Soukromé bezpečnostní služby a standardy Národního bezpečnostního úřadu

Michaela Mikuličová

Bakalářská práce
2014

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2013/2014

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Michaela Mikuličová**
Osobní číslo:	**A11042**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**prezenční**
Téma práce:	**Soukromé bezpečnostní služby a standardy Národního bezpečnostního úřadu**

Zásady pro vypracování:

1. **Zpracujte rešerši literatury a pramenů, které souvisí se zvolenou problematikou.**
2. **Vymezte zkoumanou oblast (fenomenologie, etiologie), včetně právních aspektů a historických souvislostí ve vztahu k ochraně utajovaných informací a bezpečnostní způsobilosti.**
3. **Analyzujte aktuální stav problémů při plnění standardů Národního bezpečnostního úřadu ze strany soukromých bezpečnostních služeb.**
4. **Tvůrčí část bakalářské práce zaměřte na syntézu, prezentujte vlastní návrhy a doporučení, která mohou nalézt uplatnění v bezpečnostní praxi.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **BRABEC, František et al. Bezpečnost pro firmu, úřad, občana. Praha: Public History, 2001. ISBN 80-86445-04-6.**
2. **KAMENÍK, Jiří et al. Komerční bezpečnost: Soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostních agentur. Praha: ASPI, 2007. ISBN 978-80-7357-309-6.**
3. **LAUCKÝ, Vladimír. Technologie komerční bezpečnosti II. 2. vyd. Zlín: Univerzita Tomáše Bati, 2007. ISBN 978-80-7318-631-9.**
4. **MACEK, Pavel a František NOVÁK. Privátní bezpečnostní služby. Praha: POLICE HISTORY, 2005. ISBN 80-86477-23-1.**
5. **MACEK, Pavel et al. Bezpečnostní služby. Praha: POLICE HISTORY, 2001. ISBN 80-86477-03-7.**

Vedoucí bakalářské práce: **PhDr. Mgr. Stanislav Zelinka**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **7. března 2014**

Termín odevzdání bakalářské práce: **10. června 2014**

Ve Zlíně dne 7. března 2014

prof. Ing. Vladimír Vašek, CSc.
děkan

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

doc. Mgr. Milan Adámek, Ph.D.
ředitel ústavu

ABSTRAKT

Cílem bakalářské práce je zpracovat problematiku ochrany utajovaných informací a bezpečnostní způsobilosti, analyzovat problémy, kterým čelí soukromé bezpečnostní služby při plnění standardů Národního bezpečnostního úřadu a následně navrhnout řešení těchto problémů.

Klíčová slova: soukromé bezpečnostní služby, Národní bezpečnostní úřad, utajovaná informace

ABSTRACT

The aim of this bachelor thesis is to write up the issue of protection of classified information and security eligibility, analyze the problems that private security services face in meeting the standards of the National Security Authority and then propose solutions to these problems.

Keywords: private security agency, National Security Authority, classified information

Ráda bych poděkovala vedoucímu bakalářské práce panu PhDr. Mgr. Stanislavu Zelinkovi za vedení této práce, rady a poskytnuté informace.

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně …….
podpis diplomanta

OBSAH

ÚVOD

Problematika ochrany určitých informací provází lidstvo od nepaměti. Znalost takové informace zajišťovala výhodu nad těmi, kteří informaci neznali. Zvláštní kategorii chráněných informací tvoří utajované informace. Ústředním správním úřadem pro tuto oblast je Národní bezpečnostní úřad, který byl zřízen v roce 1998 zákonem č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů.

Národní bezpečnostní úřad je velmi důležitou institucí, protože plní mnoho úkolů v oblasti ochrany utajovaných informací. NBÚ např. vydává osvědčení pro přístup k utajovaným informacím, zajišťuje jednotné provádění ochrany utajovaných informací v ČR, provádí certifikaci technických prostředků, informačních systémů, kryptografických prostředků, kryptografických pracovišť a stínicích komor používaných při ochraně utajovaných informací atd.

Od roku 2006 byl zákon č. 148/1998 Sb. nahrazen zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. Ten je v době psaní této práce stále platný.

Cílem mé práce je popsat problematiku ochrany utajovaných informací a bezpečnostní způsobilosti v ČR, stručně vymezit vývoj a činnost soukromých bezpečnostních služeb, popsat hlavní úkoly, oprávnění a strukturu Národního bezpečnostního úřadu a nakonec analyzovat problémy, kterým čelí soukromé bezpečnostní služby při plnění standardů NBÚ, a navrhnout možná řešení těchto problémů.

I. TEORETICKÁ ČÁST

1 SOUKROMÉ BEZPEČNOSTNÍ SLUŽBY V ČR

Tato kapitola stručně popisuje vývoj soukromých bezpečnostních služeb, právní aspekty jejich činnosti a jejich hlavní úkoly.

1.1 Stručný vývoj soukromých bezpečnostních služeb

Forma soukromé ochrany osob a majetku předcházela policejní a vojenské síle státní moci. Ve feudalismu panovníci vytvářeli pro svou osobní ochranu a ochranu svého majetku soukromé ozbrojené síly a také využívali vyšetřovací a rozvědné služby, díky kterým získávali informace pro své rozhodování. Vyčleňováním z ozbrojených sil vznikaly policejní oddíly, které zajišťovaly pořádek ve městech a dobytých regionech. Postupně vznikala metodika ochrany pořádku, vlastnictví, zdraví a života obyvatelstva. [4]

Za první republiky fungovaly na území ČR privátní detektivní kanceláře jako např. Bubníkův detektivní ústav nebo Foglarova detektivní kancelář. Činnosti těchto kanceláří byly v období okupace zakázány správou Protektorátu Čechy a Morava, čímž došlo na pět let k jejich útlumu. K částečné obnově privátních detektivních kanceláří došlo po osvobození Československa v roce 1945. Po komunistickém převratu v únoru 1948 pak došlo k jejich úplné likvidaci. [2, 10]

Po listopadu 1989 začaly na základě NV č. 1/1988 Sb., o prodeji zboží a poskytování jiných služeb občany na základě povolení národního výboru, vznikat firmy, které se specializovaly na ochranu majetku a osob, tzv. hlídací služby. V roce 1992 pak přešly činnosti poskytované soukromými bezpečnostními službami do režimu živnostenského zákona jako koncesované živnosti a podnikání formou soukromých bezpečnostních služeb se začalo stávat významných odvětvím, které má i dnes doplňující roli v bezpečnostní komunitě státu. [2, 7, 10]

1.2 Právní aspekty činnosti soukromých bezpečnostních služeb

Činnost SBS český právní řád samostatně a výslovně neupravuje. Proto SBS na svou činnost aplikují obecně platné právní normy, které upravují práva fyzických a právnických osob na svépomoc při ochraně oprávněných zájmů. Mezi základní právní normy, které SBS ke své činnosti využívají, patří např.:

- zákon č. 2/1993 Sb., Listina základních práv a svobod,

- zákon č. 89/2012 Sb., občanský zákoník,
- zákon č. 262/2006 Sb., zákoník práce,
- zákon č. 455/1991 Sb., o živnostenském podnikání,
- zákon č. 40/2009 Sb., trestní zákoník. [4, 8]

1.3 Hlavní úkoly soukromých bezpečnostních služeb

V současné době jsou jako soukromé bezpečnostní služby (SBS) označovány placené, na komerčním základě poskytované služby zajišťující ochranu a ostrahu oprávněných zájmů fyzických a právnických osob. Zákon č. 455/1991 Sb., o živnostenském podnikání pak definuje činnost SBS, když uvádí koncesované živnosti:

- poskytování technických služeb k ochraně majetku a osob,
- služby soukromých detektivů,
- ostraha majetku a osob. [6, 8]

Mezi hlavní úkoly vykonávané při poskytování technických služeb k ochraně majetku a osob patří:

- projektování, montáž, kontrola, údržba a oprava PZTS, EPS, systémů kontroly vstupu, kamerových systémů a dalších systémů určených k ochraně majetku a osob před neoprávněnými zásahy,
- montáž, opravy, údržba, revize a správa mechanických zábranných systémů, které dodatečně zvyšují účinnost běžných standardů při zabezpečení majetku a osob,
- poradenství věcně související s těmito úkoly. [5]

Mezi hlavní úkoly služeb soukromých detektivů patří např.:

- hledání majetku a osob,
- zjišťování skutečností, které mohou sloužit jako důkazní prostředky v řízení před soudem nebo správním orgánem,
- získávání informací o fyzických nebo právnických osobách,
- získávání informací v souvislosti s vymáháním pohledávek,
- vyhledávání protiprávních jednání, která ohrožují obchodní tajemství,
- poradenství v souvislosti s těmito úkoly. [5, 8]

Mezi hlavní úkoly při poskytování služeb k ostraze majetku a osob, tj. při poskytování hlídacích služeb, pak patří:

- ostraha a ochrana nemovitého majetku,
- ostraha při přepravě peněz, cenností a jiného majetku,
- ochrana osob a vymezených zájmů,
- zajišťování pořádku v místech soustředění osob jako jsou veřejná shromáždění, slavnosti, sportovní podniky atp.,
- zpracování plánů ochrany,
- provozování DPPC,
- poradenství v souvislosti s těmito úkoly. [5, 8]

2 NÁRODNÍ BEZPEČOSTNÍ ÚŘAD

Národní bezpečnostní úřad (NBÚ) je orgánem moci výkonné a je ústředním správním úřadem pro oblast ochrany utajovaných informací a bezpečnostní způsobilosti. Byl zřízen zákonem č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů, a to k 1. srpnu 1998. V současné době se NBÚ ve své činnosti řídí především zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. [11, 12] V následujících podkapitolách jsou popsány hlavní úkoly NBÚ, jeho oprávnění při plnění těchto úkolů a také jeho organizační struktura.

2.1 Hlavní úkoly

Mezi hlavní úkoly NBÚ, jakožto ústředního správního úřadu, patří:

- rozhodování o vydání osvědčení fyzické osoby, osvědčení podnikatele, dokladu o bezpečnostní způsobilosti fyzické osoby a také rozhodování o zrušení platnosti těchto osvědčení a tohoto dokladu,
- zajišťování zkoušek zvláštní odborné způsobilosti a vydávání osvědčení o zvláštní odborné způsobilosti,
- plnění úkolů v oblasti ochrany utajovaných informací, a to v souladu se závazky vyplývajícími z členství ČR v EU a NATO,
- provádění certifikace technického prostředku, informačního systému, kryptografického prostředku, kryptografického pracoviště a stínicí komory,
- zajišťování výzkumu, vývoje a výroby národních kryptografických prostředků,
- vyvíjení a schvalování národních šifrových algoritmů a vytváření národní politiky kryptografické ochrany,
- zjišťování kompromitujícího vyzařování tam, kde se vyskytují nebo budou vyskytovat utajované informace,
- vydávání bezpečnostních standardů,
- ukládání sankcí za nedodržení povinností stanovených zákonem č. 412/2005 Sb. atd. [9, 20]

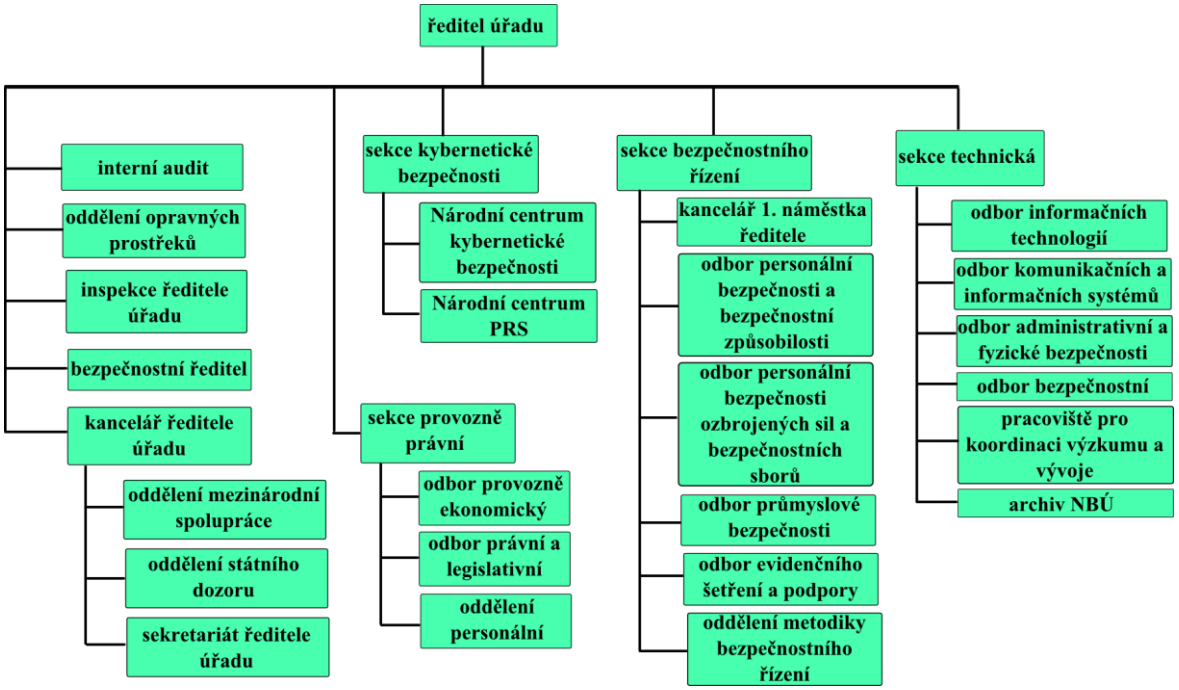
2.2 Oprávnění

NBÚ má při plnění svých úkolů podle zákona č. 412/2005 Sb. oprávnění:

- zpracovávat osobní údaje v rozsahu, který je nezbytný pro plnění těchto úkolů,
- uchovávat ve svých informačních systémech údaje získané v rámci plnění těchto úkolů,
- vést evidenci porušení ochrany utajovaných informací a evidenci osob, které mají přístup k utajovaným informacím,
- vést certifikační spis informačního systému, kryptografického prostředku, kryptografického pracoviště a stínicí komory,
- nahlížet do trestních spisů a pořizovat si z nich výpisy nebo jejich kopie,
- poskytovat v nezbytném rozsahu orgánu státu, právnické nebo podnikající fyzické osobě potřebné osobní údaje, které se vztahují k vyžádané informaci, atd. [20]

2.3 Organizační struktura

V čele NBÚ je ředitel úřadu, kterého jmenuje a odvolává vláda. Ředitel je odpovědný předsedovi vlády nebo pověřenému členovi vlády. Pod ředitele úřadu spadá bezpečnostní ředitel, oddělení opravných prostředků, interní audit, inspekce ředitele úřadu, kancelář ředitele úřadu, sekce kybernetické bezpečnosti, sekce provozně právní, sekce bezpečnostního řízení a sekce technická. [13, 20]



Obr. 1: Schéma organizační struktury NBÚ

3 OCHRANA UTAJOVANÝCH INFORMACÍ A BEZPEČNOSTNÍ ZPŮSOBILOST

V následujících podkapitolách je stručně popsána historie a právní aspekty ochrany utajovaných informací a bezpečnostní způsobilosti, dále jsou vymezeny pojmy, které souvisí s ochranou utajovaných informací, a druhy zajištění ochrany utajovaných informací. Nakonec je stručně popsána bezpečnostní způsobilost.

3.1 Historie a právní aspekty ochrany utajovaných informací a bezpečnostní způsobilosti

Problematika utajování určitých informací je stará jako lidstvo samo. Jedinci, skupiny lidí i instituce jako církev nebo stát se snažili o to, aby určité informace o nich byly přístupné pouze vybranému okruhu osob. Důvodem bylo to, že znalost a utajení těchto informací byla pro oprávněnou osobu výhodou, která jí zajišťovala náskok vůči jiným osobám resp. institucím. [1]

Na území ČR byla do roku 1998 problematika utajování informací řešena zákonem č. 102/1971 Sb., o ochraně státního tajemství. Ten byl 1. listopadu 1998 nahrazen zákonem č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů, a to především z toho důvodu, že bylo třeba vytvořit systém ochrany kompatibilní se systémy uplatňovanými v EU a NATO. [3]

Pozornost při tvorbě zákona č. 148/1998 Sb. byla kladena zejména na personální bezpečnost, která byla v zákoně č. 102/1971 řešena nedostatečně, a také na průmyslovou bezpečnost, která v zákoně č. 102/1971 nebyla řešena vůbec. Další druhy bezpečnosti byly řešeny zcela samostatně jednotlivými vyhláškami NBÚ. Tento systém ochrany byl postaven na dvou základních principech. První princip říká, že by se měly skutečnosti utajovat co nejméně, ale co nejkvalitněji. Druhý princip říká, že s utajovanými skutečnostmi se mohou seznamovat pouze osoby, které je nezbytně nutně potřebují znát k výkonu povolání apod. [3]

Na těchto dvou principech je postaven i v současné době platný zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

Ten nabyl účinnosti dnem 1. ledna 2006 a nahradil tak zákon č. 148/1998 Sb. [20] Prováděcí právní předpisy k zákonu č. 412/2005 Sb. jsou uvedeny v tabulce.

Vyhláška č. 363/2011 Sb.,	o personální bezpečnosti a o bezpečnostní způsobilosti, ve znění vyhlášky č. 415/2013 Sb.
Vyhláška č. 405/2011 Sb.,	o průmyslové bezpečnosti ve znění vyhlášky č. 416/2013 Sb.
Vyhláška č. 432/2011 Sb.,	o zajištění kryptografické ochrany utajovaných informací, ve znění vyhlášky č. 417/2013 Sb.
Nařízení vlády č. 522/2005 Sb.,	kterým se stanoví seznam utajovaných informací, ve znění nařízení vlády č. 240/2008 Sb.
Vyhláška 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 vyhlášky č. 453/2011 Sb.
Vyhláška č. 525/2005 Sb.,	o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací, ve znění vyhlášky č. 434/2011 Sb.
Vyhláška č. 528/2005 Sb.,	o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008 Sb. a vyhlášky č. 454/2011 Sb.
Vyhláška č. 529/2005 Sb.,	o administrativní bezpečnosti a o registrech utajovaných informací, ve znění vyhlášky č. 55/2008 Sb. a vyhlášky č. 433/2011 Sb.

Tab. 1: Prováděcí právní předpisy k zákonu č. 412/2005 Sb.

Se zákonem č. 412/2005 Sb. je spjat také zákon č. 413/2005 Sb., o změně zákonů v souvislosti s přijetím zákona o ochraně utajovaných informací a o bezpečnostní

způsobilosti, ve znění pozdějších předpisů. Změny se týkají některých zákonů trestního řádu, zákona o bankách, zákona o ochraně osobních údajů atd. [21]

Samotný zákon č. 412/2005 Sb. obsahuje 161 paragrafů a je rozdělen do devíti částí:

- Část první (Základní ustanovení) uvádí předmět úpravy tohoto zákona a vymezuje pojmy pro účely tohoto zákona.
- Část druhá (Ochrana utajovaných informací) má celkem 12 hlav, ve kterých je řešena újma zájmu České republiky a dále jsou řešeny stupně utajení, jednotlivé druhy zajištění ochrany utajovaných informací, certifikace, osvědčení, povinnosti při ochraně utajovaných informací a poskytování utajovaných informací v mezinárodním styku.
- Část třetí (Bezpečnostní způsobilost) definuje citlivou činnost, popisuje podmínky pro vydání dokladu o bezpečnostní způsobilosti fyzické osoby a povinnosti právnické osoby, podnikající fyzické osoby a orgánu státu.
- Část čtvrtá (Bezpečnostní řízení) obsahuje 5 hlav, ve kterých jsou popsány obecné zásady bezpečnostního řízení, průběh řízení, rozklad a soudní přezkum, závěrečné a zmocňovací ustanovení.
- Část pátá (Výkon státní správy) podrobně popisuje postavení, práva a povinnosti Národního bezpečnostního úřadu, zpravodajských služeb, Ministerstva vnitra a policie.
- Část šestá (Státní dozor) se zabývá státním dozorem v oblasti ochrany utajovaných informací a bezpečnostní způsobilosti a přijmutím opatření k nápravě při porušení právních předpisů v této oblasti.
- Část sedmá (Kontrola činnosti Úřadu) pojednává o zřizování kontrolního orgánu, který provádí kontrolu činnosti Národního bezpečnostního úřadu a dále o právech a povinnostech tohoto orgánu.
- Část osmá (Správní delikty) popisuje přestupky a správní delikty, kterých se lze v oblasti ochrany utajovaných informací a bezpečnostní způsobilosti dopustit, a maximální finanční hodnoty pokut, které lze za jednotlivé přestupky a správní delikty uložit.

- Část devátá (Přechodná a závěrečná ustanovení) popisuje změny nebo zrušení v této části uvedených právních předpisů, a to v souvislosti s nabytím účinnosti tohoto zákona dnem 1. ledna 2006. [20]

3.2 Vymezení pojmů souvisejících s ochranu utajovaných informací

3.2.1 Utajovaná informace

Utajovaná informace je informace v jakékoli podobě a na jakémkoli nosiči označená podle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. Vyzrazení nebo zneužití utajované informace by mohlo způsobit újmu zájmu ČR nebo by mohlo být pro tento zájem nevýhodné. Utajované informace jsou uvedeny v seznamu utajovaných informací, který jednotlivé utajované informace klasifikuje do jednoho nebo více stupňů utajení. [20]

Zákon č. 412/2005 Sb. definuje celkem čtyři stupně utajení:

- Stupeň utajení Přísně tajné pro informace, jejichž vyzrazení nebo zneužití může způsobit mimořádně vážnou újmu zájmům ČR.
- Stupeň utajení Tajné pro informace, jejichž vyzrazení nebo zneužití může způsobit vážnou újmu zájmům ČR.
- Stupeň utajení Důvěrné pro informace, jejichž vyzrazení nebo zneužití může způsobit prostou újmu zájmům ČR.
- Stupeň utajení Vyhrazené pro informace, jejichž vyzrazení nebo zneužití může být nevýhodné pro zájmy ČR. [20]

3.2.2 Zájem České republiky

Zájmem ČR se rozumí zachování její ústavnosti, svrchovanosti a územní celistvosti. Dále pak zajištění vnitřního pořádku a bezpečnosti, mezinárodních závazků a obrany a také ochrana ekonomiky a ochrana života nebo zdraví fyzických osob. [20]

3.2.3 Původce utajované informace

Původcem utajované informace je ten, u koho utajovaná informace vznikla. Původcem může být orgán státu, právnická osoba, podnikající fyzická osoba nebo Úřad průmyslového vlastnictví. [20]

3.2.4 Neoprávněná osoba

Neoprávněnou osobou je taková fyzická nebo právnická osoba, jež nesplňuje podmínky pro přístup k utajovaným informacím dané zákonem č. 412/2005 Sb. [20]

3.2.5 Poučení

Poučení je písemný záznam o seznámení fyzické osoby s jejími právy a povinnostmi v souvislosti s ochranou utajovaných informací a také s následky porušení těchto povinností. Poučení zajistí ten, kdo je vůči fyzické osobě v rámci služebního poměru nebo pracovněprávního vztahu odpovědnou osobou, nebo odpovědná osoba toho, kdo umožní fyzické osobě přístup k utajované informaci. [20]

3.2.6 Bezpečnostní standard

Bezpečnostní standard je utajovaný soubor pravidel, ve kterém jsou stanoveny postupy, technická řešení, bezpečnostní parametry a organizační opatření. Tato pravidla slouží pro zajištění nejmenší možné míry ochrany utajovaných informací. [20]

3.2.7 Bezpečnostní provozní mód

Bezpečnostní provozní mód je prostředí, ve kterém pracuje informační systém. Toto prostředí je charakterizováno stupněm utajení zpracovávané utajované informace a úrovněmi oprávnění jeho uživatelů. [20]

3.2.8 Újma zájmu České republiky a nevýhodnost pro tyto zájmy

Újmou zájmu ČR se rozumí poškození nebo ohrožení zájmu ČR. Újma je členěna podle závažnosti tohoto poškození nebo ohrožení zájmu na mimořádně vážnou újmu, vážnou újmu a prostou újmu. [20]

Mimořádně vážná újma vznikne vyzrazením nebo zneužitím utajované informace stupně utajení Přísně tajné. Následkem tohoto vyzrazení resp. zneužití může dojít k bezprostřednímu ohrožení svrchovanosti, územní celistvosti nebo demokratických základů ČR, k rozsáhlým ztrátám na životech nebo rozsáhlému ohrožení zdraví obyvatel, k mimořádně vážnému nebo rozsáhlému poškození ekonomiky ČR, ke značnému narušení vnitřního pořádku a bezpečnosti, k mimořádně vážnému ohrožení významných bezpečnostních operací nebo činnosti zpravodajských služeb. Také může dojít k mimořádně vážnému ohrožení činnosti nebo bojeschopnosti NATO a EU nebo k mimořádně vážnému poškození diplomatických nebo jiných vztahů ČR k NATO, EU nebo členskému státu. [20]

Vážná újma vznikne, pokud je neoprávněné osobě vyzrazena nebo je zneužita utajovaná informace stupně utajení Tajné. To může mít za následek ohrožení svrchovanosti, územní celistvosti a demokratických základů ČR, značnou škodu ČR ve finanční, měnové nebo hospodářské oblasti, ztráty na životech nebo ohrožení zdraví obyvatel, narušení vnitřního pořádku a bezpečnosti ČR. Dále pak vážné ohrožení bojeschopnosti ČR, NATO nebo EU, vážné ohrožení činnosti NATO nebo EU, vážné ohrožení diplomatických vztahů ČR k NATO, EU nebo jinému státu nebo také vážné zvýšení mezinárodního napětí. [20]

Prostá újma vznikne vyzrazením nebo zneužitím utajované informace stupně utajení Důvěrné, což může mít za následek zhoršení vztahů ČR s cizí mocí, ohrožení bezpečnosti jednotlivců, ohrožení bojeschopnosti ČR, NATO nebo EU, ohrožení bezpečnostních operací nebo činnosti zpravodajských služeb, ohrožení činnosti NATO nebo EU, vznik nezanedbatelné škody ČR, závažné narušení ekonomických zájmů ČR nebo také zmaření, ztížení, ohrožení vyšetřování zvlášť závažných zločinů nebo usnadnění jejich páchání. [20]

Vyzrazení utajované informace stupně utajení Vyhrazené je nevýhodné pro zájmy ČR a může mít za následek narušení činnosti ozbrojených sil ČR, NATO nebo členského státu EU, poškození významných ekonomických zájmů ČR nebo EU, narušení důležitých obchodních nebo politických jednání ČR s cizí mocí, narušení bezpečnostních operací nebo činnosti zpravodajských služeb anebo zmaření, ztížení, ohrožení vyšetřování ostatních trestných činů než zvlášť závažných nebo usnadnění jejich páchání. [20]

3.2.9 Bezúhonnost

Bezúhonná je taková fyzická osoba, která nebyla pravomocně odsouzena za spáchání úmyslného trestného činu nebo trestného činu, který se vztahuje k ochraně utajovaných informací, nebo se na ni pohlíží jako by odsouzena nebyla. [20]

3.2.10 Osobnostní způsobilost

Fyzická osoba je osobnostně způsobilá, pokud netrpí poruchou nebo obtížemi, které mohou mít vliv na její spolehlivost nebo schopnost utajovat informace. To se ověřuje na základě prohlášení k osobnostní způsobilosti případně i na základě znaleckého posudku o osobnostní způsobilosti. [20]

3.2.11 Bezpečnostní spolehlivost a bezpečnostní riziko

Fyzické osoby nebo podnikatelé jsou bezpečnostně spolehliví, pokud u nich není zjištěno bezpečnostní riziko. Bezpečnostním rizikem u fyzické osoby je např. závažná nebo opakovaná činnost proti zájmům ČR, činnost spočívající v potlačování základních práv a svobod, pravomocné odsouzení pro trestný čin nebo porušení povinnosti při ochraně utajovaných informací. Bezpečnostním rizikem u podnikatele je pak např. činnost statutárního nebo kontrolního orgánu proti zájmům ČR, činnost statutárního nebo kontrolního orgánu spočívající v potlačování základních práv a svobod, pravomocné odsouzení podnikatele pro trestný čin nebo porušení povinnosti při ochraně utajovaných informací. [20]

3.2.12 Administrativní pomůcky

Utajovaná informace je evidována v administrativních pomůckách k tomu určených prováděcím právním předpisem (vyhláška č. 529/2005 Sb.). V administrativních pomůckách se zaznamenává také předávání, přebírání příp. jiný pohyb utajované informace. Mezi administrativní pomůcky patří např. jednací protokol, ve kterém je evidován utajovaný dokument, pomocný jednací protokol, ve kterém je evidován pohyb utajovaného dokumentu, a manipulační kniha, ve které je evidováno vytváření, převzetí a předání utajovaného dokumentu. Vzory administrativních pomůcek jsou uvedeny v přílohách k vyhlášce č. 529/2005 Sb. [19, 20]

3.2.13 Ochrana utajovaných informací před únikem kompromitujícím vyzařováním

Utajované informace stupně utajení Přísně tajné, Tajné a Důvěrné musí být před únikem kompromitujícím vyzařováním chráněny zabezpečením elektrických a elektronických zařízení, zabezpečené oblasti nebo objektu. Způsobilost elektrických a elektronických zařízení, zabezpečené oblasti nebo objektu k ochraně před únikem utajované informace kompromitujícím vyzařováním ověřuje NBÚ, a to při certifikaci informačního systému nebo kryptografického prostředku, při schvalování projektu bezpečnosti komunikačního systému atd. Ochrana utajované informace před únikem kompromitujícím vyzařováním může být zabezpečena také stínicí komorou. Takováto komora pak musí být certifikována NBÚ. [20]

3.2.14 Certifikace

Certifikace je postup, kterým NBÚ ověřuje způsobilost technických a kryptografických prostředků a stínicích komor k ochraně utajovaných informací, způsobilost informačních systémů k nakládání s utajovanými informacemi a způsobilost kryptografických pracovišť, která jsou určena k výrobě nebo testování materiálu k zajištění funkce kryptografického prostředku nebo která jsou centrálním distribučním a evidenčním místem kryptografického materiálu orgánu státu, právnické osoby nebo podnikající fyzické osoby. Pokud dané prostředky, systémy resp. pracoviště splňují způsobilost, vydá NBÚ certifikát. [20]

3.3 Druhy zajištění ochrany utajovaných informací

Podle zákona č. 412/2005 Sb. je ochrana utajovaných informací zajišťována personální, průmyslovou, administrativní a fyzickou bezpečností, bezpečností informačních a komunikačních systémů a kryptografickou ochranou. Tyto druhy zajištění ochrany utajovaných informací jsou popsány v následujících podkapitolách.

3.3.1 Personální bezpečnost

Personální bezpečnost zahrnuje výběr fyzických osob s přístupem k utajovaným informacím, ověřování podmínek pro jejich přístup k utajovaným informacím a také jejich výchovu a ochranu. [20]

Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti dělí personální bezpečnost na dvě části, a to na podmínky přístupu fyzické osoby k utajované

informaci stupně utajení Vyhrazené a na podmínky přístupu fyzické osoby k utajované informaci stupně utajení Přísně tajné, Tajné nebo Důvěrné. [20]

Aby byl fyzické osobě umožněn přístup k utajované informaci stupně utajení Vyhrazené, musí jej nezbytně potřebovat k výkonu své funkce, být držitelem oznámení o splnění podmínek pro přístup k utajované informaci stupně utajení Vyhrazené, být držitelem osvědčení fyzické osoby nebo dokladu a musí být poučena podle zákona č. 412/2005 Sb. Oznámení o splnění podmínek pro přístup k utajované informaci stupně utajení Vyhrazené vydá fyzické osobě buď ten, kdo je vůči ní v rámci služebního poměru nebo pracovněprávního vztahu odpovědnou osobou, anebo odpovědná osoba toho, kdo umožní fyzické osobě přístup k utajované informaci stupně utajení Vyhrazené. V ostatních případech vydá oznámení NBÚ na základě odůvodněné písemné žádosti. K vydání oznámení musí fyzická osoba splnit podmínky dané zákonem č. 412/2005 Sb., tzn. že musí být plně svéprávná, musí mít alespoň 18 let a musí být bezúhonná. Tyto podmínky musí fyzická osoba, která je držitelem oznámení, splňovat po celou dobu přístupu k utajované informaci stupně utajení Vyhrazené, což je jednou za 5 let povinen ověřovat ten, kdo oznámení vydal. [20]

Přístup k utajované informaci stupně utajení Přísně tajné, Tajné nebo Důvěrné lze umožnit osobě, která jej nezbytně potřebuje k výkonu své funkce, je držitelem platného osvědčení fyzické osoby příslušného stupně utajení a je poučena podle zákona č. 412/2005 Sb. Osvědčení fyzické osoby může získat fyzická osoba, pokud je státním občanem ČR nebo státním příslušníkem členského státu EU nebo NATO, je plně svéprávná, má alespoň 18 let, je bezúhonná, je osobnostně způsobilá a bezpečnostně spolehlivá. Tyto podmínky musí fyzická osoba splňovat po celou dobu platnosti osvědčení. Osvědčení vydává NBÚ a jeho platnost je 5 let pro stupeň utajení Přísně tajné, 7let pro stupeň utajení Tajné a 9 let pro stupeň utajení Důvěrné. [20]

Bez platného osvědčení fyzické osoby lze umožnit přístup k utajované informaci všech stupňů utajení pouze prezidentu republiky, poslancům a senátorům Parlamentu, členům vlády, Veřejnému ochránci práv a jeho zástupci, soudcům a prezidentovi, viceprezidentovi a členům Nejvyššího kontrolního úřadu. Tyto osoby mají k utajované informaci přístup po dobu výkonu své funkce a v rozsahu nezbytném pro tento výkon. [20]

Vyhláška č. 363/2011 Sb., o personální bezpečnosti a o bezpečnostní způsobilosti, ve znění vyhlášky č. 415/2013 Sb. pak stanovuje vzory v oblasti personální bezpečnosti a bezpečnostní způsobilosti, písemnosti přikládané k žádosti fyzické osoby, písemnosti přikládané k žádosti o doklad a způsob a formu podání těchto žádostí. [14]

3.3.2 Průmyslová bezpečnost

Průmyslovou bezpečnost tvoří systém opatření, která slouží jak ke zjišťování a ověřování podmínek pro přístup podnikatele k utajovaným informacím, tak i k zajištění nakládání s utajovanou informací u podnikatele v souladu se zákonem č. 412/2005 Sb. [20]

Podnikateli, který k výkonu své činnosti nezbytně potřebuje přístup k utajované informaci stupně utajení Vyhrazené, lze tento přístup umožnit v případě, že písemným prohlášením podnikatele doloží svou schopnost zabezpečit ochranu utajovaných informací nebo že je držitelem osvědčení podnikatele. Přístup k utajované informaci stupně utajení Důvěrné nebo vyšší lze podnikateli umožnit, pokud je držitelem osvědčení podnikatele příslušného stupně utajení. [20]

Osvědčení podnikatele vydá NBÚ podnikateli, který splňuje podmínky, tzn. že je ekonomicky stabilní a bezpečnostně spolehlivý, je schopen zabezpečit ochranu utajovaných informací a odpovědná osoba je držitelem platného osvědčení fyzické osoby nejméně pro takový stupeň utajení, pro který žádá podnikatel o vydání osvědčení. Tyto podmínky musí podnikatel splňovat po celou dobu platnosti osvědčení podnikatele, což je 5 let pro stupeň utajení Přísně tajné, 7 let pro stupeň utajení Tajné a 9 let pro stupeň utajení Důvěrné. [20]

Vyhláška č. 405/2011 Sb., o průmyslové bezpečnosti, ve znění vyhlášky č. 416/2013 Sb. pak stanovuje vzory v oblasti průmyslové bezpečnosti, písemnosti k ověření podmínek pro vydání osvědčení podnikatele a způsob a formu podání žádosti podnikatele. [15]

3.3.3 Administrativní bezpečnost

Administrativní bezpečnost je tvořena systémem opatření pro nakládání s utajovanými informacemi. Takovýmto nakládáním s utajovanými informacemi může být jejich tvorba, příjem, evidence, zpracování, přeprava, ukládání atd. [20]

Původce utajované informace je povinen na informaci vyznačit svůj název, stupeň jejího utajení, její evidenční označení a datum jejího vzniku. Pokud je ČR poskytnuta utajovaná

informace a pokud ČR tuto informaci eviduje jako první, pak na ni orgán státu, právnická osoba nebo podnikající fyzická osoba vyznačí stupeň utajení v souladu s mezinárodní smlouvou a také zkratku podle této smlouvy. [20]

Vyznačený stupeň utajení musí být zachován po celou dobu trvání utajení a bez souhlasu původce nebo poskytující cizí moci nesmí být změněn ani zrušen. Původce je pak povinen nejméně jednou za pět let prověřit, jestli důvod pro utajení informace trvá. Pokud původce zruší nebo změní stupeň utajení, musí o tom neprodleně písemně uvědomit všechny adresáty utajované informace. [20]

Vyhláška č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací, ve znění pozdějších předpisů (vyhlášky č. 55/2008 Sb. a vyhlášky č. 433/2011 Sb.) pak stanovuje způsob vyznačování náležitostí na utajované informace, druhy administrativních pomůcek a rozsah podkladových materiálů stupně utajení Vyhrazené, podrobnosti k přepravě, převzetí a pořizování kopie utajovaných dokumentů a také organizaci a činnost registrů utajovaných informací. [19]

3.3.4 Fyzická bezpečnost

Fyzickou bezpečnost tvoří systém opatření, jejichž účelem je neoprávněné osobě zabránit nebo ztížit přístup k utajovaným informacím, popř. tento přístup nebo pokus o něj zaznamenat. [20]

Pro zabezpečení ochrany utajovaných informací jsou v rámci fyzické bezpečnosti určeny objekty, zabezpečené oblasti a jednací oblasti. Objekt je budova nebo jiný ohraničený prostor, ve kterém se nachází zabezpečená oblast nebo jednací oblast. Zabezpečená oblast je, stejně jako jednací oblast, ohraničený prostor v objektu. Utajovanou informaci stupně utajení Přísně tajné nebo Tajné je pak možné projednávat pouze v jednací oblasti. [20]

Zabezpečené oblasti a objekty se řadí do kategorií Přísně tajné, Tajné, Důvěrné nebo Vyhrazené, a to podle nejvyššího stupně utajení utajované informace, která se v nich ukládá, resp. zpracovává. Zabezpečené oblasti se podle možnosti přístupu k utajované informaci dále dělí do dvou tříd, a to třída I, kdy vstupem do této oblasti dochází k seznámení s utajovanou informací, a třída II, kdy vstupem do této oblasti k seznámení s utajovanou informací nedochází. [20]

Odpovědná osoba musí zajistit, aby v jednací oblasti nedocházelo k ohrožení nebo úniku projednávaných utajovaných informací. V souvislosti s tím musí požádat NBÚ o provedení kontroly, zda nejsou v jednací oblasti nedovoleně umístěny technické prostředky k získávání informací. Vstup do jednací oblasti a výstup z ní pak musí být kontrolován opatřeními fyzické bezpečnosti, a to ostrahou, režimovými opatřeními a technickými prostředky. [20]

Zákon č. 412/2005 Sb. stanovuje požadavky na ostrahu zabezpečených oblastí podle jejich kategorie. Ostraha je nepřetržitě zajišťována nejméně dvěma osobami u objektu pro zabezpečenou oblast kategorie Přísně tajné, nejméně jednou osobou u objektu a jednou osobou, která rychle zasáhne, pokud dojde k narušení ochrany utajovaných informací, pro zabezpečenou oblast kategorie Tajné a nejméně jednou osobou, která rychle zasáhne v případě narušení ochrany utajovaných informací, pro zabezpečenou oblast kategorie Důvěrné. U zabezpečené oblasti kategorie Vyhrazené je ostraha zajišťována v rozsahu stanoveném odpovědnou osobou. Ostraha jednacích oblastí pro utajované informace stupně utajení Přísně tajné a Tajné je zajišťována obdobně jako ostraha zabezpečených oblastí těchto stupňů utajení. Ostraha je prováděna zaměstnanci orgánu státu, právnické osoby nebo podnikající fyzické osoby, o jejichž objekt jde, a dále pak příslušníky ozbrojených sil, ozbrojených bezpečnostních sborů, příslušníky ozbrojených sil cizí moci nebo zaměstnanci soukromé bezpečnostní služby. [20]

Režimová opatření stanovují oprávnění osob a dopravních prostředků pro vstup, resp. vjezd do objektu, oprávnění pro vstup do zabezpečené oblasti a jednací oblasti, způsob kontroly těchto oprávnění, podmínky a způsob kontroly pohybu osob v objektu, zabezpečené oblasti a jednací místnosti atd. Tato oprávnění vydává odpovědná osoba nebo osoba jí pověřená. Osoby bez oprávnění pak mohou do objektu kategorie Důvěrné, Tajné nebo Přísně tajné a do zabezpečené nebo jednací oblasti vstupovat pouze v doprovodu osoby, která je ke vstupu oprávněná, a za podmínky, že je tento vstup nezbytný a nenaruší ochranu utajovaných informací. Na vstupu do objektu kategorie Důvěrné, Tajné nebo Přísně tajné se provádí kontrola vstupu a u osob, které nemají oprávnění ke vstupu, je vedena také evidence údajů. [18, 20]

Technickými prostředky, jakožto opatřením fyzické bezpečnosti, jsou především mechanické zábranné prostředky, elektrická zámková zařízení a systémy pro kontrolu vstupů, zařízení poplachových zabezpečovacích systémů, speciální televizní systémy, tísňové systémy, zařízení elektrické požární signalizace, zařízení proti pasivnímu a aktivnímu

odposlechu atd. Objekt kategorie Vyhrazené se zabezpečuje pomocí mechanických zábranných prostředků, objekt kategorie Důvěrné nebo Tajné se zabezpečuje pomocí mechanických zábranných prostředků a zařízení poplachových zabezpečovacích systémů a objekt kategorie Přísně tajné se zabezpečuje pomocí mechanických zábranných prostředků, zařízení poplachových zabezpečovacích systémů a speciálních televizních systémů, které ale nesmí narušit ochranu utajovaných informací. Zabezpečená oblast kategorie Vyhrazené je zabezpečována mechanickými zábrannými prostředky, zabezpečená oblast kategorie Důvěrné je zabezpečována mechanickými zábrannými prostředky a zařízeními poplachových zabezpečovacích systémů a zabezpečená oblast kategorie Tajné nebo Přísně tajné je zabezpečována mechanickými zábrannými prostředky, systémy pro kontrolu vstupů, zařízeními poplachových zabezpečovacích systémů, zařízeními EPS a speciálními televizními systémy, které však nesmí narušit ochranu utajovaných informací. Speciální televizní systémy mohou být nahrazeny tísňovými systémy. Jednací oblasti pro projednávání utajovaných informací stupňů utajení Tajné a Přísně tajné se zabezpečují stejnými technickými prostředky jako zabezpečené oblasti pro tyto stupně utajení a navíc také zařízeními proti pasivnímu a aktivnímu odposlechu. [18, 20]

Opatření fyzické bezpečnosti musí odpovídat alespoň nejnižší míře zabezpečení jednací nebo zabezpečené oblasti. Opatření se stanoví v závislosti na vyhodnocení rizik a na stupni utajení utajovaných informací v jednací místnosti projednávaných nebo v závislosti na kategorii zabezpečené oblasti. Hodnocení rizik musí být prováděno průběžně a případně musí být míra opatření upravena. Orgán státu, právnická a fyzická osoba jsou pak povinni pravidelně ověřovat, jestli tato opatření odpovídají projektu fyzické bezpečnosti a právním předpisům v oblasti utajovaných informací. [20]

Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů (vyhlášky č. 19/2008 Sb. a vyhlášky č. 454/2011 Sb.) pak stanovuje bodové ohodnocení jednotlivých opatření fyzické bezpečnosti, nejnižší míru zabezpečení zabezpečené a jednací oblasti, způsob ukládání utajovaných informací v závislosti na stupni jejich utajení, organizační požadavky na provádění ostrahy, podrobnosti režimových opatření, požadavky na technické prostředky a náležitosti žádosti o certifikaci technického prostředku. [18, 20]

3.3.5 Bezpečnost informačních a komunikačních systémů

Bezpečnost informačních a komunikačních systémů je tvořena systémem opatření, která mají zajistit důvěrnost, integritu a dostupnost utajovaných informací, se kterými tyto systémy nakládají. Tato opatření mají také zajistit odpovědnost správy a uživatele za jejich činnost v těchto systémech. [20]

Informační systém nakládající s utajovanými informacemi tvoří jeden nebo více počítačů, jejich programové vybavení, periferní zařízení, správa tohoto informačního systému a k tomuto systému se vztahující procesy nebo prostředky, které jsou schopné provádět sběr, tvorbu, zpracování, ukládání, zobrazení nebo přenos utajovaných informací. Takovýto informační systém musí být certifikován NBÚ a písemně schválen do provozu odpovědnou osobou nebo jí pověřenou osobou. [20]

Komunikační systém nakládající s utajovanými informacemi je systém, který zajišťuje přenos těchto informací mezi koncovými uživateli a který zahrnuje koncové komunikační zařízení, přenosové prostředí, kryptografické prostředky, obsluhu a provozní podmínky a postupy. Takovýto komunikační systém musí být provozován v souladu s projektem bezpečnosti komunikačního systému, který je schválen NBÚ. Komunikační systém musí být schválen do provozu také písemně, a to odpovědnou osobou nebo jí pověřenou osobou. [20]

Vyhláška 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 vyhlášky č. 453/2011 Sb. pak stanovuje požadavky na informační a komunikační systémy nakládající s utajovanými informacemi, požadavky na ochranu utajovaných informací v elektronické podobě v zařízeních, která nejsou součástí informačního nebo komunikačního systému a požadavky na ochranu utajovaných informací před jejich únikem kompromitujícím vyzařováním. Také stanovuje požadavky na provádění certifikace informačních systémů a stínicích komor a požadavky na schvalování projektů bezpečnosti komunikačních systémů. [17]

3.3.6 Kryptografická ochrana

Kryptografická ochrana je systém opatření, která slouží k ochraně utajovaných informací za pomoci kryptografických metod a kryptografických materiálů, a to při zpracování, přenosu nebo ukládání utajovaných informací. [20]

Výkon kryptografické ochrany musí provádět pracovník kryptografické ochrany, který je k tomu pověřen odpovědnou osobou, je držitelem platného osvědčení fyzické osoby a je držitelem osvědčení o zvláštní odborné způsobilosti pracovníka kryptografické ochrany. K získání osvědčení o zvláštní odborné způsobilosti musí pracovník složit zkoušku odborné způsobilosti před zkušební komisí. Osvědčení pak vydá NBÚ nebo orgán státu, a to nejdéle na 5 let. [20]

Vyhláška č. 432/2011 Sb., o zajištění kryptografické ochrany utajovaných informací, ve znění vyhlášky č. 417/2013 Sb. pak stanovuje podrobnosti o odborné zkoušce, způsoby a prostředky manipulace s kryptografickým materiálem, podrobnosti způsobu vyznačování náležitostí na utajované informace z oblasti kryptografické ochrany a stanovuje také administrativní pomůcky kryptografické ochrany utajovaných informací. [16]

3.4 Bezpečnostní způsobilost

Bezpečnostně způsobilá je osoba, která je držitelem platného dokladu o bezpečnostní způsobilosti fyzické osoby. Tento doklad vydá NBÚ takové fyzické osobě, která je plně svéprávná, má alespoň 18 let, je bezúhonná, osobnostně způsobilá a spolehlivá. Platnost dokladu je 5 let. [20]

Pro účely bezpečnostní způsobilosti se rozumí bezúhonnou fyzickou osobou taková osoba, která nebyla pravomocně odsouzena za spáchání úmyslného trestného činu nebo se na ni hledí jako by odsouzena nebyla. Osobnostně způsobilou fyzickou osobou se rozumí taková osoba, která netrpí poruchou nebo obtížemi, které by mohly mít vliv na její spolehlivost vykonávat citlivou činnost. Spolehlivou fyzickou osobou se rozumí taková osoba, u které nebyla zjištěna negativní okolnost, jako je činnost proti zájmu ČR, pravomocné odsouzení pro trestný čin atd. [20]

Bezpečnostně způsobilá osoba nebo osoba, která je držitelem platného osvědčení fyzické osoby, může vykonávat citlivou činnost. Citlivá činnost je taková činnost, jejímž zneužitím by mohlo dojít k ohrožení zájmu ČR. [20]

II. PRAKTICKÁ ČÁST

4 ANALÝZA PROBLÉMŮ SOUKROMÝCH BEZPEČNOSTNÍCH SLUŽEB PŘI PLNĚNÍ STANDARDŮ NÁRODNÍHO BEZPEČNOSTNÍHO ÚŘADU

Standardy jsou požadavky na ochranu utajovaných informací uvedené v zákoně č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, a v souvisejících prováděcích předpisech. V následujících podkapitolách jsou analyzovány problémy, kterým SBS při plnění těchto standardů čelí.

4.1 Problém mlčenlivosti zaměstnanců

Povinnost zachovávat mlčenlivost o utajované informaci má podle zákona č. 412/2005 Sb. každý, kdo k utajované informaci měl nebo má přístup, pokud nebyl této mlčenlivosti zproštěn. [20] Některé SBS sice splňují požadavky na ochranu utajovaných informací, ale musí čelit problému se zaměstnanci, kteří nezachovávají mlčenlivost.

Tento problém se týká především těch zaměstnanců SBS, kteří mají při výkonu svých činností přístup k utajovaným informacím. U těchto zaměstnanců někdy dochází k tomu, že utajovanou informaci vyzradí neoprávněné osobě, a to obvykle za úplatu. V mnoha případech pak není možné zjistit, který zaměstnanec utajovanou informaci vyzradil.

Zachování mlčenlivosti se do jisté míry týká také zaměstnanců SBS, kteří při výkonu svých činností nemají přístup k utajovaným informacím. Jedná se např. o zaměstnance provádějící ostrahu objektu, ve kterém se nacházejí utajované informace. Problémem je, že tito zaměstnanci mohou poskytnout některé informace o zabezpečení objektu neoprávněné osobě a usnadnit jí tak přístup do objektu, ve kterém se nacházejí utajované informace. K tomu dochází nejčastěji za úplatu.

4.2 Problém namátkových prohlídek

Namátkové prohlídky jsou součástí fyzické bezpečnosti a jsou prováděny při vstupu do objektu nebo zabezpečené oblasti resp. při výstupu z nich. Tyto prohlídky se týkají vozidel i osob. Protože činnost SBS není upravena vlastním právním předpisem, musí se zaměstnanci SBS při provádění osobních prohlídek řídit trestním řádem. Ten říká, že osobní prohlídku může provádět pouze osoba stejného pohlaví.

SBS, které jako ostrahu zaměstnávají pouze muže, pak čelí problému, že podle trestního řádu neprovádějí osobní prohlídky na ženách, které vstupují do objektu, a podstupují tak riziko, že tyto ženy do objektu vnesou nežádoucí zařízení, např. zařízení sloužící k odposlechu, resp. že z objektu vynesou utajovanou informaci apod. Nebo plní požadavky na ochranu utajovaných informací a osobní prohlídky provádějí i na ženách a porušují tak trestní řád.

4.3 Problém se zaměstnanci umisťujícími v objektu odposlechová a nahrávací zařízení

Průchozí detektor kovových předmětů a rentgenový přístroj pro kontrolu zavazadel se používají na vstupu do objektu nebo zabezpečené oblasti kategorie Přísně tajné a na vstupu do jednací oblasti, ve které se pravidelně projednávají utajované informace stupně utajení Přísně tajné. Jednací oblasti, ve kterých se pravidelně projednávají utajované informace stupně utajení Přísně tajné nebo Tajné, musí být také zabezpečeny technickými prostředky proti pasivnímu a aktivnímu odposlechu.

Pro objekty a zabezpečené oblasti jiných kategorií než Přísně tajné a pro objekty, ve kterých nejsou jednací oblasti pro projednávání utajované informace stupňů utajení Přísně tajné nebo Tajné, nejsou stanoveny požadavky na použití detektorů kovových předmětů, rentgenových přístrojů ani technických prostředků proti pasivnímu a aktivnímu odposlechu. Proto je pro zaměstnance snazší do těchto objektů a zabezpečených oblastí vnést a umístit odposlechové nebo nahrávací zařízení a po splnění jeho účelu jej zase odnést. Tyto nezákonně získané odposlechy utajovaných informací pak prodávají neoprávněným osobám.

4.4 Problémy s nezodpovědnými uživateli informačních systémů

Mezi požadavky počítačové bezpečnosti informačních systémů patří jednoznačná identifikace a autentizace uživatele. Tento požadavek lze splnit např. použitím přístupového hesla. Stanovuje se minimální délka hesla, způsob jeho vytvoření a interval, po kterém by mělo být heslo změněno.

Problém, kterému SBS čelí, jsou nezodpovědní uživatelé, kteří, ač byli proškoleni, nepoužívají stanovenou minimální délku hesla, způsob jeho vytvoření nebo si nemění heslo

ve stanovených intervalech. Takto usnadňují neoprávněné osobě prolomení hesla a tím i přístup do informačního systému.

Problémem jsou také uživatelé, kteří si heslo nepamatují, a proto ho mají napsané např. na papírku, který ztratí, je jim ukraden nebo si z něj heslo někdo přečte. Informační systém pak může být vystaven útoku neoprávněné osoby, která toto heslo získá.

Jedním z častých problémů s nezodpovědnými uživateli informačních systémů je také problém s uživateli, kteří nechají počítač s přístupem k utajovaným informacím zapnutý a odejdou, aniž by se odhlásili. Tím umožňují přístup k utajovaným informacím neoprávněným osobám, které se k počítači dostanou.

5 SHRNUTÍ A NÁVRHY ŘEŠENÍ JEDNOTLIVÝCH PROBLÉMŮ SOUKROMÝCH BEZPEČNOSTNÍCH SLUŽEB PŘI PLNĚNÍ STANDARDŮ NÁRODNÍHO BEZPEČNOSTNÍHO ÚŘADU

V této kapitole jsou shrnuty jednotlivé problémy, kterým čelí SBS při plnění standardů NBÚ a které byly analyzovány v předchozí kapitole. Pro každý problém je navržena alespoň jedna varianta řešení.

5.1 Návrh řešení problému mlčenlivosti zaměstnanců

Zaměstnanci SBS, kteří porušili povinnost zachovávat mlčenlivost o utajované informaci a za úplatu tuto informaci vyzradili neoprávněné osobě, se dopustili přestupku, za který mohou být NBÚ pokutováni až do 5 milionů Kč. Tito zaměstnanci se obvykle spoléhají na to, že se na jejich přestupek nepřijde.

Obdobná situace je i u zaměstnanců SBS, kteří nejsou oprávněni se seznamovat s utajovanými informacemi, ale poskytli neoprávněné osobě informace o zabezpečení objektu, ve kterém se vyskytují utajované informace, a usnadnili jí tak přístup do tohoto objektu. Tito zaměstnanci SBS se dopustili přestupku, protože umožnili neoprávněné osobě přístup k utajované informaci. Za tento přestupek mohou být NBÚ pokutováni do 5 milionů Kč.

Tato porušení povinnosti při ochraně utajovaných informací musí SBS hlásit NBÚ. V opačném případě se SBS dopustí správního deliktu, za který může být pokutována do výše 500 000 Kč.

Aby SBS problému mlčenlivosti zaměstnanců předešly, musí vybírat spolehlivé a loajální zaměstnance. Je vhodné prověřit minulost těchto zaměstnanců, především problémy v jejich minulých zaměstnáních, a to z toho důvodu, že mnoho firem řeší tyto problémy interně, aby si před veřejností nepoškodily své dobré jméno.

SBS by své zaměstnance měla také pravidelně prověřovat a zjišťovat, jestli tito zaměstnanci nemají finanční problémy, kvůli kterým by mohli prodávat neoprávněným osobám informace, a také jestli nemají kontakty s osobami, které provozují nezákonnou činnost, nebo s firmami, které by mohly mít o dané utajované informace zájem a které by se mohly

snažit zaměstnance podplatit, aby jim k těmto informacím umožnili přístup, resp. jim utajované informace vyzradili.

S loajalitou zaměstnanců pak souvisí i jejich finanční ohodnocení. Jejich mzda by měla být adekvátní vykonávané práci a zároveň dostatečně vysoká, aby je nelákalo vyzrazení utajovaných informací neoprávněným osobám, resp. poskytnutí informací o zabezpečení objektu, ve kterém se nacházejí utajované informace, neoprávněným osobám. Možností je také stanovit prémie pro spolehlivé a loajální zaměstnance.

5.2 Návrh řešení problému namátkových prohlídek

Namátkové prohlídky slouží ke zjišťování, zda do objektu nebo zabezpečené oblasti osoby nevnášejí nežádoucí zařízení apod., resp. jestli z objektu nebo zabezpečené oblasti osoby něco nevynášejí. Tyto prohlídky mají především odstrašující efekt.

Při provádění osobních prohlídek se zaměstnanci SBS musí řídit trestním řádem, který říká, že osobní prohlídku smí provádět pouze osoba stejného pohlaví. Během prohlídek pak nesmí být narušena lidská důstojnost.

Aby SBS plnily standardy NBÚ a zároveň požadavky trestního řádu na provádění osobní prohlídky, je vhodné u ostrahy, která osobní prohlídky provádí, zaměstnat i ženy. Variantou také je dohodnout se se zaměstnankyněmi, které vykonávají jinou činnost než ostrahu, že v případě potřeby budou provádět osobní prohlídku. V takovém případě je třeba tyto zaměstnankyně proškolit o tom, jak osobní prohlídku provádět, a také je k provádění osobní prohlídky zplnomocnit.

5.3 Návrh řešení problému se zaměstnanci umisťujícími v objektu odposlechová a nahrávací zařízení

Pro objekty a zabezpečené oblasti kategorií nižších než Přísně tajné a pro objekty, ve kterých nejsou jednací oblasti pro projednávání utajované informace stupňů utajení Přísně tajné nebo Tajné, nejsou stanoveny požadavky na použití detektorů kovových předmětů, rentgenových přístrojů ani technických prostředků proti pasivnímu a aktivnímu odposlechu. SBS, které v takovýchto objektech nebo zabezpečených oblastech tato zařízení nepoužívají, čelí problému se zaměstnanci, kteří v objektu nezákonně umisťují odposlechová nebo

nahrávací zařízení a získané odposlechy utajovaných informací prodávají neoprávněným osobám.

Stejně jako u problému mlčenlivosti zaměstnanců, je vhodné, aby SBS problému zaměstnanců, kteří umisťují v objektu odposlechová a nahrávací zařízení, předcházely výběrem spolehlivých a loajálních zaměstnanců. Je také vhodné zaměstnance pravidelně prověřovat a stanovit jim adekvátní mzdu.

Problém je možné řešit také technicky, a to použitím detektorů kovových předmětů a rentgenových přístrojů pro kontrolu zavazadel. Toto řešení je možné doplnit prováděním osobních prohlídek, protože dnes existují odposlechová a nahrávací zařízení, která nemusí detektor kovových předmětů odhalit. Méně vhodnou variantou je řešit problém pouze prováděním osobních prohlídek, a to z toho důvodu, že moderní odposlechová zařízení mohou dosahovat velmi malých rozměrů nebo mohou být maskována jako propiska, flash disk apod.

5.4 Návrh řešení problémů s nezodpovědnými uživateli informačních systémů

V oblasti bezpečnosti informačních systémů čelí SBS nejčastěji problémům s nezodpovědnými uživateli těchto systémů, kteří nedodržují stanovená pravidla. Mezi tyto problémy patří problém s uživateli, kteří nedodržují pravidla týkající se přístupového hesla, problém s uživateli, kteří si heslo nepamatují a nezodpovědně si ho někam zapisují a také problém s uživateli, kteří nechávají počítač s přístupem k utajovaným informacím zapnutý bez dozoru.

Nezodpovědní uživatelé informačních systémů, kteří nedodržují stanovená pravidla pro vytváření hesel, neoprávněné osobě usnadňují prolomení hesla a tím i přístup do systému. Řešením je instalovat do informačního systému software, který uživateli nedovolí používat kratší hesla než je stanovená minimální délka těchto hesel, který nedovolí uživateli použití jednoduchých slovníkových hesel a který po uplynutí stanoveného časového intervalu vynutí změnu hesla.

Špatně odhalitelný je problém s uživateli, kteří si heslo někam zapisují, protože si ho nedokáží zapamatovat. Ztráta zapsaného hesla je nebezpečná a může vést k napadení informačního systému neoprávněnou osobou. Tento problém a stejně tak problém

s uživateli, kteří nedodržují stanovená pravidla pro vytváření hesel, lze vyřešit tím, že místo přístupového hesla se bude k autentizaci a identifikaci uživatele používat kombinace USB tokenu a biometrického prvku jako je např. otisk prstu.

Problém s nezodpovědnými uživateli informačních systémů, kteří nechávají počítač s přístupem k utajovaným informacím zapnutý a usnadňují tak přístup k utajovaným informacím neoprávněným osobám, lze řešit také použitím kombinace USB tokenu a biometrického prvku. A to tak, že když uživatel odchází, stačí mu odpojit USB token od počítače, čímž dojde k odhlášení tohoto uživatele.

Místo výše zmíněných USB tokenů lze použít čipové karty tzv. smart card. K tomu je třeba, aby počítač disponoval čtečkou těchto karet. Výhodou těchto karet pak je, že mohou mít i RFID čip a díky tomu mohou být používány také jako přístupové karty v systémech kontroly vstupu apod.

ZÁVĚR

Cílem mé bakalářské práce bylo popsat problematiku ochrany utajovaných informací a bezpečnostní způsobilosti v ČR, stručně vymezit vývoj a činnost soukromých bezpečnostních služeb, popsat hlavní úkoly, oprávnění a strukturu Národního bezpečnostního úřadu a nakonec analyzovat problémy, kterým čelí soukromé bezpečnostní služby při plnění standardů NBÚ, a navrhnout možná řešení těchto problémů.

Teoretická část práce, především problematika ochrany utajovaných informací a bezpečnostní způsobilosti, byla pojata jako studijní materiál pro každého, kdo se chce seznámit se základy ochrany utajovaných informací. A to proto, že většina existujících skript, studijních materiálů i dostupné literatury pojednává o této problematice podle zákona č. 148/1998 Sb., který dnes již neplatí.

Praktická část práce se zabývala analýzou problémů, kterým soukromé bezpečnostní služby čelí při plnění standardů Národního bezpečnostního úřadu. Informace o těchto problémech je těžké získat, protože každá SBS si je chrání, aby neunikly na veřejnost. Z toho důvodu nejsou uvedeny všechny existující problémy, ale pouze ty, o kterých se při rešerši k této problematice, podařilo získat alespoň základní informace.

V poslední kapitole byly shrnuty jednotlivé analyzované problémy, kterým SBS čelí při plnění standardů NBÚ. Pro každý problém je pak navržena jedna nebo více variant možných řešení, které lze uplatnit v bezpečnostní praxi.

SEZNAM POUŽITÉ LITERATURY

Monografické publikace:

[1] BRABEC, František. *Bezpečnost pro firmu, úřad, občana*. 1.vyd. Praha: Public History, 2001, 400 s. ISBN 80-864-4504-6.

[2] BRABEC, František. *Technologie detektivních činností*. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2009, 160 s. ISBN 978-80-7318-780-4.

[3] IVANKA, Ján. *Systemizace bezpečnostního průmyslu II*. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2009, 86 s. ISBN 978-80-7318-863-4.

[4] KAMENÍK, Jiří a František BRABEC. *Komerční bezpečnost: soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostních agentur*. Vyd. 1. Praha: ASPI, 2007, 338 s. ISBN 978-807-3573-096.

[5] KOLEKTIV, Luděk Lukáš a. *Bezpečnostní technologie, systémy a management I*. 1. vyd. Zlín: VeRBuM, 2011. ISBN 978-808-7500-057.

[6] LAUCKÝ, Vladimír. *Technologie komerční bezpečnosti II*. Vyd. 2. Zlín: Univerzita Tomáše Bati ve Zlíně, 2007, 123 s. ISBN 978-80-7318-631-9.

[7] MACEK, Pavel. *Bezpečnostní služby*. Vyd. 1. Praha: Police History, 2001, 196 s. ISBN 80-864-7703-7.

[8] MACEK, Pavel a František NOVÁK. *Privátní bezpečnostní služby*. Vyd. 1. Praha: Police History, 2005, 316 s. ISBN 80-864-7723-1.

Internetové zdroje:

[9] Hlavní úkoly. *Národní bezpečnostní úřad* [online]. [cit. 2014-04-11]. Dostupné z: http://www.nbu.cz/cs/o-nas/hlavni-ukoly-nbu/

[10] KYNCL, Jaromír. Z historie SBS: Legislativa bezpečnostních služeb. In: *ABAS Report* [online]. [cit. 2014-03-15]. Dostupné z: http://www.abasreport.cz/casopisy/2012-10-19-12-33-41/z-historie-sbs

[11] *Národní bezpečnostní úřad* [online]. [cit. 2014-04-11]. Dostupné z: http://www.nbu.cz/cs/

[12] O nás. *Národní bezpečnostní úřad* [online]. [cit. 2014-04-11]. Dostupné z: http://www.nbu.cz/cs/o-nas/o-nas/

[13] Organizační struktura a hlavní úkoly organizačních celků. *Národní bezpečnostní úřad* [online]. [cit. 2014-04-11]. Dostupné z: http://www.nbu.cz/cs/o-nas/organizacni-struktura/

Zákonné normy:

[14] Vyhláška č. 363/2011 Sb., o personální bezpečnosti a o bezpečnostní způsobilosti, ve znění vyhlášky č. 415/2013 Sb.

[15] Vyhláška č. 405/2011 Sb., o průmyslové bezpečnosti, ve znění vyhlášky č. 416/2013 Sb.

[16] Vyhláška č. 432/2011 Sb., o zajištění kryptografické ochrany utajovaných informací, ve znění vyhlášky č. 417/2013 Sb.

[17] Vyhláška 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 vyhlášky č. 453/2011 Sb.

[18] Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008 Sb. a vyhlášky č. 454/2011 Sb.

[19] Vyhláška č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací, ve znění vyhlášky č. 55/2008 Sb. a vyhlášky č. 433/2011 Sb.

[20] Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

[21] Zákon č. 413/2005 Sb., o změně zákonů v souvislosti s přijetím zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ČR	Česká republika.
EPS	Elektrická požární signalizace.
EU	Evropská unie.
NATO	Severoatlantická aliance (The North Atlantic Treaty Organization).
NBÚ	Národní bezpečnostní úřad.
PKB	Evropská unie.
PZTS	Poplachové zabezpečovací a tísňové systémy.
RFID	Identifikace pomocí rádiové frekvence (Radio Frequency Identification).
SBS	Soukromé bezpečnostní služby.
USB	Univerzální sériová sběrnice (Universal Serial Bus).

SEZNAM OBRÁZKŮ

SEZNAM TABULEK