mají nelegislativní charakter, avšak z hlediska zajištění jednotného postupu při aplikaci krizového zákona a dalších norem z oblasti bezpečnosti, jsou velmi významné. [26]

Mezi nejdůležitější nelegislativní dokumenty lze zařadit následující:

- Bezpečnostní strategie ČR (aktualizované znění z roku 2015, schválena usnesením vlády ze dne 4. února 2015 č. 78);
- Audit národní bezpečnosti (schválen usnesením vlády ze dne 14. prosince 2016 č. 1125);

- Analýza hrozeb pro ČR (schválena usnesením vlády ze dne 27. dubna 2016 č. 369);
- Zpráva o stavu ochrany obyvatelstva v ČR (schválena usnesením vlády ze dne 7. listopadu 2018 č. 730);
- Směrnice Ministerstva vnitra čj. MV-117572-2/PO-OKR-2011 ze dne 24. listopadu 2011, kterou se stanoví jednotná pravidla organizačního uspořádání krizového štábu kraje, krizového štábu obce s rozšířenou působností a krizového štábu obce (vydalo MV-GŘ HZS ČR, publikována ve Věstníku vlády pro orgány krajů a orgány obcí, ročník 9, částka 6);
- Metodika zpracování krizových plánů podle § 15 a § 16 nařízení vlády č. 462/2000 Sb. (vydalo MV – GŘ HZS ČR pod č.j.: MV-76085-1/PO-OKR-2011);
- Metodika zpracování plánů krizové připravenosti podle § 17 a §18 nařízení vlády č. 462/2000 Sb. (vydalo MV-GŘ HZS ČR pod č.j.: MV-140690-1/PO-OKR-2011);
- Metodický pokyn ke zpracování typových plánů (vydalo MV-GŘ HZS ČR, schválen usnesením vlády ze dne 14. prosince 2016 č. 1140);
- Metodika pro vyžadování věcných zdrojů za krizové situace (vydala SSHR, schválena usnesením vlády ze dne 54. ledna 2012 č. 14);
- Metodika plánování nezbytných dodávek v systému hospodářských opatření pro krizové stavy (vydala SSHR, 2013);
- Koncepce ochrany obyvatelstva do roku 2020 s výhledem do roku 2030 (schválena usnesením vlády ze dne 23. října 2013 č. 805);
- Koncepce vzdělávání v oblasti ochrany obyvatelstva a krizového řízení (schválena usnesením vlády ze dne 10. července 2017 č. 508);
- Koncepce přípravy občanů k obraně státu (schválena usnesením vlády ze dne 16. ledna 2013 č. 38);
- Koncepce aktivní zálohy ozbrojených sil ČR (schválena usnesením vlády ze dne 23. ledna 2013 č. 52);
- Koncepce mobilizace ozbrojených sil ČR (schválena usnesením vlády ze dne 23. ledna 2013 č. 51). [27]

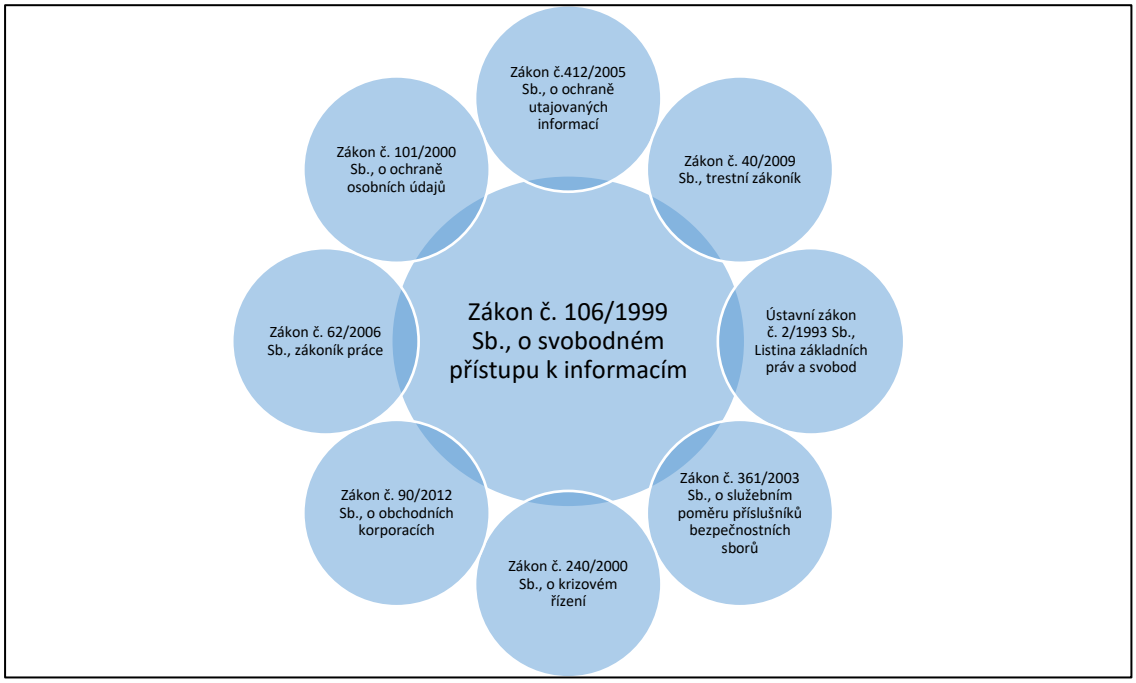
## 2.4 Bezpečnost informací a její řízení

V rámci této práce je několikrát uváděna skutečnost, že informace je aktivem firmy. Pojmem aktivum lze obecně v souvislosti s bezpečností označit vše, co má pro danou organizaci či společnost hodnotu, která může být snížena působením hrozby. Aktiva se dělí na hmotná, jejichž příkladem mohou být lidé, nemovitosti či peníze, životní prostředí a technologické systémy, a dále na nehmotná, reprezentována např. **informacemi**, předměty průmyslového a autorského vlastnictví a kvalitou personálu. [28] O každé aktivum firmy je možné pečovat, dále je rozmnožovat, ale zároveň je možno ho ukrást, zneužít nebo ztratit. [29] Z tohoto důvodu je nutno aktivum současně chránit.

Z pohledu podoby jednotlivých informací, jimiž daná společnost disponuje, je zapotřebí v rámci zajišťování jejich ochrany zohlednit způsoby možného úniku. Zaměstnanci by neměli vydávat významné dokumenty vně organizace a neměli by diskutovat o důvěrných otázkách na veřejných místech. Únik informací hrozí také při sdělení v tisku a dalších médiích, a z tohoto důvodu by tyto informace měl před jejich zveřejněním prověřit právník či bezpečnostní manažer. Dalším způsobem úniku informací může být nevhodné nakládání s nosnými médii (CD, DVD, flash disk), která obsahují pro firmu cenné informace. Tato média by měla být po použití a ukončení práce mechanicky zničena. Samostatnou oblastí, ve které hrozí možný únik informací je infomační systém organizace. [30] V globálním měřítku se dá říci, že informační systém a resp. celý kyberprostor je samostatným paralelním světem, ve kterém se vyskytuje množství hrozeb, jejichž charakter je stále více sofistikovanější.

Při orientaci na zajištění bezpečnosti informací je však nutno pohlížet na věc současně z hlediska práva občana na svobodný přístup k informacím. [31] Tyto dvě roviny náhledu spolu však v praxi, např. v rámci krizového řízení, často kolidují a osoby odpovědné za činnosti s tímto spojené tzv. balancují na hranách několika zákonů. S ohledem na uvedené je tedy pro stanovení systému ochrany informací důležité charakterizovat, s jakým druhem informací při své činnosti daný subjekt disponuje. V souvislosti se zajištěním ochrany informací je vhodné poukázat na skutečnost, že v korporátním prostředí se můžeme stále častěji setkat se zaváděním tzv. Compliance programů. Compliance obecně vyjadřuje soulad s pravidly, a to jak s pravidly stanovenými právními předpisy, tak současně s etickými pravidly či pravidly slušného chování a společnosti je zavádí z toho

důvodu, aby byla tato stanovená či interně nastavená pravidla důsledně dodržována. Ve své podstatě compliance vyjadřuje soulad činnosti společnosti s právními a vnitřními předpisy, kde součástí jsou vždy mechanismy monitoringu a prevence případného nesouladu. [32] Právní rámec ochrany informací s ohledem na jejich původce, vlastníka a charakter je zobrazen na obrázku 4.




*Obrázek 4 Právní rámec ochrany informací v ČR*

V návaznosti na výše uvedené lze předmětné konstatování podpořit výsledky výzkumu v oblasti krizového řízení, kde u 17 % oslovených respondentů z řad příslušníků Hasičského záchranného sboru ČR, Policie ČR a příslušných zaměstnanců krajských úřadů zazněl názor, že informace z oblasti krizového řízení by bylo vhodnější veřejně neposkytovat. Zjištěné skutečnosti je možno vysvětlit tím, že je v praxi velmi těžké rozlišit, které informace jsou veřejné a které již spadají do skupiny informací neveřejných, resp. ostatních. [33] Z pohledu jednotlivých společností je tak pouze na nich samotných, jakým způsobem vybrané informace ochrání, aby nedošlo k jejich zneužití. [34]

K řešení bezpečnosti informací je zapotřebí určit, kdo bude mít jednotlivé segmenty předmětného procesu na starosti. Daný proces nelze řešit samospádem, po celou dobu musí být řízen. Bez řízení by byl proces chaotický a organizace by ani neměla jistotu,

že bude úspěšně ukončen. Současně je tato varianta řešení neefektivní, a to jak z hlediska finančního, tak celkově z hlediska bezpečnostního. V rámci organizací zajišťuje řízení bezpečnosti tzv. bezpečnostní management.

### 2.4.1 Proces řešení bezpečnosti

Proces řešení bezpečnosti informací je řetězcem dílčích úkonů, který je ukončen tím, že se určená opatření zařadí do provozu, resp. užívání. V té chvíli však nastává další fáze týkající se nepřetržitého hodnocení provozu a další analýzy požadavků. Do procesu řešení bezpečnosti lze zahrnout zpracování studie bezpečnosti, vymezení bezpečnostní politiky a vypracování bezpečnostního projektu. Předmětné pojmy je možné primárně definovat následovně:

- **Studie bezpečnosti** představuje dokument obsahující tzv. zhodnocení stávajícího stavu bezpečnosti informací, v jehož důsledku jsou určeny další postupy řešení v rámci zajištění bezpečnosti informací.
- Obsah **bezpečnostní politiky** z pohledu státu je již vymezen výše v rámci podkapitoly bezpečnostní systém a bez ohledu na typ zájmového subjektu lze obecně uvést, že představuje činnost k dosažení bezpečnostních zájmů a cílů. Uvedené konstatování je tedy možno využít i při charakterizaci pojmu v oblasti ochrany informací. Ve vztahu k ochraně informací se bezpečnostní politika dělí na dvě části, konkrétně na část celkovou (globální politika) a část systémovou (bezpečnostní politika informačního systému).
- **Bezpečnostní projekt** je výstupním dokumentem, který určuje konkrétní požadavky na provedení přesně stanovených činností. [29]

Každá společnost by se při tvorbě strategie v oblasti ochrany informací měla na začátku procesu zabývat právě studií informační bezpečnosti, která představuje dokument obsahující stručný přehled aktuálně dosaženého stavu. Jelikož předmětem studie bezpečnosti není plnohodnotná analýza, lze konstatovat, že tento dokument nemůže nahradit bezpečnostní politiku, která vychází především z analýzy rizik. [29]

V krizovém řízení je analýza rizik definována jako *„proces pochopení povahy rizika a stanovení úrovně rizika. Analýzou rizik se rozumí také například zvážení relevantních scénářů hrozeb s cílem posoudit zranitelnost a možný dopad narušení nebo zničení prvků*

*kritické infrastruktury“.* S obdobným popisem se můžeme setkat i v managementu rizik, kde je analýza rizik vymezena jako *„proces pochopení podstaty rizika a stanovení jeho úrovně. Poskytuje bázi pro hodnocení rizik a návrh opatření k minimalizaci rizika“*. [28] Výstupy a závěry rizikové analýzy se následně ve formě zpracovaných opatření prolínají do všech přijatých dokumentů v oblasti bezpečnosti. [29]

Bezpečnostní politika zahrnuje principy a východiska pro další strategická řešení, kterými jsou návrhy a řešení úspěšných standardů, směrnic a dalších opatření. Bezpečnostní politika ze své podstaty musí v organizaci nalézt odpovědi na otázky vyvstávající zejména zevnitř společnosti, a to např. jaké aktivum musí být chráněno, kdy to bude efektivní a jakým způsobem bude výsledné řešení uvedeno do praxe. [29]

Bezpečnostní projekt ve svém důsledku představují konkrétní požadavky na realizaci konkrétních činností. V rámci těchto projektů je dokumentován přechod od požadavků (bezpečnostní opatření z analýzy rizik) k definovanému řešení bezpečnosti. Předmětné projekty lze definovat jako výstupy na základě vstupů. [29]

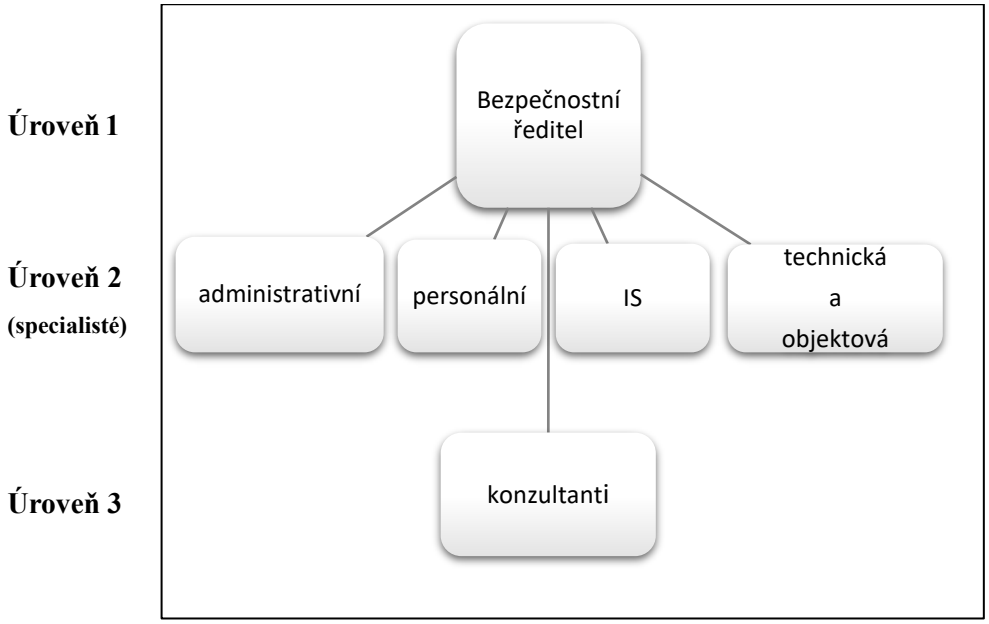
### 2.4.2 Řízení bezpečnosti – bezpečnostní management

Jak již předchozí podkapitola uvádí, řízení bezpečnosti je nezbytnou součástí strategického řízení společnosti. Obecně lze řízení bezpečnosti zahrnout pod pojem „security management“ nebo „corporate security“. Představuje oblast řízení, která řeší bezpečnost aktiv v organizaci, a to jak celkovou bezpečnost, tak bezpečnost elektronickou. [35]

Z hlediska ochrany informací lze tedy pod řízení bezpečnosti v dané oblasti podhrnout bezpečnost personální a administrativní, objektovou bezpečnost a bezpečnost informačních systémů.

Úkolem řízení informační bezpečnosti je především zavedení pravidel a postupů nutných pro řízení informační bezpečnosti dané organizace. V tomto smyslu musí být primárně důkladně popsána organizace řízení a odpovědnost řídících pracovníků (bezpečnostního managementu) a dalších odborných entit a jednotlivých zaměstnanců v systému bezpečnosti informací. [31]

Vytvoření struktury bezpečnostního managementu je alfou a omegou celé bezpečnostní strategie a je klíčem k úspěšnému zahájení procesu realizace informační bezpečnosti. Nejefektivnějším přístupem k zajištění ochrany informací je definování tří úrovní bezpečnostního managementu. [29] Předmětné rozdělení úrovní řízení je zobrazeno na obrázku 5.




*Obrázek 5 Úrovně bezpečnostního managementu*

## 2.5 Ochrana utajovaných informací

Ochrana UI je považována za významný pilíř národní a současně mezinárodní bezpečnosti. Znalost informací týkající se bezpečnosti je rozhodující při boji proti současným vnějším a vnitřním bezpečnostním hrozbám souvisejícím s rostoucím extremismem, migrační krizí, hrozbou teroristických útoků (včetně kyberterorismu) a celkově s činnostmi proti zájmům ČR, EU a NATO. To, zda budou mít příslušné bezpečnostní složky v předmětném boji převahu, závisí kromě jiného na precizní a důsledné ochraně UI. [36]

Zajištění ochrany UI není doménou pouze samotného státu, ale závisí zejména na pečlivém přístupu všech osob a subjektů, které mohou v rámci své činnosti přijít s UI do styku. Z toho důvodu je důležitá kvalitní právní úprava v dané oblasti.

V situaci, kdy podnikatel zpravidla naváže obchodní kontakt (jednání s cílem uzavřít smlouvu o dílo,…) s jinou institucí či obchodním partnerem, který požaduje, aby byl podnikatel držitelem platného osvědčení podnikatele (Důvěrné, Tajné, Přísně tajné), protože při plnění podmínek smlouvy se bude seznamovat s UI příslušného stupně utajení či mu UI budou poskytovány nebo u něho budou vznikat, nastává chvíle, kdy se statutární orgán podnikatele rozhodne podat na NBÚ žádost o vydání osvědčení podnikatele. Na základě podané žádosti NBÚ zahájí tzv. bezpečnostní řízení, ve kterém ověřuje, zda podnikatel splňuje všechny podmínky pro vydání osvědčení podnikatele. V případě, že podnikatel všechny podmínky splňuje, vydá NBÚ rozhodnutí a v návaznosti na toto rozhodnutí veřejnou listinu, tzv. osvědčení podnikatele.

### 2.5.1 Základní pojmy

Základním právním předpisem pro oblast UI je zákon č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti ve znění pozdějších předpisů (dále jen „zákon o ochraně UI“). Pro účely tohoto zákona jsou v § 2 vymezeny základní pojmy v oblasti UI. V následujících odstavcích jsou uvedeny a popsány vybrané pojmy, které se vztahují k předmětu diplomové práce.

**Utajovaná informace** je *„informace v jakékoliv podobě zaznamenaná na jakémkoliv nosiči označená v souladu s tímto zákonem, jejíž vyzrazení nebo zneužití může způsobit újmu zájmu České republiky nebo může být pro tento zájem nevýhodné, a která je uvedena v seznamu utajovaných informací.“* [13] Z předmětné definice vyplývá, že se jedná o takovou informaci, která splňuje všechny uvedené znaky, které mohou mít povahu formální nebo materiální. Pod znaky formálního charakteru lze podhrnout zaznamenání UI a její označení příslušným stupněm utajení (Vyhrazené, Důvěrné, Tajné, Přísně tajné). Dalším znakem formálního charakteru je požadavek na její uvedení v seznamu UI. Tento seznam zpracovává NBÚ a vydává jej vláda svým nařízením. Konkrétně se jedná o nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací, ve znění pozdějších předpisů. Pro určení UI však nelze použít doslovný výklad definice, jelikož UI nemusí být konkrétně uvedena v seznamu UI, avšak je možno ji pod některou z položek seznamu UI subsumovat. Současně je nutno uvést, že ne každá informace, kterou lze podhrnout pod některou z položek seznamu UI, musí být informací utajovanou. Při posuzovaní, zda je daná informace informací utajovanou, je rozhodující skutečnost,

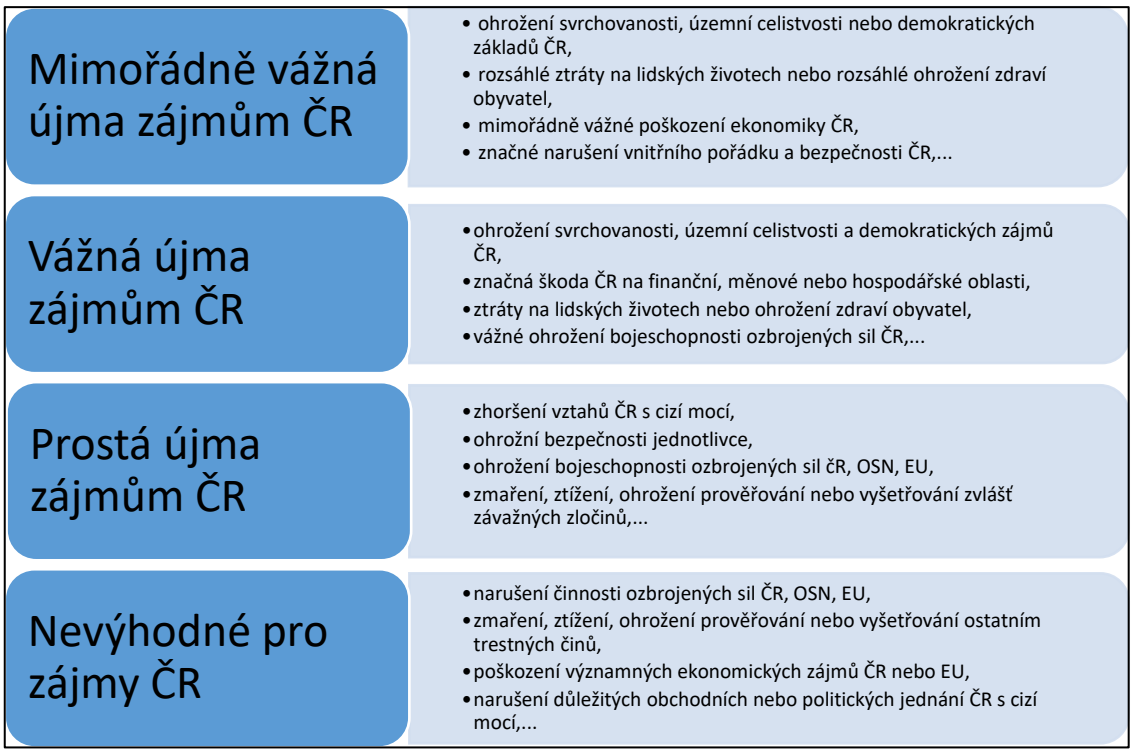
zda případné vyzrazení nebo zneužití informace může způsobit újmu zájmu ČR nebo může být pro zájem ČR nevýhodné. Zohlednění této skutečnosti lze považovat za zohlednění materiální stránky, kterou předmětná definice obsahuje. [37]

**Zájmem ČR** se rozumí *„zachování její ústavnosti, svrchovanosti a územní celistvosti, zajištění vnitřního pořádku a bezpečnosti, mezinárodních závazků a obrany, ochrana ekonomiky a ochrana života nebo zdraví fyzických osob.“* [13] Uvedená definice již z podstaty věci vykazuje určitou podobnost s ustanovením čl. 1 ústavního zákona č. 110/1993 Sb., o bezpečnosti České republiky, ve znění pozdějších předpisů, který uvádí, že *„zajištění svrchovanosti a územní celistvosti České republiky, ochrana jejích demokratických základů a ochrana životů, zdraví a majetkových hodnot je základní povinností státu.“* [10] Uvedené definice tak zobrazují provázanost jednotlivých segmentů bezpečnostního systému.

V návaznosti na předchozí definice lze nyní vymezit UI podle jednotlivých stupňů utajení:

- **Přísně tajné** – její vyzrazení neoprávněné osobě nebo zneužití může způsobit mimořádně vážnou újmu zájmům ČR;
- **Tajné** – její vyzrazení neoprávněné osobě nebo zneužití může způsobit vážnou újmu zájmům ČR;
- **Důvěrné** – její vyzrazení neoprávněné osobě nebo zneužití může způsobit prostou újmu zájmům ČR;
- **Vyhrazené** – její vyzrazení neoprávněné osobě nebo zneužití může být nevýhodné pro zájmy ČR. [13]

Následky vyzrazení nebo zneužití UI jsou uvedeny na obrázku 6.




*Obrázek 6 Následky vyzrazení (zneužití) UI*

Obsahem pojmu **porušení povinnosti při ochraně UI** je de iure porušení povinností uložené zákonem o ochraně UI nebo na základě tohoto zákona. [13] Jestliže je fyzická či právnická osoba držitelem osvědčení pro přístup k UI, tak je povinna po celou tuto dobu splňovat všechny podmínky dle zákona o ochraně UI. V souvislosti s podnikateli (právnickými osobami a podnikajícími fyzickými osobami) je v § 18 zákona o ochraně UI vymezen výčet bezpečnostních rizik, která jsou charakteru obligatorního a fakultativního. V případě, že je u podnikatele shledáno bezpečnostní riziko, dochází v samotném důsledku k situaci, že podnikatel přestává splňovat podmínku bezpečnostní spolehlivosti určenou v § 16 odst. 1 písm. b) zákona o ochraně UI. Jedním z bezpečnostních rizik fakultativního charakteru je porušení povinnosti při ochraně UI. Vzhledem k fakultativnímu charakteru uvedeného rizika je pro závěr o ohrožení zájmů ČR důležité posouzení všech souvisejících skutečností a zjištěných okolností jako celku. V tomto spočívá také rozdíl mezi fakultativním a obligatorním bezpečnostním rizikem.

V rámci této diplomové práce, resp. její praktické části, zaznívá také pojem „odpovědná osoba“. Tento pojem je kodifikován v zákonu o ochraně UI a přímo vymezuje osobu, která je dle tohoto zákona oprávněna jednat za podnikatele ve věcech týkajících se zákona o ochraně UI. Dle zákona o ochraně UI je **odpovědnou osobou**:

- u ministerstva ministr (člen vlády);
- u jiného ústředního správního úřadu ten, kdo stojí v jeho čele;
- u organizační složky státu, zřízené jinou organizační složkou státu ten, kdo je odpovědnou osobou u organizační složky státu vykonávající funkci jejího zřizovatele;
- u dalších organizačních složek státu ten, kdo stojí v jejich čele;
- u BIS a VZ ředitel;
- u ČNB guvernér;
- u kraje ředitel krajského úřadu;
- u hlavního města Prahy ředitel Magistrátu hlavního města Prahy;
- u městské části hlavního města Prahy tajemník úřadu městské části, pokud není, tak starosta městské části;
- u statutárního města tajemník magistrátu;
- u dalších měst (obcí) tajemník městského (obecního) úřadu, pokud není, tak starosta města (obce),
- u organizační složky územního samosprávného celku ten, kdo je odpovědnou osobou u územního samosprávného celku vykonávajícího funkci jejího zřizovatele;
- **u právnických osob odlišných od předchozích** statutární orgán; jedná-li jménem těchto jiných právnických osob více osob, které jsou statutárním orgánem, nebo osoba, která statutárním orgánem není, pak je odpovědnou osobou pouze ta z nich, která je jednáním ve věcech upravených zákonem o ochraně UI pověřena;
- **v případě podnikající fyzické osoby** je to sama podnikající fyzická osoba.

Poslední dva uvedené (zvýrazněné) příklady se týkají tématu (předmětu) mé diplomové práce. Jedná se o osoby, které lze zahrnout pod pojem „podnikatel“ ve smyslu

ustanovení § 420 a § 421 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů. [19]

### 2.5.2 Právní předpisy a další dokumenty

Novodobá historie právního zakotvení problematiky UI se váže k zákonu č. 102/1971 Sb., o ochraně státního tajemství. Tento předpis měl v novelizovaném znění nezastupitelné místo v právním řádu i po roce 1989, jelikož byl i poté jediným zákonem, ve kterém byla problematika tzv. státního tajemství řešena. Zákon byl zrušen teprve ke dni 1. 11. 1998, kdy nabyl účinnosti zákon č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů. Tímto zákonem došlo ke zřízení nového úřadu, kterým je NBÚ. V roce 2005 byl schválen nový, zatím poslední **zákon o ochraně UI**, který nabyl účinnosti ke dni 1. 1. 2006. Podle kompetenčního zákona (zákon č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy České republiky, ve znění pozdějších předpisů), lze od tohoto data hovořit o NBÚ jako o ústředním orgánu státní správy pro ochranu UI. [38] Předmětem úpravy zákona o ochraně UI jsou *„zásady pro stanovení informací jako informací utajovaných, podmínky pro přístup k nim a další požadavky na jejich ochranu, zásady pro stanovení citlivých činností a podmínky pro jejich výkon a s tím spojený výkon státní správy.“* [13]

Souvisejícím právním předpisem je dále **zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)**, který *„upravuje práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti“*, a to i přes skutečnost, že daný zákon ze své působnosti přímo vylučuje informační a komunikační systémy, které nakládají s UI. Dne 1. 8. 2017 vznikl **Národní úřad pro kybernetickou a informační bezpečnost** (dále jen „NÚKIB“), který od NBÚ převzal část agendy ochrany UI, konkrétně bezpečnost informačních a komunikačních systémů a kryptografickou ochranu UI. Působnost v této oblasti byla NÚKIB svěřena novelou zákona o ochraně UI. NÚKIB ve své podstatě vznikl na základě odštěpení sekcí kybernetické bezpečnosti NBÚ (Národního centra kybernetické bezpečnosti a Národního centra PRS – Public Regulated Service). [38]

Za prameny právní úpravy ochrany UI lze považovat také následující předpisy:

- zákon č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů;

- zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů;
- zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů aj.

Oblast ochrany UI je dotčena také právními předpisy **EU** (rozhodnutí Rady 2013/488/EU ze dne 23. září 2013, o bezpečnostních pravidlech na ochranu utajovaných informací EU, Rozhodnutí Komise 2001/844/ES, ESUO, Euratom ze dne 29. listopadu 2001, kterým se mění její jednací řád, Nařízení Rady č. 3, kterým se provádí článek 24 Smlouvy o založení Evropského společenství pro atomovou energii) a dále předpisy **NATO**, z nichž většina není volně k dispozici nebo je přímo označena jako UI. [36]

K zákonu o ochraně UI byla vydána řada prováděcích právních předpisů. Na úvod jejich výčtu je nutno uvést **nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací**, ve znění pozdějších předpisů (dále jen „nařízení vlády č. 522/2005 Sb.“), které ve svých přílohách stanovuje seznamy UI z jednotlivých oblastí působnosti, např. z oblastí působnosti ministerstev, ČNB, ČTÚ, SSHR, NBÚ, NÚKIB, aj. Položky uvedené v seznamech však apriori nepředstavují UI. Při posuzování, zda informace spadající pod položku ze seznamu lze klasifikovat příslušným stupněm utajení, je rozhodné, jestli při jejím vyzrazení nebo zneužití může být způsobena újma zájmům ČR nebo může být pro zájem ČR nevýhodné. [39] Předmětné nařízení vlády prošlo za dobu své platnosti několika novelizacemi, z nichž poslední nabyla účinnosti k 1. 1. 2019. V rámci předmětné novely byly modifikovány stávající položky seznamu UI a současně doplněny položky nové.

Dalšími prováděcími právními předpisy v oblasti ochrany UI jsou prováděcí vyhlášky, které se vztahující ke konkrétním oblastem zajištění ochrany UI:

### A) Oblast personální bezpečnosti

Personální bezpečností je druh zajištění ochrany UI, který *„tvoří výběr fyzických osob, které mají mít přístup k utajovaným informacím, ověřování podmínek pro jejich přístup k utajovaným informacím, jejich výchova a ochrana.“* [13] Personální bezpečnost je základním druhem ochrany UI a je upravena v hlavě II zákona o ochraně UI.

Prováděcím právním předpisem v oblasti personální bezpečnosti je **vyhláška NBÚ č. 363/2011 Sb., o personální bezpečnosti a o bezpečnostní způsobilosti**, ve znění pozdějších předpisů. Tato vyhláška obsahuje vzory formulářů vztahujících se k personální bezpečnosti a bezpečnostní způsobilosti, dále obsahuje informace k žádosti fyzické osoby o vydání osvědčení či dokladu a zároveň informace k hlášení změn údajů fyzických osob, které jsou držiteli platného osvědčení či dokladu.

### B) Oblast průmyslové bezpečnosti

Průmyslovou bezpečností je rozuměn *„systém opatření k zjišťování a ověřování podmínek pro přístup podnikatele k utajovaným informacím a k zajištění nakládání s utajovanou informací u podnikatele v souladu se zákonem o ochraně UI.“* [13] Uvedená oblast je upravena v hlavě III zákona o ochraně UI. Prováděcím právním předpisem v dané oblasti je **vyhláška NBÚ č. 405/2011 Sb., o průmyslové bezpečnosti**, ve znění pozdějších předpisů, jejíž přílohy obsahují vzory formulářů vztahujících se k průmyslové bezpečnosti. V předmětné vyhlášce jsou dále zaneseny informace k žádosti podnikatele o vydání osvědčení a k hlášení změn údajů podnikatele, který je držitelem platného osvědčení.

### C) Oblast administrativní bezpečnosti

Administrativní bezpečností rozumíme druh zajištění ochrany UI, který *tvoří „systém opatření při tvorbě, příjmu, evidenci, zpracování, odesílání, přepravě, přenášení, ukládání, skartačním řízení, archivaci, případně jiném nakládání s utajovanými informacemi.“* [13] Danou oblast upravuje hlava IV zákona o ochraně UI a současně **vyhláška č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací**, ve znění pozdějších předpisů, která mj. stanoví způsob vyznačování náležitostí na UI v listinné a nelistinné podobě, druhy administrativních pomůcek a podrobnosti k přepravě, přenášení, převzetí, zapůjčování a jiné manipulaci s utajovaným dokumentem.

### D) Oblast fyzické bezpečnosti

Fyzickou bezpečnost *tvoří „systém opatření, která mají neoprávněné osobě zabránit nebo ztížit přístup k utajovaným informacím, popřípadě přístup nebo pokus o něj zaznamenat.“* [13] Oblast fyzické bezpečnosti je zanesena v hlavě V zákona o ochraně UI a současně ve **vyhlášce NBÚ č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků**, ve znění pozdějších předpisů (dále jen „vyhláška č. 528/2005 Sb."), která stanoví bodové ohodnocení jednotlivých opatření fyzické bezpečnosti, nejnižší míru zabezpečení zabezpečené oblasti a jednací oblasti, základní metodu hodnocení rizik, další požadavky na opatření fyzické bezpečnosti a náležitosti certifikace technického prostředků.

### E) Bezpečnost informačních nebo komunikačních systémů

Bezpečnost informačních nebo komunikačních systémů tvoří *„systém opatření, jejichž cílem je zajistit důvěrnost, integritu a dostupnost UI, s nimiž tyto systémy nakládají a odpovědnost správy a uživatele za jejich činnost v těchto systémech.“* [13] Zákon o ochraně UI upravuje tuto oblast v hlavě VI. Jak je již výše uvedeno, státní správu v oblasti ochrany UI dle této hlavy vykonává NÚKIB. Souvisejícím právním předpisem je **vyhláška NBÚ č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor**, ve znění pozdějších předpisů.

### F) Kryptografická ochrana

Kryptografickou ochranu tvoří systém opatření na ochranu UI použitím kryptografických metod a materiálů při zpracování, přenosu nebo ukládání UI. Upravena je v hlavě VIII zákona o UI. Mezi prováděcí právní předpisy lze zařadit **vyhlášku NBÚ č. 525/2005 Sb., o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací**, ve znění pozdějších předpisů **a vyhlášku NBÚ č. 432/2011 Sb., o zajištění kryptografické ochrany utajovaných informací**, ve znění pozdějších předpisů. Státní správu v dané oblasti opět vykonává NÚKIB.

## 2.6 Systém ochrany utajovaných informací u podnikatelů

Systém ochrany UI lze zjednodušeně definovat jako souhrn opatření, které podnikatel realizuje z důvodu zajištění ochrany UI. Z hlediska zákonného je nutno stanovit tento systém ochrany již v rámci žádosti o vydání osvědčení podnikatele, kterou spolu s dalšími dokumenty předkládá NBÚ. Stanovení systému deklaruje podnikatel dokumentem, jehož obsah je uveden v § 98 zákona o ochraně UI a nazývá se „bezpečnostní dokumentace podnikatele“ (dále jen „bezpečnostní dokumentace“). Bezpečnostní dokumentace je dokumentem, ve kterém podnikatel na vlastních konkrétních podmínkách rozpracovává způsob ochrany UI za užití jednotlivých druhů zajištění ochrany UI s ohledem na formu přístupu podnikatele k UI. [40]

Užití jednotlivých druhů ochrany UI závisí na formě přístupu podnikatele k UI, která určuje způsob, jakým bude podnikatel k UI přistupovat. V praxi zákon o ochraně UI v § 20 rozlišuje dvě formy přístupu k UI:

- **UI u podnikatele vzniká, nebo je mu poskytnuta (tzv. poskytování a vznik UI);**
- UI u podnikatele nevzniká, ani mu není poskytována, ale mají k ní přístup zaměstnanci podnikatele nebo osoby jednající jménem podnikatele nebo za podnikatele, a to v souvislosti s výkonem pracovní nebo jiné činnosti pro podnikatele na základě smlouvy (tzv. seznamování se s UI). [41]

Jak je již výše uvedeno, obsah bezpečnostní dokumentace podnikatele stanoví systém ochrany UI u podnikatele. Bezpečnostní dokumentace musí být u podnikatele uložena a průběžně aktualizována.

Obsahem této dokumentace je dle zákona o ochraně UI:

- Výčet UI uložených u podnikatele a specifikace UI, k nimž by měl mít podnikatel přístup (v případě, že by mu UI měla být poskytnuta nebo by u něj měla vzniknout na základě zakázky, uvádí podnikatel také předpokládanou specifikaci zakázky) – podnikatel zpravidla vychází z informací poskytnutých potencionálním zadavatelem a dále z nařízení vlády č. 522/2005 Sb.

- Analýza možného ohrožení UI, vhodná a účinná ochranná opatření ke snížení rizik – tato analýza představuje vlastní hodnocení podmínek u podnikatele ve vztahu k ochraně UI. Podnikatel se při jejím zpracování zaměřuje na zjištění faktických i potencionálních rizik z oblasti lidských zdrojů, technických prostředků, přičemž zohledňuje i rizika vně objektu, ve kterém se nachází/bude nacházet tzv. zabezpečená oblast.
- Způsoby realizace jednotlivých druhů zajištění ochrany UI – konkrétní druhy ochrany využívané podnikatelem souvisí s formou přístupu podnikatele k UI a dále i se způsobem, jakým bude podnikatel s UI nakládat. V případě formy přístupu dle **§ 20 odst. 1 písm. a) zákona o ochraně UI** (tzv. poskytování a vznik UI) podnikatel realizuje nejméně opatření v oblasti **personální, administrativní a fyzické bezpečnosti**. Oblast fyzické bezpečnosti popisuje v projektu fyzické bezpečnosti, který je přílohou bezpečnostní dokumentace. Oblast bezpečnosti informačních a komunikačních systémů a kryptografickou ochranu podnikatel řeší samostatně, jelikož je již předmětem samostatného řízení, které vede NÚKIB. V případě formy přístupu dle **§ 20 odst. 1 písm. b) zákona o ochraně UI** podnikatel realizuje **pouze** opatření v oblasti **personální bezpečnosti.**
- Seznam funkcí a osob, u kterých podnikatel předpokládá přístup k UI – podnikatel jej vypracovává s ohledem na aktuální potřeby zabezpečení své činnosti. [40]

## 2.7 Povinnosti podnikatele při ochraně utajovaných informací

Po celou dobu, kdy je podnikatel držitelem platného osvědčení pro přístup k UI, musí splňovat všechny podmínky stanovené zákonem o ochraně UI pro vydání osvědčení podnikatele. Podle § 16 zákona o ochraně UI se jedná o následující podmínky, kdy podnikatel musí být:

- ekonomicky stabilní,
- bezpečnostně spolehlivý,
- schopen zabezpečit ochranu UI,
- odpovědná osoba musí být držitelem platného osvědčení fyzické osoby nejméně pro takový stupeň utajení jako podnikatel.

Poslední podmínkou je úhrada správního poplatku, která se však vztahuje pouze na řízení o žádosti o vydání osvědčení.

Jak je již uvedeno v předchozí kapitole, bezpečnostně spolehlivý podnikatel je ten, u něhož je vyloučena existence bezpečnostního rizika. Jedním z bezpečnostních rizik fakultativního charakteru je porušení povinnosti při ochraně UI. Existenci uvedeného rizika může NBÚ vyhodnotit například na základě výsledků prováděných kontrol zaměřených na dodržování povinností podnikatele a na zajištění ochrany UI u podnikatele.

Podnikatel, který je držitelem platného osvědčení pro přístup k UI, má současně celou řadu dalších povinností, které musí po celou dobu držitelství dodržovat. V případě jejich nedodržení je podnikatel ohrožen rizikem uložení sankce, a to v případech definovaných v zákoně o ochraně UI a v neposlední řadě tím, že přestane splňovat výše uvedené podmínky.

# 3 Cíl práce a hypotézy

Cílem diplomové práce je analýza systému vlastní ochrany UI u vybraných podnikatelů z odlišných oblastí podnikání, v rámci jejichž činnosti je požadován přístup k UI, resp. zjištění, zda je systém ochrany UI v rámci jednotlivých subjektů odlišný z pohledu možných hrozeb, míry rizika jejich výskytu a definovaných opatření k eliminace těchto rizik. Konkrétně se jedná o subjekty z oblasti energetiky, informatiky a dopravy. Pro ověření cíle jsou stanoveny následující hypotézy.

**HYPOTÉZA 1:** Lze předpokládat, že u všech porovnávaných subjektů je v systému ochrany UI lidský faktor považován za slabinu.

**HYPOTÉZA 2:** Za daného stavu lze předpokládat, že ochrana UI je u všech subjektů bez ohledu na předmět podnikání nastavena obdobným způsobem.

**HYPOTÉZA 3:** Při porovnání údajů z analýzy rizik jednotlivých subjektů lze předpokládat, že celková míra rizika bude nižší u subjektu z oblasti dopravy než u subjektu z oblasti energetiky.

# 4 Metodika

Metoda je soustavný postup, který v dané oblasti vede k cíli, a to nejlépe nezávisle na schopnostech toho, kdo ho provádí. Metodikou rozumíme teoreticko-praktické schéma určující postup provádění určité odborné činnosti. [42] Na základě uvedených konstatování lze odvodit, že metodika diplomové práce obecně odráží vlastní přístup k řešení tématu a vlastní schopnost volby metody s ohledem na charakter cíle práce.

## 4.1 Použité metody

V rámci této diplomové práce jsou k analýze systému ochrany UI sestaveny k jednotlivým podnikatelským subjektům SWOT matice, jejichž výsledky jsou následně komparativně porovnány. Předmětná metoda (SWOT analýza) je vybrána z toho důvodu, že při zpracovávání bezpečnostní dokumentace podnikatelé vycházejí z vlastní vnitřní a vnější analýzy, která je pro zpracování bezpečnostní dokumentace nezbytná. Z tohoto důvodu je SWOT analýza dle mého názoru nejvhodnější metodou pro zhodnocení informací vyplývajících z dokumentů jednotlivých subjektů.

SWOT analýzu lze definovat jako jednu z metod strategické analýzy, kdy na základě vnitřní analýzy, resp. definování silných stránek – strenghts, a stránek slabých – weaknesses, a vnější analýzy, resp. určení příležitostí – oportunities a hrozeb – threats, jsou generovány alternativy strategií. [43] V daném případě použitá SWOT analýza definuje silné a slabé stránky ochrany UI u vybraných subjektů a současně zobrazuje příležitosti a hrozby související s danou oblastí. Silné a slabé stránky představují interní část SWOT analýzy (uvnitř systému), naopak příležitosti a hrozby představují vnější vlivy na systém (část externí). Interní část se týká přímo společnosti a v podstatě se jedná o soupis kladů a záporů. Externí část je spojena s okolím společnosti, které lze těžko ovlivnit, ale které společnost výrazně ovlivňuje. SWOT analýza je ve svém důsledku určitou rozvahou. Je nástrojem dlouhodobého plánování, přičemž hodnotí fungování (v tomto případě soubor opatření k ochraně UI) a pomáhá nalézt problémy nebo nové možnosti ke zlepšení současného stavu. [44] V daném případě lze obecně uvést,

že provedené SWOT analýzy je možno využít k identifikaci kritických oblastí podnikatelů ve vztahu k UI.

Komparativní analýzu je možno v širším spektru definovat jako metodu, která se zakládá na srovnání vlastností několika různých jevů, v našem případě systémů. Komparace je metodou, jejíž postup je aplikovatelný ve všech vědních oblastech a oborech.

## 4.2 Postup zpracování diplomové práce

Při zpracování teoretické části diplomové práce bylo využito informací z odborných publikací, které byly získány na základě provedené vlastní rešerše. Tyto publikace byly zapůjčeny zejména z Městské knihovny v Praze a z Odborné knihovny ČNB. Část publikací byla využita z vlastních zdrojů. S ohledem na specifické téma diplomové práce je nutno uvést, že se počet vydaných publikací týkajících se ochrany UI limitně blíží k nule. Z tohoto důvodu byla v rámci přípravy na vypracování práce provedena ve spolupráci s pracovnicí Ústřední knihovny ČVUT jemná rešerše dalších dostupných zdrojů. V neposlední řadě byly k vypracování diplomové práce prostudovány a využity právní předpisy a další dokumenty, které jsou v přímém vztahu se zajištěním bezpečnosti ČR a dále s ochranou UI.

K analýze systému ochrany UI jsou v rámci diplomové práce využity skutečnosti vyplývající jak z bezpečnostních dokumentací, tedy z dokumentů, ve kterých jednotlivé subjekty (v tomto případě z oblasti energetiky, informatiky a dopravy) stanovují a popisují realizovaný systém ochrany UI, tak ze skutečností a poznatků získaných v rámci pracovního procesu a zároveň z informací poskytnutých HZS ČR, na jejichž základě se v souhrnu lze s údaji uvedenými v bezpečnostní dokumentaci ztotožnit. Důležitým aspektem pro výběr subjektů byl stupeň utajení, kterým v rámci přístupu k UI dané subjekty disponují. Vybrány byly pouze subjekty, které jsou držiteli osvědčení pro přístup k UI stupně utajení Důvěrné a vyšší, a to z toho důvodu, že pro přístup k UI stupně utajení Vyhrazené postačuje podnikatelům vydání vlastního písemného prohlášení, kterým doloží svou schopnost zabezpečit ochranu UI. Dalším důležitým aspektem

pro výběr subjektů byla forma přístupu k UI. Pro účely výzkumu tak byly vybrány subjekty, které zajišťují ochranu UI personální, administrativní, fyzickou bezpečností a současně bezpečností informačních systémů. Vybrané subjekty byly vybrány tak, aby si svými charakteristickými vlastnostmi, uvedenými v tabulce 2, byly podobné. Toto kritérium bylo zvoleno z toho důvodu, aby prováděný výzkum měl objektivně vypovídající hodnotu a aby zároveň výsledky předmětného výzkumu bylo možno považovat za relevantní.

*Tabulka 2 Charakteristika vybraných subjektů*

| | Subjekt energetika | Subjekt informatika | Subjekt doprava |
|---|---|---|---|
| **Osvědčení podnikatele pro přístup k UI** (Důvěrné a vyšší) | x | x | x |
| **Forma přístupu k UI** (tzv. poskytování a vznik UI) | x | x | x |
| **Nakládání s UI v informačním systému** | x | x | x |
| **Strategický význam podnikatele pro ČR** (v souvislosti s předmětem podnikání a realizovanou činností) | x | x | x |

Vzhledem ke skutečnosti, že pro vlastní výzkum byly vybrány subjekty, jejichž charakter činnosti je možno považovat za strategický, a současně s ohledem na skutečnost, že tato diplomová práce bude veřejně přístupná, nebudou zde uvedeny informace vedoucí k identifikaci popisovaných subjektů. S ohledem na charakter výzkumu je však plně dostačující informace o oblasti podnikání vybraných subjektů.

Bezpečnostní dokumentací se v souvislosti s ochranou UI rozumí dokument obsahující výčet UI, analýzu možného ohrožení UI, včetně opatření pro eliminaci rizik, způsoby realizace jednotlivých druhů zajištění UI a seznam funkcí a osob, u kterých se předpokládá přístup k UI. [13]

Předmětné skutečnosti jsou v rámci diplomové práce identifikovány sestavením SWOT analýz ochrany UI jednotlivých subjektů, resp. určením silných a slabých stránek, příležitostí a hrozeb. U silných stránek a příležitostí (viz tabulka 3) je použita pro hodnocení jednotlivých položek stupnice hodnot od 1 do 5 s tím, že 5 znamená nejvyšší spokojenost (největší atraktivita) a 1 nejnižší spokojenost (nejmenší atraktivita).

U slabých stránek a hrozeb (viz tabulka 4) je využívána také stupnice hodnot od 1 (nejnižší nespokojenost/nejmenší závažnost) do 5 (nejvyšší nespokojenost/největší závažnost).

*Tabulka 3 Hodnocení silných stránek/příležitostí*

| **SILNÁ STRÁNKA/ PŘÍLEŽITOST** | **Nejvyšší spokojenost/ Největší atraktivita** | **Vysoká spokojenost/ Velká atraktivita** | **Standard** | **Nízká spokojenost/ Malá atraktivita** | **Nejnižší spokojenost/ Nejmenší atraktivita** |
|---|---|---|---|---|---|
| **HODNOCENÍ** | 5 | 4 | 3 | 2 | 1 |

*Tabulka 4 Hodnocení slabých stránek/hrozeb*

| **SLABÁ STRÁNKA/ HROZBA** | **Nejvyšší nespokojenost/ Největší závažnost** | **Vysoká nespokojenost/ Velká závažnost** | **Standard** | **Nízká nespokojenost/ Malá závažnost** | **Nejnižší nespokojenost/ Nejmenší závažnost** |
|---|---|---|---|---|---|
| **HODNOCENÍ** | 5 | 4 | 3 | 2 | 1 |

Definované hodnoty jednotlivých položek SWOT matic byly současně konzultovány s odborníky v daných oblastech z důvodu ověření kvality jejich vypovídající hodnoty. Výstupy analýz jsou dále komparativně porovnány. Na základě zjištěných skutečností jsou v neposlední řadě uvedeny návrhy dalších opatření k zajištění ochrany UI v souladu se splňováním podmínek nutných pro vydání osvědčení podnikatele, které musí podnikatel splňovat po celou dobu, kdy je držitelem osvědčení podnikatele.

# 5 Výsledky

V této kapitole jsou uvedeny výsledky z analýzy systémů vlastní ochrany UI u podnikatelů z odlišných oblastí podnikání, které jsou následně zhodnoceny formou komparativního porovnání a dále jsou zde uvedeny návrhy dalších opatření k zajištění ochrany UI.

## 5.1 Zajištění ochrany utajovaných informací u vybraných subjektů

Jak již z uvedených skutečností vyplývá, všechny analyzované subjekty, vybrané na základě určitých kritérií, realizují ve svém prostředí systém ochrany UI sestávající se z personální, administrativní, fyzické bezpečnosti a bezpečnosti informačních systémů.

**Personální bezpečnost** zahrnuje vedle ověřování podmínek, které musí fyzická osoba splnit, aby jí byl umožněn přístup k UI, také „výchovu“ těchto osob. Každoročně je odpovědná osoba povinna mj. zajistit školení těchto fyzických osob, které spočívá v proškolení z právních předpisů v oblasti ochrany UI. V rámci své funkce je odpovědná osoba podnikatele současně povinna neprodleně písemně oznámit NBÚ ukončení služebního nebo pracovního či jiného vztahu, ve kterém byl fyzické osobě umožněn přístup k UI. [41] Způsob a rozsah ověřování podmínek, které musí fyzická osoba splnit, se liší podle stupňů utajení, k nimž má mít daná osoba přístup. Podmínky, které musí daná fyzická osoba splňovat, jsou uvedeny v tabulce 5.

*Tabulka 5 Podmínky pro jednotlivé stupně UI [41]*

| **PODMÍNKY** | **VYHRAZENÉ** (oznámení; podmínky ověřuje podnikatel) | **DŮVĚRNÉ, TAJNÉ, PŘÍSNĚ TAJNÉ** (osvědčení; podmínky ověřuje NBÚ) |
|---|---|---|
| Svéprávnost | x | x |
| Věk minimálně 18 let | x | x |
| Bezúhonnost | x | x |
| Státní občanství ČR, země EU, NATO | | x |
| Osobnostní způsobilost | | x |
| Bezpečnostní spolehlivost | | x |

**Administrativní bezpečnost** ve svém důsledku úzce souvisí s bezpečností personální. Zahrnuje především opatření, která podnikatel, resp. osoby, které mají přístup k UI, realizují při tvorbě, příjmu, evidenci, zpracování, odesílání, přepravě, přenášení, ukládání, skartačním řízení, archivaci, případně jiném nakládání s UI. [45]

**Fyzickou bezpečnost** tvoří systém opatření, která mají neoprávněné osobě zabránit nebo ztížit přístup k UI, případně přístup nebo pokus o něj zaznamenat. Pro zabezpečení ochrany UI v rámci fyzické bezpečnosti se určují objekty, zabezpečené oblasti a jednací oblasti. Za objekt je možné považovat budovu či jiný ohraničený prostor, ve kterém se zpravidla nachází zabezpečená nebo jednací oblast, a kde je manipulováno s UI nebo se zde UI zpracovává. Zabezpečená oblast je zřízena za účelem ukládání UI, a to do umístěného trezoru nebo jiné uzamykatelné schránky. Zabezpečení této oblasti, objektu či jednací místnosti je zajišťováno kombinací opatření (ostraha, režimová opatření a technické prostředky). Rozsah použití uvedených opatření závisí na stupni utajení UI a vyhodnocení rizik. Pro ochranu zabezpečených oblastí kategorie Vyhrazené se používají certifikované nebo necertifikované technické prostředky, na rozdíl od oblastí kategorie Důvěrné a vyšší, pro jejichž ochranu se používají certifikované technické prostředky. Certifikace těchto prostředků provádí NBÚ. [41]

Požadavky na zajištění **bezpečnosti informačních systémů** jsou závislé na stupni utajení UI, s nimiž podnikatel v informačním systému nakládá. Jedná se o požadavky na bezpečnostní provozní mód a obsah bezpečnostní dokumentace informačního systému, které jsou uvedeny ve vyhlášce č. 523/2005 Sb., o bezpečnosti informačních

a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor, ve znění pozdějších předpisů. V případě, že podnikatel splňuje dle NÚKIB všechny požadavky, NÚKIB certifikuje podnikatelem užívaný informační systém pro nakládání s UI. [46]

Ze zákona o ochraně UI současně vyplývá i zajištění **průmyslové bezpečnosti**. Touto bezpečností je myšlen systém opatření k zajišťování a ověřování podmínek pro přístup podnikatele k UI a k zajištění nakládání s UI u podnikatele. [37] Tuto bezpečnost však ve své podstatě nerealizuje přímým způsobem podnikatel, ale NBÚ, který svou činností ověřuje výše uvedené splňování podmínek podnikatelem.

### 5.1.1 Subjekt z oblasti energetiky

V návaznosti na skutečnosti uvedené v předchozí kapitole jsou v tabulce 6 identifikovány silné a slabé stránky, včetně příležitostí a hrozeb v oblasti ochrany UI u subjektu z oblasti energetiky. Hodnocení jednotlivých položek bude předmětem komparace výsledků provedených SWOT analýz (viz kapitola 5.2).

*Tabulka 6 SWOT analýza ochrany UI – subjekt energetika*

| **Silné stránky**<br>**STRENGTHS** | | | **Slabé stránky**<br>**WEAKNESSES** | | |
|---|---|---|---|---|---|
| | | *hodno-cení* | | | *hodno-cení* |
| 1. | Pravidelná aktualizace bezpečnostní dokumentace | **4** | 1. | Selhání lidského faktoru (porušení povinností ostrahy, neloajalita zaměstnanců k zaměstnavateli, porušení povinností oprávněných osob - únik UI) | **2** |
| 2. | Přehlednost bezpečnostní dokumentace | **5** | 2. | Vyšší počet oprávněných osob s přístupem k UI (>10 osob) - únik UI | **2** |
| 3. | Výběr a odborná příprava fyzických osob s přístupem k UI | **4** | 3. | Ukončení pracovního poměru zaměstnanců, u kterých se předpokládá přístup k UI | **3** |
| 4. | Výkon funkce bezpečnostního ředitele a odpovědné osoby dvěma osobami | **5** | | | |
| 5. | Certifikovaný informační systém | **5** | | | |
| 6. | Dislokace objektu v území | **4** | | | |
| 7. | Instalace prvků systému technické ochrany | **4** | | | |
| 8. | Nepřetržitá ostraha budovy | **4** | | | |
| 9. | Režimová opatření v objektu | **4** | | | |
| **Příležitosti**<br>**OPPORTUNITIES** | | | **Hrozby**<br>**THREATS** | | |
| | | *hodno-cení* | | | *hodno-cení* |
| 1. | Možnost využití vzorové dokumentace vydané NBÚ (dosud nevydána) | **4** | 1. | Mimořádné události a krizové situace (živelná pohroma, havárie dopravního prostředku, průmyslová havárie,...) | **2** |
| 2. | Využití poradenských služeb externí firmy v oblasti ochrany UI | **4** | 2. | Pasivní odposlech, nasazení operativní techniky | **2** |
| 3. | Možnost časté obměny hardware a software z finančních zdrojů získaných ze státních zakázek, v rámci jejichž realizace je nutný přístup k UI | **3** | 3. | Nepředvídatelné kybernetické útoky | **2** |

**Silné stránky**

- Přehlednost bezpečnostní dokumentace – propracovanost bezpečnostní dokumentace s rozdělením na obecnou část a přílohy obsahující administrativní projekt a projekt fyzické bezpečnosti.
- Pravidelná aktualizace bezpečnostní dokumentace – nastavení interního algoritmu pro aktualizaci dokumentu.
- Výběr a příprava fyzických osob s přístupem k UI – pečlivý výběr zaměstnanců na konkrétní pozice, na kterých je požadován přístup k UI (nutnost držitelství oznámení nebo osvědčení fyzické osoby).
- Výkon funkce bezpečnostního ředitele a odpovědné osoby dvěma osobami – pověření výkonem funkce odpovědné osoby a jmenování další osoby bezpečnostním ředitelem – rozdělení kompetencí.
- Certifikovaný informační systém – důsledek splnění požadavků na informační systém, ve kterém subjekt nakládá s UI.
- Dislokace objektu v území – poloha objektu, ve kterém je subjekt umístěn, a ve kterém se současně nachází zabezpečená oblast podnikatele, a to v souvislosti s možným výskytem rizik (hrozeb) a dále s ohledem na vlastníka objektu a přítomnost dalších podnikatelských subjektů v objektu.
- Instalace prvků technické ochrany – využití prostředků technické ochrany v souvislosti s požadavky pro ochranu UI.
- Ostraha – zajištění výkonu ostrahy v souvislosti s minimálními požadavky pro ochranu UI.
- Režimová opatření – nastavení systému režimových opatření v souvislosti s požadavky pro ochranu UI.

**Slabé stránky**

- Selhání lidského faktoru – porušení povinností (nedbalostí či úmyslem) oprávněnými osobami a osobami bez přístupu k UI s následným možným únikem UI.
- Vyšší počet oprávněných osob s přístupem k UI (více než 10 osob) – vyšší pravděpodobnost zneužití/úniku UI.
- Ukončení pracovního poměru zaměstnanců, u kterých se předpokládá přístup k UI – možnost fluktuace osob v souvislosti s aktuálním stavem na trhu práce.

**Příležitosti**

- Možnost využití vzorové dokumentace vydané NBÚ (dosud nevydána) – využití možnosti vypracování přehledné bezpečnostní dokumentace na základě vzoru dokumentu.
- Využití poradenských služeb externí firmy v oblasti ochrany UI – možnost využití externí firmy k vypracování bezpečnostní dokumentace a nastavení systému ochrany UI.
- Možnost časté obměny hardware a software z finančních zdrojů získaných ze státních zakázek, v rámci jejichž realizace je nutný přístup k UI – zlepšení finanční situace subjektů s následnou rozpočtovou strategií.

**Hrozby**

- Mimořádné události a krizové situace – identifikované v analýze hrozeb pro dané území a uvedené v příslušném havarijním plánu kraje nebo krizovém plánu kraje, resp. vycházející z analýzy a vyhodnocení míry rizik provedené subjektem.
- Pasivní odposlech, nasazení operativní techniky – hrozba odposlechu nebo odezírání z prostor mimo zabezpečenou oblast, instalace odposlechové techniky, která směřuje k získání UI a dalších důležitých informací vycházejících z analýzy a vyhodnocení rizik provedené subjektem.
- Nepředvídatelné kybernetické útoky – ohrožení informačního systému, ve kterém je nakládáno s UI, s důsledkem úniku UI z informačního systému.

### 5.1.2 Subjekt z oblasti informatiky

Tabulka 7 zobrazuje silné a slabé stránky, včetně příležitostí a hrozeb v oblasti ochrany UI u subjektu z oblasti informatiky. Hodnocení jednotlivých položek bude předmětem komparace výsledků provedených SWOT analýz (viz kapitola 5.2).

*Tabulka 7 SWOT analýza ochrany UI – subjekt informatika*

| Silné stránky | | | Slabé stránky | | |
|---|---|---|---|---|---|
| STRENGTHS | | | WEAKNESSES | | |
| | | hodnocení | | | hodnocení |
| 1. | Pravidelná aktualizace bezpečnostní dokumentace | 5 | 1. | Selhání lidského faktoru (porušení povinností ostrahy, neloajalita zaměstnanců k zaměstnavateli, porušení povinností oprávněných osob - únik UI) | 2 |
| 2. | Přehlednost bezpečnostní dokumetace | 3 | 2. | Ukončení pracovního poměru zaměstnanců, u kterých se předpokládá přístup k UI | 1 |
| 3. | Výběr a odborná příprava fyzických osob s přístupem k UI | 4 | 3. | Výkon funkce bezpečnostního ředitele a odpovědné osoby jednou osobou | 2 |
| 4. | NIžší počet oprávněných osob s přístupem k UI (<10 osob) - únik UI | 4 | 4. | Dislokace objektu v území | 3 |
| 5. | Certifikovaný informační systém | 5 | | | |
| 6. | Instalace prvků systému technické ochrany | 4 | | | |
| 7. | Nepřetržitá ostraha budovy | 4 | | | |
| 8. | Režimová opatření v objektu | 4 | | | |
| **Příležitosti** | | | **Hrozby** | | |
| OPPORTUNITIES | | | THREATS | | |
| | | hodnocení | | | hodnocení |
| 1. | Možnost využití vzorové dokumentace vydané NBÚ (dosud nevydána) | 5 | 1. | Mimořádné události a krizové situace (živelná pohroma, havárie dopravního prostředku, průmyslová havárie,...) | 3 |
| 2. | Využití poradenských služeb externí firmy v oblasti ochrany UI | 4 | 2. | Pasivní odposlech, nasazení operativní techniky | 2 |
| 3. | Možnost časté obměny hardware a software z finančních zdrojů získaných ze státních zakázek, v rámci jejichž realizace je nutný přístup k UI | 4 | 3. | Nepředvídatelné kybernetické útoky | 2 |

V návaznosti na legendu k položkám uvedeným v předchozí SWOT matici lze uvést, že u subjektu z oblasti informatiky jsou definovány shodné položky, vyjma položek následujících:

**Silné stránky**

- Nižší počet oprávněných osob s přístupem k UI (méně než 10 osob) – nižší pravděpodobnost zneužití/úniku UI.

**Slabé stránky**

- Dislokace objektu v území je v daném případě zanesena do slabých stránek.
- Výkon funkce bezpečnostního ředitele a odpovědné osoby jednou osobou je v daném případě také slabou stránkou subjektu – všechny povinnosti jsou delegovány na jednu osobu.

### 5.1.3 Subjekt z oblasti dopravy

Následující tabulka 8 prezentuje silné a slabé stránky, včetně příležitostí a hrozeb v oblasti ochrany UI u subjektu z oblasti dopravy. Hodnocení jednotlivých položek bude předmětem komparace výsledků provedených SWOT analýz (viz kapitola 5.2).

*Tabulka 8 SWOT analýza ochrany UI – subjekt doprava*

| **Silné stránky** | | | **Slabé stránky** | | |
|---|---|---|---|---|---|
| **STRENGTHS** | | | **WEAKNESSES** | | |
| | | *hodnocení* | | | *hodnocení* |
| 1. | Pravidelná aktualizace bezpečnostní dokumentace | **3** | 1. | Selhání lidského faktoru (porušení povinností ostrahy, neloajalita zaměstnanců k zaměstnavateli, porušení povinností oprávněných osob - únik UI) | **3** |
| 2. | Přehlednost bezpečnostní dokumentace | **5** | 2. | Vyšší počet oprávněných osob s přístupem k UI (>10 osob) - únik UI | **2** |
| 3. | Výběr a odborná příprava fyzických osob s přístupem k UI | **4** | 3. | Ukončení pracovního poměru zaměstnanců, u kterých se předpokládá přístup k UI | **3** |
| 4. | Certifikovaný informační systém | **5** | 4. | Výkon funkce bezpečnostního ředitele a odpovědné osoby jednou osobou | **1** |
| 5. | Instalace prvků systému technické ochrany | **4** | 5. | Dislokace objektu v území | **2** |
| 6. | Nepřetržitá ostraha budovy | **4** | | | |
| 7. | Režimová opatření v objektu | **4** | | | |
| **Příležitosti** | | | **Hrozby** | | |
| **OPPORTUNITIES** | | | **THREATS** | | |
| | | *hodnocení* | | | *hodnocení* |
| 1. | Možnost využití vzorové dokumentace vydané NBÚ (dosud nevydána) | **4** | 1. | Mimořádné události a krizové situace (živelná pohroma, havárie dopravního prostředku, průmyslová havárie,...) | **3** |
| 2. | Využití poradenských služeb externí firmy v oblasti ochrany UI | **4** | 2. | Pasivní odposlech, nasazení operativní techniky | **1** |
| 3. | Možnost časté obměny hardware a software z finančních zdrojů získaných ze státních zakázek, v rámci jejichž realizace je nutný přístup k UI | **3** | 3. | Nepředvídatelné kybernetické útoky | **2** |

V návaznosti na legendu uvedenou u SWOT matice subjektu z oblasti informatiky lze uvést, že u subjektu z oblasti dopravy jsou definovány shodné položky, vyjma položek následujících:

**Slabé stánky**

- Vyšší počet oprávněných osob s přístupem k UI (více než 10 osob) – vyšší pravděpodobnost zneužití/úniku UI.

## 5.2 Komparace výsledků provedených analýz

Ve výše uvedených maticích SWOT analýz jsou definovány položky a hodnoty, které se vážou k danému subjektu. Tímto definováním však práce nekončí. Porovnáním hodnot vyplývajících z jednotlivých SWOT analýz lze následně určit prvotní výsledky, na jejichž základě je možno uvést konstatování o stavu systému ochrany UI. Výsledky předmětného porovnání jsou zobrazeny v tabulkách 9 – 11.

*Tabulka 9 Komparace hodnot – subjekt energetika*

| | Silné stránky | Slabé stránky | Příležitosti | Hrozby |
|---|---|---|---|---|
| Hodnocení celkem | 39 | 7 | 11 | 6 |
| Rozdíl | **32** | | **5** | |

*Tabulka 10 Komparace hodnot – subjekt informatika*

| | Silné stránky | Slabé stránky | Příležitosti | Hrozby |
|---|---|---|---|---|
| Hodnocení celkem | 33 | 8 | 13 | 7 |
| Rozdíl | **25** | | **6** | |

*Tabulka 11 Komparace hodnot – subjekt doprava*

| | Silné stránky | Slabé stránky | Příležitosti | Hrozby |
|---|---|---|---|---|
| Hodnocení celkem | 29 | 11 | 11 | 6 |
| Rozdíl | **18** | | **5** | |

Na základě výše uvedeného porovnání lze uvést, že u všech analyzovaných subjektů převyšují silné stránky a příležitosti nad slabými stránkami a hrozbami, z čehož v důsledku vyplývá, že systém ochrany UI je u předmětných subjektů nastaven tak, aby splňoval zákonné požadavky, resp. tak, aby byl podnikatel schopen zajistit ochranu UI.

Celkové hodnoty jsou však postačují pouze pro obecné zhodnocení „stavu“ systému. Hodnoty uvedené u jednotlivých položek ve SWOT analýzách je nutné považovat za ty, které mají v předmětné analýze vyšší vypovídající hodnotu, a to i přes skutečnost, že jejich určení je považováno za subjektivní. Z tohoto důvodu jsou v následujících odstavcích diplomové práce předmětné položky popsány a porovnány. Jednotlivé hodnoty u položek ve SWOT analýzách jsou důležité pro další využití, a to např. k návrhu dalších opatření se zaměřením na rozvíjení silných stránek, snížení slabých stránek s využitím příležitostí, a to takovým způsobem, aby se ze slabých stránek staly stránky silné, které je možné dále rozvíjet, a dále k eliminaci hrozeb, a to tak, aby se z nich nestaly slabé stránky.

- **Pravidelná aktualizace bezpečnostní dokumentace**

*Tabulka 12 Komparace – pravidelná aktualizace bezpečnostní dokumentace*

| **Subjekt – energetika** | **Subjekt – informatika** | **Subjekt – doprava** |
|---|---|---|
| **Silná stránka** | **Silná stránka** | **Silná stránka** |
| 4 | 5 | 3 |

Všechny subjekty mají zákonnou povinnost zpracovanou bezpečnostní dokumentaci aktualizovat. Ke splnění dané povinnosti je nutno, aby si podnikatel nastavil obecný algoritmus, který by jej upozornil při realizovaných změnách v systému, a v jehož důsledku by byla provedená změna zavedena do dokumentu. U subjektu z oblasti

energetiky a dopravy lze vidět limity u tohoto nastavení, které by bylo možno snížit využitím služeb externí společnosti v oblasti ochrany UI či u subjektu z oblasti energetiky využitím potenciálu samostatně jmenované osoby do funkce bezpečnostního ředitele.

- **Přehlednost bezpečnostní dokumentace**

*Tabulka 13 Komparace – přehlednost bezpečnostní dokumentace*

| Subjekt – energetika | Subjekt – informatika | Subjekt – doprava |
|---|---|---|
| Silná stránka | Silná stránka | Silná stránka |
| 5 | 3 | 5 |

U subjektů z oblasti energetiky a dopravy lze uvést, že bezpečnostní dokumentace je přehledně zpracována s důrazem na rozpracování jednotlivých druhů zajištění ochrany UI v samostatných přílohách. U subjektu z oblasti informatiky by ke zlepšení stavu bylo možno využít služeb externí poradenské společnosti v oblasti ochrany UI. Za ekonomičtější způsob lze uvést možnost využití konzultací na NBÚ nebo využití šablony NBÚ (dosud nevydané) k vytvoření přehledné bezpečnostní dokumentace. Nad rámec uvedeného je možno konstatovat, že přehledně a kvalitně zpracovaná dokumentace představuje základní aspekt samotné realizace systému ochrany UI a v průběhu platnosti osvědčení podnikatele je nedílnou součástí tohoto systému.

- **Výběr a příprava fyzických osob s přístupem k UI**

*Tabulka 14 Komparace – výběr a příprava fyzických osob s přístupem k UI*

| Subjekt – energetika | Subjekt – informatika | Subjekt – doprava |
|---|---|---|
| Silná stránka | Silná stránka | Silná stránka |
| 4 | 4 | 4 |

Z uvedených hodnot vyplývá, že subjekty již při výběru zaměstnanců na pozice, na nichž je nutný přístup k UI, kladou velký důraz na osobnostní profil a hodnocení jednotlivců, a to z toho důvodu, že je částečným předpokladem pro zvýšení pravděpodobnosti úspěšného ukončení následného bezpečnostního řízení za účelem vydání osvědčení fyzické osoby. V případě vydání oznámení podnikatelem pro přístup k UI stupně utajení Vyhrazené musí být daná fyzická osoba svéprávná, starší 18 let

a bezúhonná. Další podmínky (viz Tabulka 5) ověřovány nejsou. Z tohoto důvodu jsou hodnoty definovány indexem vysoká spokojenost, avšak ne nejvyšší. Ke zvýšení hodnoty může v daném případě pomoci precizní dodržování personální bezpečnosti s důrazem na kvalitní provádění periodických školení zaměstnanců zajištěné odpovědnou osobu podnikatele.

- **Výkon funkce bezpečnostního ředitele a odpovědné osoby dvěma osobami / jednou osobou**

*Tabulka 15 Komparace – výkon funkce bezpečnostního ředitele/odpovědné osoby*

| Subjekt – energetika | Subjekt – informatika | Subjekt – doprava |
|---|---|---|
| Silná stránka | Slabá stránka | Slabá stránka |
| 5 | 2 | 1 |

U subjektu z oblasti energetiky zastává funkci odpovědné osoby statutární orgán a do funkce bezpečnostního ředitele byla jmenována osoba, která je specialistou pro oblast bezpečnosti jako celku. Z tohoto důvodu je možno považovat tento stav, související s rozdělením kompetencí a v samotném důsledku i objemu práce, za silnou stránku subjektu. U dalších dvou subjektů vykonává funkci odpovědné osoby a bezpečnostního ředitele tatáž osoba, v případě subjektu z oblasti informatiky statutární orgán, u subjektu z oblasti dopravy osoba mimo statutární orgán, která u podnikatele vykonává současně funkci tzv. krizového manažera. S ohledem na funkci a specializaci těchto osob, které disponují klíčovými kompetencemi, je možno považovat tuto slabou stránku za takovou, u které není za daného stavu nutno pracovat na jejím zlepšení, resp. odstranění.

- **Certifikovaný informační systém**

*Tabulka 16 Komparace – certifikovaný informační systém*

| Subjekt – energetika | Subjekt – informatika | Subjekt – doprava |
|---|---|---|
| Silná stránka | Silná stránka | Silná stránka |
| 5 | 5 | 5 |

S ohledem na skutečnost, že všechny tři subjekty disponují požadovaným hardwarem, nastavením softwaru a dalšími prvky (fyzická bezpečnost informačního systému),

které splňují všechny podmínky nutné k certifikaci informačního systému, a na základě toho jim byl informační systém certifikován k nakládání s UI, je možno tuto skutečnost považovat za silnou stránku, se kterou jsou subjekty nejvíce spokojeny.

- **Dislokace objektu v území**

*Tabulka 17 Komparace – dislokace objektu v území*

| Subjekt – energetika | Subjekt – informatika | Subjekt – doprava |
|---|---|---|
| **Silná stránka** | **Slabá stránka** | **Slabá stránka** |
| 4 | 3 | 2 |

V návaznosti na informace zjištěné u HZS ČR je možno uvést, že dislokace objektu, ve kterém se nachází subjekt z oblasti energetiky, je silnou stránkou podnikatele, jelikož je umístěn mimo záplavovou oblast. V blízkosti je však stacionární zdroj ohrožení (zásobník chloru), ale riziko vnějšího ohrožení subjektu je minimální. Definovaná položka je u dalších dvou subjektů považována za slabou stránku, a to z toho důvodu, že objekty, ve kterých subjekty sídlí, se nacházejí v záplavovém území. Subjekt z oblasti dopravy však sídlí ve vyšším podlaží objektu. Opatřením vztahujícím se k ochraně UI je v daném případě důsledné dodržování činností vyplývajících z bezpečnostní dokumentace podnikatele (revizní zkoušky technologických zařízení, …), příp. zajištění vhodnější dislokace objektu (zabezpečené oblasti).

- **Instalace prvků technické ochrany**

*Tabulka 18 Komparace – instalace prvků technické ochrany*

| Subjekt – energetika | Subjekt – informatika | Subjekt – doprava |
|---|---|---|
| **Silná stránka** | **Silná stránka** | **Silná stránka** |
| 4 | 4 | 4 |

K zajištění ochrany UI jsou u subjektů naistalovány prvky technické ochrany, mezi které lze zahrnout mechanické zábrany, zařízení elektrické zabezpečovací signalizace či systém kontroly vstupu do objektu. Vzhledem ke skutečnosti, že předmětné subjekty mají nainstalovány prvky technické ochrany, jejichž bodová hodnota je v součtu totožná či dokonce převyšuje stanovenou minimální hodnotu pro danou kategorii zabezpečené

oblasti a podnikatelem definovanou míru rizika dle vyhlášky č. 528/2005 Sb., je možno tuto položku považovat za silnou stránku, se kterou jsou subjekty velmi spokojeny. Dobrovolné umístění prvků technické ochrany, které v souhrnu bodově spadají do „vyšší kategorie“ by pro podnikatele znamenalo jistě větší bezpečnostní výhodu (zvýšení hodnocení ve SWOT analýze), avšak také větší náklady, které není nezbytně nutné v daném případě vynakládat.

- **Ostraha**

*Tabulka 19 Komparace – ostraha*

| Subjekt – energetika | Subjekt – informatika | Subjekt – doprava |
|---|---|---|
| **Silná stránka** | **Silná stránka** | **Silná stránka** |
| 4 | 4 | 4 |

K zajištění ostrahy využívají subjekty externí bezpečnostní služby, jejichž zaměstnanci tuto zajišťují 24 hodin denně. Vzhledem ke skutečnosti, že subjekty využívají stejný typ ostrahy definovaný ve vyhlášce č. 528/2005 Sb., je možno položku považovat za silnou stránku, se kterou jsou subjekty velmi spokojeny. Dobrovolné zajištění ostrahy odpovídající vyššímu typu dle předmětné vyhlášky, by pro podnikatele také znamenalo jistě větší bezpečnostní výhodu (zvýšení hodnocení ve SWOT analýze), avšak také větší náklady, které není nezbytně nutné v daném případě vynakládat.

- **Režimová opatření**

*Tabulka 20 Komparace – režimová opatření*

| Subjekt – energetika | Subjekt – informatika | Subjekt – doprava |
|---|---|---|
| **Silná stránka** | **Silná stránka** | **Silná stránka** |
| 4 | 4 | 4 |

U všech subjektů spočívají režimová opatření v dodržování interních předpisů (zejména provozního řádu podnikatele) zaměstnanci, pracovníky ostrahy a návštěvníky. Vzhledem ke skutečnosti, že u všech subjektů jsou nastavena obdobná režimová opatření (vstup zaměstnanců do budovy pouze hlavním vstupem v pracovní době, vstup návštěv v pracovní době, ohlášení a identifikace návštěvy na recepci, vyzvednutí návštěvy

navštívenou osobou, příp. pohyb návštěvy po objektu pouze s doprovodem, namátková kontrola při výstupu), která v souvislosti s výběrem externí bezpečnostní služby a výběrem vlastních zaměstnanců zajišťuje podnikateli přidanou hodnotu v oblasti ochrany UI, je možno položku považovat za silnou stránku, se kterou jsou subjekty velmi spokojeny.

- **Selhání lidského faktoru**

*Tabulka 21 Komparace – selhání lidského faktoru*

| Subjekt – energetika | Subjekt – informatika | Subjekt – doprava |
|---|---|---|
| **Slabá stránka** | **Slabá stránka** | **Slabá stránka** |
| 2 | 2 | 3 |

Jednou ze slabých stránek, která je definována u všech subjektů, je možnost selhání lidského faktoru s následným únikem UI nebo jejich vyzrazením. Jednotlivé subjekty definovaly při vlastním hodnocení rizik interní hrozbu takto:

- vyzrazení UI osobami, které splňují zákonem stanovené podmínky přístupu k UI, a to jak úmyslně (umožnění přístupu k UI neoprávněné osobě, která nesplňuje zákonem stanovené podmínky přístupu k UI příslušného stupně utajení – poskytnutí, pořízení kopie, ústní sdělení UI), tak neúmyslnou formou (neuložení UI do úschovného objektu, porušení pravidel manipulace s UI);
- manipulace s UI neoprávněnými osobami – porušení interních předpisů podnikatele dalšími zaměstnanci, zaměstnanci ostrahy.

Subjekt z oblasti energetiky vyhodnotil, že riziko výskytu této hrozby je **malé**. Stejnou hodnotu určil v souvislosti s uvedenou hrozbou subjekt z oblasti informatiky. Subjekt z oblasti dopravy stanovil riziko v souvislosti s touto hrozbou jako **střední**. Hodnoty uvedené ve SWOT analýze tak přímo vycházejí z analýzy realizované podnikatelem. Opatřením pro eliminaci dané slabé stránky je pečlivý výběr zaměstnanců na pozice, u kterých je nutný přístup k UI, důsledné dodržování interních předpisů, včetně směrnice administrativní bezpečnosti, která je součástí bezpečnostní dokumentace podnikatele a dále důkladný výběr bezpečnostní služby zajišťující nepřetržitou ostrahu a dodržování dalších opatření fyzické bezpečnosti.

- **Vyšší/nižší počet oprávněných osob s přístupem k UI**

*Tabulka 22 Komparace – počet oprávněných osob s přístupem k UI*

| Subjekt – energetika | Subjekt – informatika | Subjekt – doprava |
|---|---|---|
| Slabá stránka | Silná stránka | Slabá stránka |
| 2 | 4 | 2 |

Uvedenou položku je možno považovat u subjektu z oblasti informatiky za silnou stránku, a to z toho důvodu, že nižší počet osob s přístupem k UI může obecně znamenat i nižší pravděpodobnost úniku UI. Naopak u subjektu z oblasti energetiky a dopravy může vyšší počet osob s přístupem k UI obecně znamenat vyšší pravděpodobnost úniku UI. Nižší hodnota u těchto slabých stránek je dána skutečností, že oba subjekty kladou velký důraz na výběr a přípravu fyzických osob s přístupem k UI (viz výše), v důsledku čehož je možno tuto slabou stránku eliminovat.

Počet osob, které budou mít přístup k UI je však odvislý od činností, které podnikatel realizuje, a v rámci kterých je nutno mít přístup k UI. Na základě tohoto je bezpečnostním ředitelem schvalován přehled pracovních pozic nebo funkcí, u nichž je vyžadován přístup k UI. V návaznosti na tato zjištění podnikatel nemůže apriori ovlivnit počet oprávněných osob, jelikož na určitou činnost je zapotřebí osob více, na jinou méně. Z tohoto důvodu může podnikatel oblast ovlivnit pouze zajištěním a důsledným dodržováním pravidel spadajících do oblasti personální bezpečnosti.

- **Ukončení pracovního poměru zaměstnanců, u kterých se předpokládá přístup k UI**

*Tabulka 23 Komparace – ukončení pracovního poměru*

| Subjekt – energetika | Subjekt – informatika | Subjekt – doprava |
|---|---|---|
| Slabá stránka | Slabá stránka | Slabá stránka |
| 3 | 1 | 3 |

Při současném stavu na trhu práce, kdy nabídka převyšuje poptávku, je nutno vzít v potaz i fluktuaci zaměstnanců. S ohledem na charakter aktuální situace je možné tuto skutečnost zohlednit i u analyzovaných subjektů, a to jako slabou stránku.

Výběr a výchova osob, které v rámci své činnosti mají mít přístup k UI, znamená pro subjekty další náklady, a proto by společnost měla tyto osoby motivovat tak, aby u společnosti na dané pozici setrvaly co nejdéle. Nejmenší hodnotou, tedy hodnotou znamenající nejnižší nespokojenost je tato slabá stránka ohodnocena u subjektu z oblasti informatiky. Jedním ze způsobů motivace je samozřejmě motivace finanční, která je u tohoto subjektu, s ohledem na předmět podnikání a činnost (tvorba a údržba softwarových produktů), jenž je v současně době v popředí, značným bonusem. Z tohoto důvodu je subjektu z oblasti informatiky přiřazena daná hodnota. V případě dalších dvou subjektů lze uvést, že k eliminaci této slabé stránky je možné využít motivačních prostředků v souvislosti s personální politikou organizace a v neposlední řadě i důsledný prvotní výběr zaměstnanců.

- **Možnost využití vzorové dokumentace vydané NBÚ (dosud nevydána)**

*Tabulka 24 Komparace – využití vzorové dokumentace*

| Subjekt – energetika | Subjekt – informatika | Subjekt – doprava |
|---|---|---|
| **Příležitost** | **Příležitost** | **Příležitost** |
| 4 | 5 | 4 |

Bezpečnostní dokumentace je alfou celého systému ochrany UI, jelikož tento systém stanoví v listinné podobě. Dodržováním postupů a opatření popsaných v bezpečnostní dokumentaci je zajištěna kvalitní ochrana UI. Pokud jsou tyto informace v bezpečnostní dokumentaci přehledně popsány, může podnikatel, resp. pověřené osoby, v důsledku pružněji reagovat na vzniklou událost. Následně je na základě této „listinné podoby systému ochrany UI“ stanovený systém realizován. Všechny subjekty považují jako příležitost vydání vzorové dokumentace, a to z toho důvodu, že by v případě využití této příležitosti mohly vypracovat bezpečnostní dokumentaci využitím vlastních sil s jistotou přehlednosti dokumentu. Tato příležitost je pro dané subjekty tzv. příležitostí ex-post, jelikož všechny subjekty již mají bezpečnostní dokumentaci zpracovanou. Subjekt z oblasti energetiky a dopravy při jejím zpracování využil externí společnost, která se oblastí ochrany UI zabývá. Jejich výsledná dokumentace je přehledným dokumentem, avšak toto vypracování znamenalo pro společnost určité náklady. Subjekt z oblasti informatiky vypracovával bezpečnostní dokumentaci vlastními silami, dokument je méně přehledný, avšak je nutno uvést, že svým obsahem splňuje všechny zákonné požadavky.

Nad rámec je zde nutno také uvést, že jednoznačně neplatí přímá úměra: vlastní vypracování bezpečnostní dokumentace = menší přehlednost dokumentu. Z výše uvedeného důvodu by předmětný subjekt využitím této příležitosti v rámci aktualizace dokumentu mohl získat nespornou výhodu.

- **Využití poradenských služeb externí firmy v oblasti ochrany UI**

*Tabulka 25 Komparace – využití externí firmy*

| Subjekt – energetika | Subjekt – informatika | Subjekt – doprava |
|---|---|---|
| **Příležitost** | **Příležitost** | **Příležitost** |
| 4 | 4 | 4 |

Využitím poradenských služeb externí firmy v oblasti ochrany UI může podnikatel získat výhodu, která je svým rozsahem odvislá od rozsahu služeb stanovených smluvně. Všechny subjekty tuto možnost považují za vysoce atraktivní příležitost. Je však nutno poznamenat, že využití této příležitosti znamená i vyšší finanční náklady.

- **Možnost časté obměny hardware a software z finančních zdrojů získaných ze státních zakázek, v rámci jejichž realizace je nutný přístup k UI**

*Tabulka 26 Komparace – častá obměna hardware a software*

| Subjekt – energetika | Subjekt – informatika | Subjekt – doprava |
|---|---|---|
| **Příležitost** | **Příležitost** | **Příležitost** |
| 3 | 4 | 3 |

Obecně lze říci, že státní zakázka představuje jistý a stabilní zdroj financí. Vyšší hodnota u subjektu z oblasti informatiky je stanovena z toho důvodu, že pro tento subjekt je zakázka, pro jejíž realizaci je nutno mít přístup k UI, jedinou „objemově významnou“ zakázkou daného druhu a rozsahu, tudíž pro subjekt znamená vysoce atraktivní příležitost v souvislosti s možností časté obměny hardware a software. Další subjekty realizují množství jiných zakázek, v rámci jejichž realizace není nutný přístup k UI a jejichž rozsah, resp. finanční objem, je značný. V důsledku tohoto je pro subjekt z oblasti energetiky a dopravy možno považovat danou příležitost za položku s nižší validitou.

- **Mimořádné události a krizové situace**

*Tabulka 27 Komparace – mimořádné události a krizové situace*

| Subjekt – energetika | Subjekt – informatika | Subjekt – doprava |
|---|---|---|
| **Hrozba** | **Hrozba** | **Hrozba** |
| 2 | 3 | 3 |

Při stanovení hodnoty ve SWOT maticích u předmětné položky bylo využito informací, které v rámci vlastní analýzy definoval podnikatel. Všechny analyzované subjekty definovaly stejné hrozby, v případě jejichž výskytu hrozí poškození (zničení) UI. Tyto skutečnosti jsou uvedeny v tabulce 28.

*Tabulka 28 Výčet hrozeb a míra rizika*

| **hrozba** | **energetika míra rizika** | **informatika míra rizika** | **doprava míra rizika** |
|---|---|---|---|
| živelná pohroma | malá | střední | střední |
| havárie dopravního prostředku | malá | malá | střední |
| průmyslová havárie | malá | malá | malá |
| havárie technologického zařízení | malá | střední | malá |
| teroristický útok | malá | střední | střední |
| celková míra rizika | **malá** | **střední** | **střední** |

K eliminaci uvedených rizik využívají analyzované subjekty totožná opatření:

- živelná pohroma – zajištění vhodné dislokace objektu, provádění pravidelných zkoušek technologických zařízení v rámci revize;
- havárie dopravního prostředku – zajištění vhodné dislokace objektu;
- průmyslová havárie – zajištění vhodné dislokace objektu, instalace technických prostředků;
- havárie technologického zařízení – instalace technických prostředků;
- teroristický útok – zajištění vhodné dislokace objektu, nepřetržitá ostraha, instalace technických prostředků, režimová opatření.

- **Pasivní odposlech, nasazení operativní techniky**

*Tabulka 29 Komparace – pasivní odposlech, nasazení operativní techniky*

| Subjekt – energetika | Subjekt – informatika | Subjekt – doprava |
|---|---|---|
| **Hrozba** | **Hrozba** | **Hrozba** |
| 2 | 2 | 1 |

K vyzrazení UI v důsledku výskytu této hrozby může dojít náhodným nebo cíleným odposlechem osob, které UI projednávají, příp. nasazení odposlechové techniky do objektu. Riziko u této hrozby hodnotí všechny subjekty jako **malé či zanedbatelné.** K eliminaci rizika je možno využít režimových opatření (viz výše).

- **Nepředvídatelné kybernetické útoky**

*Tabulka 30 Komparace – nepředvídatelné kybernetické útoky*

| Subjekt – energetika | Subjekt – informatika | Subjekt – doprava |
|---|---|---|
| **Hrozba** | **Hrozba** | **Hrozba** |
| 2 | 2 | 2 |

Riziko úniku UI v důsledku nepředvídatelných kybernetických útoků hodnotí všechny analyzované subjekty jako **malé**, a to v návaznosti na skutečnost, že všechny subjekty mají certifikovaný informační systém, a tudíž dané riziko eliminují dodržováním bezpečnostních opatření souvisejících se zajištěním bezpečnosti informačního systému,

ve kterém je nakládáno s UI. K eliminaci hrozby všechny subjekty současně kladou velký důraz při výběru osob, které budou mít přístup k UI v informačním systému a snaží se minimalizovat počet osob, které UI v informačním systému zpracovávají.

## 5.3 Vyhodnocení hypotéz

Provedením analýzy systému vlastní ochrany UI u vybraných podnikatelů z odlišných oblastí podnikání, v rámci jejichž činnosti je požadován přístup k UI, resp. porovnáním, zda je systém ochrany UI v rámci jednotlivých subjektů odlišný z pohledu možných hrozeb, míry rizika jejich výskytu a definovaných opatření k eliminace těchto rizik, byly zjištěny mnohé skutečnosti. V rámci této kapitoly budou vyhodnoceny stanovené hypotézy, které je možno na základě přechozích zjištění potvrdit nebo vyvrátit.

**HYPOTÉZA 1:** Lze předpokládat, že u všech porovnávaných subjektů je v systému ochrany UI lidský faktor považován za slabinu.

Lidský faktor je v rámci systému ochrany UI považován za důležitou část, a to zejména v tom smyslu, že jeho selháním může dojít k narušení celého systému, a tím v samotném důsledku k možnému úniku UI. Z výše uvedených SWOT analýz je zřejmé, že u všech analyzovaných subjektů je lidský faktor slabou stránkou, která se nikdy nedá absolutně vyloučit.

**Vyhodnocení hypotézy: V souvislosti s výsledným zjištěním lze konstatovat, že hypotéza 1 byla potvrzena.**

**HYPOTÉZA 2:** Za daného stavu lze předpokládat, že ochrana UI je u všech subjektů bez ohledu na předmět podnikání nastavena obdobným způsobem.

Při pohledu na výše uvedené skutečnosti je zřejmé, že vlastní systém ochrany UI je nastaven primárně podle stupně utajení informace, ke které bude mít podnikatel v rámci své činnosti přístup, příp. se kterou bude v rámci své činnosti nakládat. Na základě těchto zjištění tak lze uvést, že při vytváření systému ochrany UI podnikatel nezohledňuje to, do jaké oblasti působnosti lze danou UI zařadit, resp. předmět podnikání, v jehož rámci

danou činnost či zakázku realizuje, avšak zohledňuje stupeň utajení a formu přístupu k UI. Uvedenou teorii je možno doložit také výsledky ze SWOT analýz, ze kterých vyplývá, že u podnikatelů z různých oblastí podnikání jsou definovány totožné silné stránky, které podnikatelé mohou využívat při eliminaci hrozeb a slabých stránek. V návaznosti na uvedené lze říci, že ochrana UI, resp. systém ochrany UI, je u všech subjektů bez ohledu na předmět podnikání nastavena obdobným způsobem.

**Vyhodnocení hypotézy: V souvislosti s výsledným zjištěním lze konstatovat, že hypotéza 2 byla potvrzena.**

**HYPOTÉZA 3:** Při porovnání údajů z analýzy rizik jednotlivých subjektů lze předpokládat, že celková míra rizika bude nižší u subjektu z oblasti dopravy než u subjektu z oblasti energetiky.

Při hodnocení poslední hypotézy je nutno vzít v potaz skutečnosti uvedené v tabulce 28. Z analýzy rizik, kterou jednotlivé subjekty provedly na základě informací zjištěných vlastní interní analýzou, následně vydefinovaly míru rizika u jednotlivých hrozeb. S odkazem na Tabulka 28 tak lze uvést, že subjekt z oblasti energetiky stanovil v souvislosti s ohrožením UI celkově **malou** míru rizika. Do celkového hodnocení je zahrnuta současně slabá stránka subjektu, kterou je selhání lidského faktoru. U tohoto možného vnitřního ohrožení stanovil **malou** míru rizika, což odpovídá i následné hodnotě ve SWOT analýze. Subjekt z oblasti dopravy stanovil v souvislosti s ohrožením UI **střední** míru rizika. Do celkového hodnocení je zahrnuta současně slabá stránka subjektu, kterou je selhání lidského faktoru. U tohoto možného vnitřního ohrožení stanovil **střední** míru rizika, což odpovídá i následné hodnotě ve SWOT analýze. Celková míra rizika je tedy nižší u subjektu z oblasti energetiky.

**Vyhodnocení hypotézy: V souvislosti s výsledným zjištěním lze konstatovat, že hypotéza 3 potvrzena nebyla.**

## 5.4 Návrh opatření

Předmětem této diplomové práce bylo současně na základě výsledků zjištěných analýzou navrhnout další opatření k zajištění ochrany UI. Jak z výše uvedeného vyplývá, při eliminaci slabých stránek, ze kterých by se do budoucna mohly stát silné stránky je využíván právě potenciál aktuálně definovaných stránek silných. Silné stránky využívá podnikatel současně k odvrácení či eliminaci hrozeb. V neposlední řadě podnikatelé mohou využít příležitostí např. k odstranění slabých stránek. Využitím příležitosti je však možno nejen odstranit slabé stránky, ale také zvýšit bodové hodnocení silné stránky tak, aby s ní byl podnikatel nejvíce spokojen. Tuto silnou stránku lze pak opět využít k odvrácení stanovených hrozeb atd. Na základě zjištěných skutečností zde uvádím návrh těchto opatření:

1. **Důsledně vybírat osoby, které mají/budou mít v rámci své činnosti u podnikatele přístup k UI –** v daném případě se jedná o osoby, které mají/budou mít přístup k UI stupně utajení Vyhrazené, nicméně dle mého názoru je neméně důležitý i prvotní výběr osob, u kterých se předpokládá/které mají přístup k UI vyššího stupně utajení. Samostatnou kapitolou je výběr osob, které budou mít přístup k UI v informačním systému podnikatele. V neposlední řadě je potřeba zmínit také výběr osob, které budou vykonávat funkci odpovědné osoby či bezpečnostního ředitele. Tyto osoby by měly být ideálně vybrány z řad statutárního orgánu nebo bezpečnostního managementu podnikatele, příp. je vhodné, pokud zástupce podnikatele pověří funkcí bezpečnostního ředitele interního či externího specialistu v oblasti bezpečnosti.

2. **Nastavit efektivní interní systém (algoritmus), který zajistí podnikateli (odpovědné osobě/bezpečnostnímu řediteli/pověřené osobě) včasné upozornění, že je nutno realizovat určitý úkon důležitý ke splnění zákonných povinností v oblasti ochrany UI** – uvedené opatření je možno realizovat pomocí kancelářských softwarových programů, které po nastavení dokáží včas dotčenou osobu upozornit, že je nutno např. oznámit NBÚ ukončení pracovního poměru osoby, která měla v rámci své činnosti přístup k UI, zajistit periodické školení, poučit osobu, která bude mít v rámci své činnosti přístup k UI, aj.

3. **Zpracovat bezpečnostní dokumentaci podle šablony** – u všech analyzovaných subjektů byla jako příležitost definována možnost využití vzorové bezpečnostní dokumentace, která by byla vydána ze strany NBÚ. Ze zkušenosti mohu říci, že se podnikatelé žádající o vydání osvědčení podnikatele zpravidla obracejí na NBÚ s žádostí o konzultaci, jelikož přesně neví, jakým způsobem předmětný dokument (bezpečnostní dokumentaci) koncipovat. V souvislosti s tímto je podnikatelům poskytována ze strany NBÚ individuální metodická pomoc. Z druhé strany je však nutno zdůraznit, že vytvoření šablony, která by svým rozsahem a obsahem byla využitelná pro potřeby všech subjektů, je z hlediska legislativního velmi obtížné a z tohoto důvodu nejsou za současného stavu stanoveny NBÚ požadavky na formu či rozsah bezpečnostní dokumentace. Jediným požadavkem je zákonný obsah dokumentu, který však musí podnikatel rozpracovat s ohledem na vlastní podmínky. V návaznosti na výše uvedené jsem vytvořila šablonu základní části bezpečnostní dokumentace, která sice reálně nedokáže pojmout požadavky všech subjektů a nelze ji považovat ani za prototyp, může však být určitým vodítkem pro podnikatele při vypracování dokumentu. Zpracováním bezpečnostní dokumentace dle šablony však není dotčena možnost konzultace individuálních požadavků s pracovníky NBÚ. Předmětná šablona je jakýmsi shrnutím zákonných požadavků na vypracování dokumentace do jednoho dokumentu a je určena zejména pro subjekty, které realizují/budou realizovat personální, administrativní a fyzickou bezpečnost, příp. bezpečnost informačních nebo komunikačních systémů a kryptografickou bezpečnost, tedy pro podnikatele, kteří předpokládají/mají přístup k UI stupně utajení Důvěrné a vyšší s formou přístupu podle ustanovení § 20 odst. 1 písm. a) zákona o ochraně UI. Na první pohled se může zdát, že vytvoření šablony není návrhem samotného opatření. Zde bych se však ráda odkázala na již uvedenou skutečnost o vypovídající hodnotě bezpečnostní dokumentace. Přehledně zpracovaná dokumentace je základním stavebním kamenem celého systému ochrany UI, silnou stránkou subjektu a v samotném důsledku ji lze v teoretické rovině využít k odvrácení (eliminaci) definovaných hrozeb. Vytvořená šablona je přílohou této diplomové práce.

# 6 Diskuze

Každá hodnota neboli aktivum má být chráněna. Primárně si každá společnost musí provést analýzu aktiv, se kterými disponuje. Na základě této analýzy následně může zavést systém ochrany aktiv, který je s ohledem na jejich charakter odlišný. Zatímco pro tzv. veřejné informace není potřeba speciálního systému, jelikož není na jejich ochranu kladen žádný důraz, informace neveřejného charakteru s přesahem do charakteru utajovaného již potřebují pro svou ochranu sofistikovaně vytvořený systém ochrany. Stejně jako má stát primárně ochraňovat své zájmy, musí i společnosti, které mají v rámci své činnosti přístup k UI, tyto informace chránit, a to z toho důvodu, že jejich vyzrazení nebo poškození může způsobit újmu zájmům státu, nebo to pro ně může být nevýhodné. Jak z uvedeného vyplývá, ochrana UI je důležitým aspektem při zajišťování bezpečnosti státu. V tomto případě je tedy velice důležité, aby měly tyto společnosti nastaven systém ochrany tak, aby splňoval zákonné požadavky a aby byl zároveň zodpovědně dodržován a plněn. K tomuto je zapotřebí nejenom systém definovat, ale i vhodně a citlivě nastavit tak, aby byl funkční jako kompatibilní celek.

Cílem této diplomové práce je analýza systému vlastní ochrany UI u vybraných podnikatelů z odlišných oblastí podnikání, v rámci jejichž činnosti je požadován přístup k UI. V rámci provedené analýzy jsou u těchto subjektů identifikovány konkrétní silné a slabé stránky předmětného systému, stejně jako příležitosti a hrozby, které na podnikatele působí zvnějšku a podnikatele mohou ovlivnit či ovlivňují.

Porovnáním celkových hodnot u jednotlivých definovaných položek jsem došla k závěru, že u všech analyzovaných subjektů hodnotově převyšují silné stránky a příležitosti nad slabými stránkami a hrozbami, z čehož v důsledku vyplývá, že systém ochrany UI je u předmětných subjektů nastaven tak, aby splňoval zákonné požadavky z pohledu zajištění ochrany UI. Systém ochrany UI je však systémem živým a neustále se vyvíjejícím. Z tohoto důvodu je potřeba nahlížet na provedenou analýzu jako na jednotlivé položky, u kterých je potřeba neustále pracovat na jejich udržitelnosti a zlepšovat jejich hodnocení, a to zejména v případě silných stránek a příležitostí. Na základě zjištěných výsledků se domnívám, že pro zajištění relativně bezproblémové funkčnosti systému by podnikatelé měly primárně realizovat strategii založenou na využívání silných stránek k eliminaci možných hrozeb. Současně se domnívám, že podnikatelé by měli aktivně pracovat na eliminaci slabých stránek. Na základě provedené

analýzy se mi potvrdilo, že lidský faktor je u všech analyzovaných subjektů slabou stránkou. Na základě tohoto zjištění se mohu přiklonit k tvrzení, ve kterém autor uvádí: *„Když mluvíme o informacích, nemůžeme přehlédnout ani jejich uživatele. Jako ostatně u všech systémů, také v oblasti informačních systémů a jejich bezpečnosti, představuje lidský faktor nejrizikovější složku. Lidé představují hazardní stroje, s nimiž se musí pracovat“*. [29] Stanovenými opatřeními se podnikatelé reálně snaží tuto slabou stránku eliminovat takovým způsobem, aby se z ní nestala hrozba. Ve chvíli, kdy s příchodem stereotypu stagnuje v samotném důsledku kontrola, může tato situace, spočívající v překlenutí slabé stránky na hrozbu, jednoduše nastat. V této souvislosti se odůvodněně domnívám, že důsledný výběr pracovníků je alfou a omegou při procesu nastavování systému ochrany UI. Tuto domněnku mi dokládá i závěr z výsledků kontrol uvedený v kapitole 2.8.2. ve Zprávě o činnosti NBÚ za rok 2017, ze kterého vyplývá, že příčinnou nedostatků bylo ve většině případů selhání lidského faktoru. [47]

V praxi je při ověřování, zda je podnikatel v průběhu platnosti vydaného osvědčení schopen zajistit ochranu UI, využíván systém fyzické kontroly NBÚ. V roce 2017 bylo oddělením kontroly NBÚ provedeno celkem 50 kontrol, z toho ve 32 případech byly zjištěny nedostatky, které byly v 9 případech předány k přestupkovému řízení, a v 6 případech z nich bylo rozhodnuto, že byl spáchán přestupek. Obecně působí NBÚ spíše preventivně, což vyplývá i z celkové výše pokut, které na základě poznatků z kontrol byly vyčísleny na částku 51 000 Kč. Preventivní funkce NBÚ spočívá dle mého názoru nejen ve výši udělovaných pokut, ale současně v metodické činnosti v oblasti bezpečnostního řízení, kdy jsou fyzickým osobám a podnikatelům, odpovědným osobám a bezpečnostním ředitelům poskytovány konzultace a vydávána doporučení. [47]

Následující text zobrazuje částečný výčet nedostatků, zjištěných při kontrolách provedených v roce 2017, kdy se nedostatky objevovaly téměř ve všech oblastech zajišťování ochrany UI. V souvislosti s výsledky SWOT analýz se lze na základě uvedeného výčtu opět ztotožnit se závěrem, že lidský činitel sehrává v oblasti ochrany UI významnou roli.

**A. Nedostatky v oblasti personální bezpečnosti:**

- s UI byla seznámena osoba, která nebyla držitelem oznámení nebo osvědčení;

- přístup k UI byl umožněn osobě, která byla držitelem oznámení nebo osvědčení, ale nebyla poučena;
- přístup k UI byl umožněn osobě, která byla držitelem oznámení nebo osvědčení, ale UI nezbytně nepotřebovala k výkonu své funkce;
- držitel osvědčení byl poučen, ale poučení nebylo zasláno NBÚ;
- nebyla prováděna pravidelná roční školení v oblasti ochrany UI;
- nebyla zaslána informace o ukončení pracovního, služebního nebo obdobného vztahu fyzické osoby, která měla přístup k UI;
- formální nedostatky vyhotovených písemných dokladů.

**B. Nedostatky v oblasti průmyslové bezpečnosti:**

- přístup k UI byl umožněn podnikateli, který nesplňoval zákonné podmínky pro přístup (absence prohlášení podnikatele či osvědčení podnikatele);
- bezpečnostní dokumentace podnikatele byla vedena, ale nebyla průběžně aktualizována.

**C. Nedostatky v oblasti administrativní bezpečnosti:**

- chybějící utajovaný dokument, neevidování utajovaného dokumentu, chybějící jednací protokol;
- nedostatky ve způsobu vedení evidence utajovaných dokumentů;
- neplnění dalších povinností (např. neuvedení rozdělovníku, nevyznačení stupně utajení na obálce, do které je vložen utajovaný dokument).

**D. Nedostatky v oblasti fyzické bezpečnosti:**

- UI byly ukládány mimo zabezpečenou oblast nebo v zabezpečené oblasti nižší kategorie;
- použité technické prostředky byly nesprávně instalovány nebo měly chybnou funkci;
- nesoulad skutečného stavu opatření fyzické bezpečnosti se stavem deklarovaným v projektu fyzické bezpečnosti.

**E. Nedostatky v oblasti bezpečnosti informačních a komunikačních systémů:**

- nakládání s UI v informačním systému, který nebyl certifikován;
- nedostatky administrativního charakteru (např. neaktualizované instalační záznamy). [47]

Z uvedeného výčtu nedostatků je dále zřejmé, že byla zjištěna i porušení plnění povinností odpovědné osoby, bezpečnostního ředitele či osoby jimi pověřené (neprovedení školení, nepoučení fyzické osoby před přístupem k UI atd.). Jak vyplývá z provedené analýzy u podnikatele z oblasti energetiky, výkon funkce odpovědné osoby a bezpečnostního ředitele dvěma osobami je považován za významnou silnou stránku, a to v praxi především s ohledem na rozdělení kompetencí. Předmětný výsledek je možno podpořit i skutečnostmi vyplývajícími z knihy Informační a znalostní management v praxi, ve které autor uvádí: *„Dříve měl být vedoucí vědoucí, ale v současné době stále více vědoucí nemusí mít zájem být vedoucí, protože řídící práce často omezuje rozvoj jeho znalostí, tvůrčí zaměření a metodickou i odbornou kompetenci“*. [48] V důsledku tohoto se domnívám, že rozdělení rolí (pověření odpovědné osoby a jmenování bezpečnostního ředitele, příp. pověření další osoby) na úrovni specialistů může být pro podnikatele přínosem v systému bezpečnosti UI. Výkon těchto dvou funkcí jednou osobou samozřejmě nemusí vždy nutně znamenat problém, a to zejména v případech, kdy odpovědnou osobou je statutární orgán, který je současně specialistou v oblasti bezpečnosti. Tuto domněnku v závěru dokreslují i dílčí výsledky SWOT analýz u subjektu z oblasti informatiky a dopravy, kde s ohledem na funkci a specializaci daných osob není nezbytně nutné pracovat na personální přeměně.

Dalším zjištěním v rámci kontrol NBÚ byly nedostatky v oblasti průmyslové bezpečnosti, konkrétně neaktualizovaná bezpečnostní dokumentace. Vzhledem ke skutečnosti, že provádění aktualizace je zákonnou povinností podnikatele, který je držitelem osvědčení pro přístup k UI, je možno ji u všech subjektů považovat za silnou stránku systému. I přes tuto skutečnost byly u analyzovaných subjektů zjištěny limity, které by dle mého názoru bylo možno řešit nastavením určitého algoritmu, který by podnikatele v případě změn, a to jak interních (např. faktická změna realizace jednotlivých druhů ochrany UI, změna v personální oblasti – nový bezpečnostní ředitel), tak změn externích (např. novelizace zákonných norem), upozornil na potřebu aktualizace v bezpečnostní dokumentaci. Současně se domnívám, že k eliminaci zjištěných

nedostatků by bylo možno využít potenciálu spočívajícím v odbornosti osob zodpovědných za aktuálnost bezpečnostní dokumentace, což plynule navazuje na předchozí výše uvedená zjištění.

Bezpečnostní dokumentace zahrnuje všechny druhy zajištění ochrany UI. Domnívám se, že jelikož jsou pravidelně v rámci kontrol zjišťovány nedostatky téměř ve všech druzích této ochrany, je nutné kvalitně aplikovat do praxe záměry uvedené v bezpečnostní dokumentaci. Jestliže je však dokument méně přehledný, a to i přes skutečnost, že splňuje všechny zákonné požadavky, nelze jeho aplikací do praxe zajistit, že bude docházet k eliminaci případných nedostatků na absolutní minimum. V případě, že podnikatel využívá služeb externích subjektů, které se ochranou UI zabývají, není zpravidla v přehlednosti dokumentu problém. Případné zjištění nedostatků při kontrole je pak záležitostí přičitatelnou zejména selhání lidského faktoru. V situaci, kdy bezpečnostní dokumentaci zpracovává podnikatel sám a v dané oblasti nemá dostatečné zkušenosti, či si nezjistí relevantní informace k vypracování dokumentace, může být na vině při následném zjištění nedostatků v rámci kontroly právě aplikace této méně přehledné dokumentace. Realisticky mohu říci, že v porovnání s ostatními příčinami by měla menší přehlednost dokumentace na celkovém podílu příčin nedostatků spíše podíl malý. I přes tuto skutečnost se domnívám, že podnikatelům by mohlo pomoci, kdyby existovala veřejně dostupná šablona bezpečnostní dokumentace, která by jim pomohla při zpracování přehledného dokumentu, a to i bez nutnosti využití služeb externí společnosti.

Obecně lze uvést, že prováděnými kontrolami NBÚ získává poznatky, které pomáhají vyhodnotit efektivitu právní úpravy a dalších řešení v oblastech ochrany UI. K těmto poznatkům by mohly přispět i výsledky výše uvedených analýz, které mohou být dále využity v rámci metodické činnosti vůči podnikatelům, kteří žádají o vydání osvědčení podnikatele či již přístup k UI na základě osvědčení mají. V souhrnu se zjištěnými nedostatky z kontrol by mohly vlastní výsledky v této diplomové práci pomoci se zaměřit na konkrétní problémové oblasti, a to nejen u výše uvedených podnikatelů. Vzhledem ke skutečnosti, že zajištění ochrany UI je v samotném důsledku primárním zájmem státu, jelikož zneužití UI může způsobit újmu zájmům ČR, které stát musí chránit, je důležité, aby stát, resp. NBÚ, jakožto ústřední správní úřad pro ochranu UI, tyto problémové oblasti dokázal definovat a byl schopen na tato zjištění účinně reagovat jak formou

metodických doporučení, tak formou přípravy novelizace příslušných právních předpisů, které jsou vydávány v jeho působnosti.

Osobně spatřuji výhodu v tom, že subjekty, které mají v rámci své činnosti přístup k UI, mají nespornou konkurenční výhodu oproti subjektům, které mají ve svém obchodním portfoliu „pouze“ informace veřejného či neveřejného charakteru, které však nejsou klasifikovány stupněm utajení, a to i přes nákladnost zajištění celého systému ochrany UI (v případě, že u podnikatele UI vzniká nebo je u něj uchovávána). Osvědčení je pro podnikatele určitým benefitem, který umožňuje realizaci finančně zajímavých nabídek a zakázek. Při jejich realizaci však stát vkládá těmto společnostem důvěru spočívající v zajištění ochrany UI, s nimiž se daná společnost, resp. její pracovníci, mohou setkat. A z tohoto důvodu je dle mého názoru nastavení kvalitního systému ochrany UI důležitou součástí bezpečnostní politiky organizace a v samotném důsledku i bezpečnostního systému státu jako celku.

# 7 Závěr

Diplomová práce souhrnně pojednává o bezpečnosti státu se zaměřením na ochranu informací a současně s důrazem na ochranu informací utajovaných. Jelikož ochrana UI představuje jednu z částí v rámci problematiky bezpečnosti státu, navazuje její popis na teoretickou rovinu definující bezpečnostní systém a bezpečnost informací. Tato rovina zároveň vychází ze zákonných ustanovení v daných oblastech.

S ohledem na rozsáhlost problematiky ochrany UI jsem v praktické části diplomové práce provedla analýzu systému ochrany UI u vybraných podnikatelských subjektů z odlišných oblastí podnikání. Na základě zjištěných výsledků jsem v kapitole 5.4 navrhla další opatření, která by mohla být využita při zajištění ochrany UI. Jedním z těchto opatření je využití šablony k vypracování bezpečnostní dokumentace podnikatele, která je součástí této diplomové práce. Propojením teoretické části s komparativně porovnanými výsledky SWOT analýz a návrhem předmětných opatření byl stanovený cíl diplomové práce splněn.

V rámci diplomové práce jsem si stanovila tři hypotézy, z nichž dvě se mi na základě získaných výsledků podařilo potvrdit. Obecně se dá říci, že žádný systém nemůže být funkční, jestliže nemá jasně stanovená pravidla. Pokud jsou pravidla nastavena, je nutno, aby byla dodržována a v případě jejich porušení musí nutně přijít reakce v podobě postihu, následné zajištění opatření proti opětovnému vzniku této situace a v samotném důsledku obnova samotného systému. Provedenou analýzou jsem si ověřila, že nastavení systému ochrany UI není v zásadě závislé na druhu UI, resp. na předmětu podnikání, v jehož rámci má podnikatel přístup k UI, a že ochrana UI je u všech tří zvolených subjektů zajištěna obdobným způsobem. Provedená analýza současně potvrdila můj předpoklad, že zásadní úlohu v oblasti ochrany UI sehrává lidský faktor. Výsledky analýz byly dále konfrontovány s poznatky z kontrol, které za účelem prověření stavu systému ochrany UI vykonává NBÚ.

Zjištěné skutečnosti tak mohou být v samotném závěru využity při definování kritických oblastí u podnikatelů za účelem realizace následných kroků NBÚ spočívajících zpravidla v metodické pomoci předmětným zájmovým subjektům.

# 8 Seznam použitých zkratek

BIS – Bezpečnostní informační služba

BRS – Bezpečnostní rada státu

ČNB – Česká národní banka

ČR – Česká republika

ČTÚ – Český telekomunikační úřad

ČVUT – České vysoké učení technické v Praze

ESUO – Evropské společenství uhlí a oceli

EU – Evropská unie

Euroatom – Evropské společenství pro atomovou energii

HZS ČR – Hasičský záchranný sbor České republiky

IZS – integrovaný záchranný systém

MF – Ministerstvo financí České republiky

MPO – Ministerstvo průmyslu a obchodu České republiky

MV – Ministerstvo vnitra České republiky

MV-GŘ HZS ČR – Ministerstvo vnitra-generální ředitelství Hasičského záchranného sboru České republiky

MZ – Ministerstvo zdravotnictví České republiky

MZe – Ministerstvo zemědělství České republiky

MŽP – Ministerstvo životního prostředí České republiky

NATO – Severoatlantická aliance (North Atlantic Treaty Organization)

NBÚ – Národní bezpečnostní úřad

NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost

OBSE – Organizace pro bezpečnost a spolupráci v Evropě

ORP – obec s rozšířenou působností

OSN – Organizace spojených národů

SSHR – Správa státních hmotných rezerv

SÚJB – Státní úřad pro jadernou bezpečnost

UI – utajovaná informace

VZ – Vojenské zpravodajství

# 9 Seznam použité literatury


[1] PROCHÁZKOVÁ, Dana. *Bezpečnost a krizové řízení*. 1. Praha: Police history, 2006. ISBN 80-864-7735-5.

[2] DOUCEK, Petr. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM*. 2., přeprac. vyd. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.

[3] ZEMAN, Petr, ed. *Česká bezpečnostní terminologie: výklad základních pojmů*. 1. vyd. Brno: Masarykova univerzita, Mezinárodní politologický ústav, 2002. ISBN 80-210-3037-2.

[4] NOHLEN, Dieter a Florian GROTZ. *Kleines Lexikon der Politik*. 5. überarbeitete und erw. Aufl. Bonn: Bundeszentrale für Politische Bildung, 2011. Schriftenreihe der Bundeszentrale für Politische Bildung, Bd. 1145. ISBN 3838901452.

[5] Bezpečnostní strategie České republiky. *Vlada.cz: Vláda ČR* [online]. b.r. [cit. 2018-09-28]. Dostupné z: https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf

[6] JANOŠEC, Josef. *Bezpečnost a obrana České republiky 2015-2025*. Praha: Ministerstvo obrany České republiky - Agentura vojenských informací a služeb, 2005. ISBN 80-7278-303-3.

[7] Bezpečnostní systém státu. *Mvcr.cz: Ministerstvo vnitra České republiky* [online]. b.r. [cit. 2018-09-28]. Dostupné z: http://www.mvcr.cz/clanek/bezpecnostni-system-statu.aspx

[8] Koncepce ochrany obyvatelstva do roku 2020 s výhledem do roku 2030. *Vlada.cz* [online]. b.r. [cit. 2018-09-30]. Dostupné z: https://www.vlada.cz/assets/ppov/brs/dokumenty/Koncepce-ochrany-obyvatelstva-2020-2030_1_.pdf

[9] VILÁŠEK, Josef. *Krizové řízení*. V Praze: Karolinum, 2009. ISBN 978-802-4617-237.

[10] Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky, ve znění pozdějších předpisů. *Zakonyprolidi.cz* [online]. b.r. [cit. 2018-09-30]. Dostupné z: https://www.zakonyprolidi.cz/cs/1998-110

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

[12] BALABÁN, Miloš a Bohuslav PERNICA. *Bezpečnostní systém ČR: problémy a výzvy*. Vydání první. Praha: Univerzita Karlova v Praze, nakladatelství Karolinum, 2015. ISBN 978-80-246-3150-9.

[13] Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. *Zakonyprolidi.cz* [online]. b.r. [cit. 2018-09-30]. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-412

[14] BAWDEN, David a Lyn ROBINSON. *Úvod do informační vědy*. Doubravník: Flow, 2017. ISBN 978-80-88123-10-1.

[15] SKLENÁK, Vilém. *Data, informace, znalosti a Internet*. Praha: C.H. Beck, 2001. C.H. Beck pro praxi. ISBN 80-717-9409-0.

[16] ŠAVELKA, Jaromír. *Právní informační systémy*. Brno: Tribun EU, 2011. Knihovnicka.cz. ISBN 978-80-7399-248-4.

[17] Neveřejné informace. *Www.nkp.cz: Databáze Národní knihovny ČR* [online]. b.r. [cit. 2018-10-29]. Dostupné z: https://aleph.nkp.cz/F/?func=direct&doc_number=000000407&local_base=ktd

[18] Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. *Zakonyprolidi.cz* [online]. b.r. [cit. 2018-10-29]. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-101#f2017701

[19] Zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů. *Zakonyprolidi.cz* [online]. b.r. [cit. 2018-10-29]. Dostupné z: https://www.zakonyprolidi.cz/cs/2012-89

[20] DOUCEK, Petr, ed. *Informační management*. Praha: Professional Publishing, 2010. ISBN 978-807-4310-102.

[21] Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů: (krizový zákon). *Hasičský záchranný sbor České republiky* [online]. b.r. [cit. 2018-10-19]. Dostupné z: http://www.hzscr.cz/clanek/krizove-rizeni-a-cnp-predpisy-predpisy.aspx?q=Y2hudW09Mw%3D%3D

[22] MUSIL, Rudolf. *Ochrana utajovaných skutečností*. Vyd. 1. Praha: Eurounion, 2001. ISBN 80-85858-93-2.

[23] *Ochrana obyvatelstva a krizové řízení: skripta*. Praha: Ministerstvo vnitra - generální ředitelství Hasičského záchranného sboru ČR, 2015. ISBN 978-80-86466-62-0.

[24] STUDIJNÍ TEXTY KE ZVLÁŠNÍ ČÁSTI ÚŘEDNICKÉ ZKOUŠKY OBOR SLUŽBY Č. 32 KRIZOVÉ ŘÍZENÍ, OCHRANA OBYVATELSTVA A INTEGROVANÝ ZÁCHRANNÝ SYSTÉM. *Ministerstvo vnitra České republiky* [online]. b.r. [cit. 2018-12-30].

[25] Předpisy. *Hasičský záchranný sbor České republiky* [online]. b.r. [cit. 2018-12-30]. Dostupné z: https://www.hzscr.cz/clanek/krizove-rizeni-a-cnp-predpisy-predpisy.aspx

[26] *Ochrana obyvatelstva v případě krizových situací a mimořádných událostí nevojenského charakteru II*. Brno: Tribun EU, 2014. ISBN 978-80-263-0724-2.

[27] Předpisy: Usnesení vlády, směrnice a metodické pokyny ministerstev a ostatních ústředních správních úřadů. *Hasičský záchranný sbor České republiky* [online]. b.r. [cit. 2018-12-30]. Dostupné z: https://www.hzscr.cz/clanek/krizove-rizeni-a-cnp-predpisy-predpisy.aspx

[28] Terminologický slovník pojmů z oblasti krizového řízení. *Ministerstvo vnitra České republiky* [online]. b.r. [cit. 2018-12-30]. Dostupné z: http://www.mvcr.cz/clanek/terminologicky-slovnik-krizove-rizeni-a-planovani-obranystatu. aspx

[29] RODRYČOVÁ, Danuše a Pavel STAŠA. *Bezpečnost informací jako podmínka prosperity firmy*. Praha: Grada, 2000. Manažer. ISBN 80-716-9144-5.

[30] POŽÁR, Josef. *Informační bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. Vysokoškolské učebnice (Vydavatelství a nakladatelství Aleš Čeněk). ISBN 80-868-9838-5.

[31] KALAMÁR, Štěpán a Josef POŽÁR. *Vybrané aspekty informační bezpečnosti*. Vyd. 1. Praha: Policejní akademie České republiky v Praze, 2010. ISBN 978-80-7251-339-0.

[32] *Kodex správy a řízení společností ČR (2018)*. Praha: Czech institute of directing, 2018. ISBN 978-80-270-4402-3.

[33] MAJEROVÁ, Zuzana. *Ochrana informací v krizovém řízení: diplomová práce = Information Protection in Crisis Management*. Kladno, 2017. Diplomová práce (Ing.). České vysoké učení technické v Praze. Fakulta biomedicínského inženýrství, katedra zdravotnických oborů a ochrany obyvatelstva. Vedoucí práce Ing. Milan Weinfurter.

[34] OSTRAVA: VŠB - TECHNICKÁ UNIVERZITA. *Organizace a řízení bezpečnosti v ČR: Sborník prezentací* [online]. OSTRAVA: VŠB - TECHNICKÁ UNIVERZITA. Ostrava, 2016 [cit. 2019-01-06]. Dostupné z: https://www.fbi.vsb.cz/export/sites/fbi/U3V/cs/materialy/U3V_Organizace_a_rizeni_b ezpecnosti_v_CR.pdf

[35] Řízení bezpečnosti (Security management). *Managementmania* [online]. b.r. [cit. 2019-01-13]. Dostupné z: https://managementmania.com/cs/rizeni-bezpecnosti

[36] PAVELKA, Ivan. Základní instituty ochrany utajovaných informací v ČR. *Správní právo* [online]. 2017, **50**(5), 258-268 [cit. 2019-01-20]. ISSN 0139-6005. Dostupné z: http://www.mvcr.cz/clanek/spravni-pravo-cislo-5-2017.aspx

[37] DVOŘÁK, Jan. *Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti: komentář*. 1. Praha: Wolters Kluwer, 2018. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7598-016-8.

[38] PAVELKA, Ivan. Institucionální zajištění ochrany utajovaných informací v ČR. *Správní právo* [online]. 2018, (3), 202-216 [cit. 2019-01-20]. ISSN 0139-6005. Dostupné z: https://www.mvcr.cz/webpm/soubor/sp3-18-pavelka-pdf.aspx

[39] Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací, ve znění pozdějších předpisů. *Zakonyprolidi.cz* [online]. b.r. [cit. 2019-01-24]. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-522

[40] Informace k bezpečnostní dokumentaci podnikatele. *Www.nbu.cz: Bližší informace k obsahu bezpečnostní dokumentaci podnikatele* [online]. b.r. [cit. 2019-01-25]. Dostupné z: https://www.nbu.cz/cs/ochrana-utajovanych-informaci/prumyslova-bezpecnost-osvedceni-podnikatele-certifikaty/1064-podkladove-materialy-k-zadosti-podnikatele/

[41] *Věstník Národního bezpečnostního úřadu*. Praha: Národní bezpečnostní úřad, 1999, (12018). ISSN 1212-7086.

[42] *Všeobecná encyklopedie ve čtyřech svazcích*. Vyd. 1. Praha: Nakladatelský dům OP, 1996. Encyklopedie Diderot. ISBN 80-85841-17-7.

[43] GRASSEOVÁ, Monika, Radek DUBEC a David ŘEHÁK. *Analýza podniku v rukou manažera: 33 nejpoužívanějších metod strategického řízení*. 2. vyd. Brno: BizBooks, 2012. ISBN 978-80-265-0032-2.

[44] SWOT analýza v Excelu. *Fotis Fotopulos, 2011* [online]. b.r. [cit. 2019-01-01]. Dostupné z: http://excel-navod.fotopulos.net/swot-analyza.html

[45] Vyhláška č. 529/2005 Sb.,o administrativní bezpečnosti a o registrech utajovaných informací, ve znění pozdějších předpisů. *Nbu.cz* [online]. b.r. [cit. 2018-09-30]. Dostupné z: https://www.nbu.cz/cs/pravni-predpisy/provadeci-pravni-predpisy/1088-vyhlaska-c-5292005/

[46] Bezpečnost informačních a komunikačních systémů. *Www.nukib.cz* [online]. b.r. [cit. 2019-01-26]. Dostupné z: https://www.nukib.cz/cs/ochrana-utajovanych-informaci-v-ict/bezpecnost-informacnich-a-komunikacnich-systemu/

[47] *Zpráva o činnosti Národního bezpečnostního úřadu za rok 2017* [online]. b.r. [cit. 2019-02-10]. Dostupné z: https://www.nbu.cz/cs/informacni-centrum/povinne-zverejnovane-informace/906-vyrocni-zpravy-o-cinnosti-nbu/

[48] VYMĚTAL, Jan, Anna DIAČIKOVÁ a Miriam VÁCHOVÁ. *Informační a znalostní management v praxi*. Praha: LexisNexis CZ, 2005. Studijní texty (LexisNexis CZ). ISBN 80-869-2001-1.

# 10 Seznam použitých obrázků

# 11 Seznam použitých tabulek

# 12 Seznam příloh

**Příloha 1**

**„V Z O R“**

Záhlaví (název a sídlo podnikatele)

Počet listů:

Počet příloh:

**Schvalovací doložka**

# BEZPEČNOSTNÍ DOKUMENTACE

# PODNIKATELE

(*uvést název podnikatele*)

## **pro přístup k utajované informaci** (dále jen „UI“)

*(uvést stupeň utajení a formu přístupu k UI podle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů (dále jen „zákon“)*

# 1. SPECIFIKACE UI

## 1.1. UI uložené u podnikatele

- pouze v případě, že je podnikatel již držitelem osvědčení pro přístup k UI *(uvést výčet UI uložených u podnikatele s uvedením jejich původce a stupně utajení a v případě, že mu UI byla poskytnuta nebo u něj vznikla na základě zakázky, též s uvedením specifikace této zakázky).*

## 1.2. Specifikace UI, k nimž by měl mít podnikatel přístup

- (*v případě, že jsou podnikateli známy všechny skutečnosti, uvést UI, k nimž by měl mít podnikatel přístup s uvedením jejich původce a stupně utajení, příp. s uvedením specifikace zakázky);*
- *(v případě, že podnikateli nejsou známy všechny skutečnosti, vychází z informací poskytnutých potenciálním zadavatelem a dále z nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací, ve znění pozdějších předpisů)*

# 2. ANALÝZA MOŽNÉHO OHROŽENÍ UI

- *Uvést **hrozby**, které podnikatel definuje na základě vlastního hodnocení podmínek ve firmě ve vztahu k ochraně UI – při vlastním hodnocení se podnikatel zaměřuje na zjištění faktických i potencionálních rizik jak v oblasti lidských zdrojů, tak v oblasti technických prostředků používaných v podmínkách podnikatele. Současně lze vycházet z analýzy hrozeb pro dané území uvedené v příslušném havarijním plánu kraje nebo krizovém plánu kraje, a to zejména v souvislosti s realizací opatření fyzické bezpečnosti a bezpečnosti informačních a komunikačních systémů nebo kryptografické ochrany.*

- *Uvést **míru rizika** ve vztahu k jednotlivým hrozbám.*

- *Uvést **opatření**, která budou přijímána k omezení určených hrozeb (opatření vycházejí z realizace jednotlivých druhů zajištění ochrany UI – viz dále).*

# 3. ZPŮSOBY REALIZACE JEDNOTLIVÝCH DRUHŮ ZAJIŠTĚNÍ OCHRANY UI

## 3.1. Personální bezpečnost

- *Uvést podmínky přístupu fyzické osoby k UI příslušného stupně utajení (Vyhrazené, Důvěrné, Tajné, Přísně tajné) dle hl. II zákona a dle vyhlášky č. 363/2011 Sb., o personální bezpečnosti a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.*

- *Uvést povinnosti odpovědné osoby a bezpečnostního ředitele podnikatele.*

## 3.2. Administrativní bezpečnost

- *Výčtem položek uvést, v jaké souvislosti budou u podnikatele realizována opatření z oblasti administrativní bezpečnosti (evidence utajovaných dokumentů, administrativních pomůcek, manipulace s utajovanými dokumenty, označování utajovaných dokumentů, zabezpečení utajovaných dokumentů při personálních a organizačních změnách, ...).*

- *Dále zpracovat samostatný dokument (tzv. administrativní směrnici), ve kterém budou výše uvedené položky rozpracovány na podmínky podnikatele v souladu s hl. IV zákona a vyhláškou č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací, ve znění pozdějších předpisů.*

- ***Směrnice bude následně přílohou č. 1 této bezpečnostní dokumentace.***

### 3.3. Fyzická bezpečnost

- *Uvést základní identifikační údaje o objektu, ve kterém se bude nacházet zabezpečená oblast/zabezpečené oblasti podnikatele.*

- *Dále zpracovat samostatný dokument (tzv. projekt fyzické bezpečnosti), ve kterém budou popsána opatření použitá k zajištění fyzické bezpečnosti, a to v souladu s hl. V zákona a vyhláškou č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů.*

- ***Projekt bude následně přílohou č. 2 této bezpečnostní dokumentace.***

### 3.4. Bezpečnost informačních a komunikačních systémů

- *V případě, že podnikatel bude daný druh zajištění ochrany UI realizovat, uvede pouze obecně tuto skutečnost a dále zpracuje bezpečnostní dokumentaci informačního systému, která je přílohou žádosti o certifikaci informačního systému pro Národní úřad pro kybernetickou a informační bezpečnost.*

- *V případě, že podnikatel nebude daný druh zajištění ochrany UI realizovat, uvede zde tuto skutečnost, nebo předmětný bod neuvede.*

## 3.5. Kryptografická ochrana

- *V případě, že podnikatel bude daný druh zajištění ochrany UI realizovat, uvede pouze obecně tuto skutečnost a dále zpracuje samostatnou dokumentaci, která je přílohou žádosti o certifikaci kryptografického prostředku pro Národní úřad pro kybernetickou a informační bezpečnost.*

- *V případě, že podnikatel nebude daný druh zajištění ochranu UI realizovat, uvede zde tuto skutečnost, nebo předmětný bod neuvede.*

# 4. SEZNAM FUNKCÍ A OSOB, U KTERÝCH SE PŘEDPOKLÁDÁ PŘÍSTUP K UI

- *Vytvořit seznam funkcí a osob, u kterých se předpokládá přístup k UI v příloze dotazníku podnikatele a zde uvést odkaz na tuto skutečnost, příp. vytvořený seznam uvést zde, včetně všech požadovaných údajů dle zákona (jméno, příjmení, rodné číslo atd.).*

# 5. PŘÍLOHOVÁ ČÁST

- **Příloha č. 1 – administrativní směrnice** (vyhláška č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací, ve znění pozdějších předpisů, aplikovaná na podmínky podnikatele).

- **Příloha č. 2 – projekt fyzické bezpečnosti** (vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů, aplikovaná na podmínky podnikatele).