Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra práva

Diplomová práce

Aktuální problémy režimu utajovaných skutečností

Autor: Bc. Petr Šebek

Vedoucí práce: JUDr. Viktor Jansa, CSc.

Česká zemědělská univerzita v Praze | Provozně ekonomická fakulta

Katedra práva | Akademický rok 2008/2009

ZADÁNÍ DIPLOMOVÉ PRÁCE

Petr Šebek

obor Veřejná správa a regionální rozvoj - k.s. Litoměřice

Vedoucí katedry Vám ve smyslu Studijního a zkušebního řádu ČZU v Praze čl. 17 odst. 2 určuje tuto diplomovou práci.

Název tématu: **Aktuální problémy režimu utajovaných skutečností**

Struktura diplomové práce:

1. Úvod
2. Cíl práce a metodika
3. Význam a smysl utajovaných skutečností
4. Režim utajovaných skutečností v ČR výhradně v působnosti NBÚ
5. Bezpečnostní prověrky , jejich udělování
6. Praktické problémy režimu utajovaných informací v ČR
7. Závěr
8. Seznam literatury
9. Přílohy

Rozsah původní zprávy: 50 - 60 stran

Seznam odborné literatury:

MUSIL, Rudolf. Ochrana utajovaných skutečností. Praha: Eurounion, s.r.o. , 2001

Zákon 412/2005 Sb. , ze dne 21.září 2005 o ochraně utajovaných informací a o bezpečnostní způsobilosti

Zákon 153/1994 Sb., o zpravodajských službách České republiky

Zákon 148/1998 Sb., ze dne 11. června 1998 o ochraně utajovaných skutečností a o změně některých zákonů

Zákon 246/1998 Sb., Seznam utajovaných skutečností
Další literatura po dohodě s vedoucím DP

Vedoucí diplomové práce: **JUDr. Viktor Jansa, CSc.**

Termín odevzdání diplomové práce: duben 2010

L.S.

.....
Vedoucí katedry

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE - Provozně ekonomická fakulta

.....
Děkan

V Praze dne: 15.12.2008

Evidováno děkanátem PEF pod č.j.: KPr-112-09D

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Aktuální problémy režimu utajovaných skutečností" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 8.dubna 2009 _____

Poděkování

Rád bych touto cestou poděkoval panu JUDr. Viktoru Jansovi, CSc. za jeho čas, trpělivost, odborné vedení a dobré rady při zpracování této práce.

Aktuální problémy režimu utajovaných skutečností

Current problems in the classified information

Souhrn

Diplomová práce Aktuální problémy režimu utajovaných skutečností se zaměřuje na identifikaci a definici problémů právní upravy v této oblasti. Popisuje a navrhuje řešení těchto problémů. Zároveň popisuje tendence ve vyvoji právní úpravy režimu utajovaných informací. Zvláštní pozornost je věnována otázce bezpečnostního řízení a praktickým problémům v režimu utajovaných informací.

Klíčová slova: normy, problémy, utajované informace, bezpečnost, bezpečnostní politika, právní systém, informační systém, právní úprava

Summary

Diploma thesis under the current problems of classified information focuses on the identification and definition of legal difficulties in this area. It describes and proposes solutions to these problems. It also describes trends in the regulatory regime of classified information. Particular attention is paid to the issue of safety procedures and practical problems under the classified information.

Keywords: standards, challenges, classified information, security, security policy, legal system, information system, legislation

OBSAH

1 ÚVOD

Po celou historii lidstva představovaly a představují získáné informace, přístup k nim a využití moc.

Informace obsahujícící zájmové či "citlivé" údaje nebo-li chráněný zájem je zcela běžným jevem a liší se pouze tím, pro koho je její ochrana podstatná, ať jde o jednotlivce, profesní či zájmovou skupinu nebo stát.

Nejen bezpečnostní aspekt a ochranou funkci státu má institut režimu utajovaných informací. Je zde i velký ekonomický dopad na veřejné statky. Nemalé částky na ochranu utajovaných skutečností jsou odčerpávány ze státního rozpočtu.

V poslední době se v podmínkách České republiky začíná postupně prosazovat názor, kdy se řešení bezpečností problematiky v organizacích nestává jen nenávratnou nákladovou položkou, která pouze zvyšuje náklady organizací, ale její přínos nad těmito náklady převažuje. V prvopočátku se jednalo většinou jen o velké organizace, ale s postupem času a získáváním zahraničních zkušeností, organizací, které to se svou bezpečností a tedy i ochranou svých oprávněnch zájmů myslí vážně, přibývá. Tento trend má dnes již zcela vzestupnou tendenci a pro právnické subjekty je to cesta k hledání mezi bezpečností a ziskem.

Právní systém v České republice vymezuje řadu oblastí či okruhů informací, které jsou chráněny nebo lépe řečeno je omezen přístup a manipulace s těmito údaji, včetně stanovení povinnosti zachovávat mlčenlivost o těchto informacích, ať již formou zákonem stanovené povinnosti či zákonem uznané povinnosti, např. zpovědní tajemství. V oblasti ochrany práv jednotlivce je to např. ochrana osobních údajů, listovní a lékařské tajemství. V oblasti zájmu veřejném pak je to např. obchodní tajemství, povinnost mlčenlivosti v oblasti bankovnictví, finanční a daňové sféry, povinnost mlčenlivosti stanovená zákoníkem práce). Všechny tyto úpravy mají jediný cíl, a to

zajistit, aby informace, s nimiž je pracováno nepřišly do rukou neoprávněné osoby a nedošlo k jejich zneužití.

Je zcela samozřejmé, že tuto nutnost ochrany vyvolávaly a vyvolávají informace, které obsahují údaje, jenž mohou mít vliv na zájmy státu a proto bylo třeba vytvořit systém ochrany těchto informací. Jedná se o skupinu informací, které je třeba chránit, tedy utajovat a to v zájmu České republiky.

Oblast ochrany utajovaných informací, dříve "utajovaných skutečností", v době předlistopadové pak ochrana "státního tajemství", zaznamenala zejména v posledním desetiletí v České republice zásadní změny a lze bez nadsázky hovořit o mimořádném vývoji v dané oblasti. Tento stav vychází zejména z rozvoje informačních a komunikačních technologií, zvláště přenosu informací a možností technického zpracování informací včetně jejich uchování.

Vznik první polistopadové právní úpravy oblasti ochrany utajovaných informací byl poměrně problematický, což bylo dáno předchozím historickým vývojem, politickou situací a přístupem veřejnosti. Tento stav vedl k tomu, že k přijetí zákonné normy došlo až v r. 1998, a to jen díky tomu, že existence systému ochrany utajovaných skutečností byla jednou ze základních podmínek pro vstup České republiky do Organizace Severoatlantické smlouvy. Následná praxe, získané zkušenosti a zejména citovaný vývoj v oblasti informačních a komunikačních technologií vedly ke vzniku nové právní úpravy, tedy zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti a o změně některých zákonů ve znění pozdějších předpisů (dále jen z.č. 412/2005 Sb.).

Novou právní úpravou se podařilo odstranit některé zásadní nedostatky a problémy předchozí praxe, avšak řada přetrvala i do současnosti, což dokládá i skutečnost, že zákon byl již sedmkrát novelizován a v současné době je připravena tzv. "velká novela". Současně přinesla nové pojmy a zavedla instituty dosud v problematice neužívané. Místo utajovaných skutečností se zde objevuje lépe

vymezený pojem utajované informace a s různými úpravami převzatý komplex úzce propojených subsystémů ochrany utajovaných informací, jmenovitě personální a průmyslová bezpečnost, administrativní bezpečnost, fyzická bezpečnost, bezpečnost komunikačních a informačních systémů a kryptografická ochrana, které ve svém souhrnu mají zajistit požadované standardy ochrany.

2 CÍL PRÁCE A METODIKA

2.1 CÍL PRÁCE

Tato práce si klade za cíl analýzu stavu v oblasti ochrany utajovaných informací po přijetí nové právní úpravy a na základě rozboru právního vymezení a aplikace v praxi poukázat na problémy v oblasti ochrany utajovaných informací, s částečným zaměřením na problematiku zpravodajských služeb s nastíněním možných variant řešení.

Při studiu problematiky a sběru pramenů a literatury v tomto oboru se poměrně často naráží na dva problémy. V prvé řadě se v českém prostředí jedná o oblast poměrně novou, která není v odborné literatuře ještě příliš zpracována. Řada sporných bodů čeká na svá řešení. Poměrně podrobně byla zpracována ochrana utajovaných skutečností v práci Rudolfa Musila[1], avšak současný stav zatím v literatuře popsán nebyl. Zahraniční literatura k problematice ochrany informací, rizik jejich stanovení a prevenci je velmi obsáhlá, avšak nepostihuje oblast, která je předmětem této práce. Obdobně neexistuje komentář k zákonu, který by podal komparativní výklad a umožnil odborné i laické veřejnosti správné chápání dané věci.

2.2 METODIKA

Metodika této práce spočívá v popisu a analýze. Pro práci byla použita výzkumná metoda studia dokumentů dále pak neřízené rozhovory s oprávněnými osobami a podložené informace z vlastní praxe. Pod pojmem dokument si lze představit psané a tištěné materiály (noviny, knihy, dopisy, zápisky, deníky atd.), ale mohou to být i fotografie, filmy, obrazy, sochy a jiné materiální výtvory člověka.[2]

[1] R. Musil – Ochrana utajovaných skutečností, Praha 2001
[2] MAJEROVÁ, V. a MAJER, M. Empirický výzkum v sociologii venkova a zemědělství, část II.

Pro účel práce byla shromážděna dostupna odborna literatura. Bylo čerpáno z vlastních zdrojů, fondů Městské knihovny v Praze a z ověřených pramenů v Internetu. Získané informace byly doplněny znalostmi a zkušenostmi získanými dlouholetou praxí v oboru. Kompletní souhrn pramenů je sumarizován v seznamu použité literatury v závěru práce.

Při zpracování vybraného téma byla věnována pozornost především právním předpisům, a to jak předchozí právní úpravě, tedy z.č. 148/1998 Sb. a prováděcím předpisům, tak zejména novému zákonu č. 412/2005 Sb. a prováděcím předpisům. Cenným vodítkem pro pochopení některých změn byly texty důvodových zpráv k zákonům a jejich kritické rozbory či komentáře publikované v médiích ze strany politických představitelů, nevládních organizací atp. Tato část literatury a pramenů představuje další problém, kterým je poměrně silná obava z neúměrného zasahování státu do lidských práv a svobod, zejména práva na přístup k informaci. Na základě znalosti studovaného problému je třeba konstatovat, že koncept ochrany utajovaných informací jde do určité míry proti konceptu přirozeného a obecného šíření informací, tak jak je chápán v systému lidských práv a svobod, byť za účelem ochrany "obecných zájmů". Je však otázkou kvality legislativy a jejího následného užití v běžném životě zda je schopna nastavit oboustranně funkční systém. Nový zákon přinesl bezesporu zprůhlednění řady postupů a větší právní jistotu pro osoby, které se v oblasti ochrany utajovaných informací pohybují nebo se s ní střetávají a přes veškeré výhrady představuje v ochraně utajovaných informací pozitivní posun v dalším rozvoji.

Pro účely porovnání užívaných postupů a pojmů byly jako cenný zdroj pro tuto práci využity právní předpisy z oblasti ochrany utajovaných informací zejména Organizace severoatlantické smlouvy, Evropské unie a partnerských států.

K posouzení odlišností a problémů zpravodajských služeb ve vztahu k oblasti ochrany utajovaných informací mi byly cenným zdrojem především zákony vymezující

působnost a činnost jednotlivých služeb, a dále zejména informace z webových stránek různých zpravodajských a bezpečnostních služeb.

Pro posouzení skutečného stavu byly využity především statistické údaje publikované Národním bezpečnostním úřadem a jejich vzájemné porovnání.

3 VÝZNAM A SMYSL UTAJOVANÝCH SKUTEČNOSTÍ

Již v dávné historii lze zaznamenat fenomén "utajování informace", neboť člověk si velmi záhy uvědomil, že znalost určité informace mu přináší výhodu, ta pak zvyšuje jeho možnosti a může mu pomoci zístakt lepší pozici, posílení vlivu a moci. Na straně druhé pak začal chránit informace, které by jej mohly, v případě vyzrazení, poškodit. S postupným vývojem společnosti, státu a práva se začal institut utajení či státního tajemství provázaný s trestnými činy velezrady a vyzvědačství, objevovat v právních systémech. Primárně se jednalo o státní tajemství v oblasti vojenství a obrany státu, pak následovala oblast diplomacie a vnitřní bezpečnosti. Míra a způsob ochrany byly v přímé závislosti na "hodnotě" chráněné informace a do doby před objevem technologií, zařízení a přístrojů umožňujících přenos informací jiným způsobem, než byly pergamen a papír, nepředstavovala ochrana utajovaných informací zásadní problém.

Technický pokrok, představovaný zejména novými informačními a komunikačními technologiemi přinesl a stále přináší obrovské možnosti pro vznik, zpracování, přenos a uchování informací. Tento vývoj však ve svém dopadu klade stále náročnější podmínky na ochranu informací, a to ve všech jejích oblastech.

Dnešní chápání významu utajovaných informací a systému ochrany v České republice vzešlo z pojetí utajovaných informací Organizace Severoatlantické smlouvy a jejich systému ochrany, který je vymezen v předpisu NATO Security Policy C-M (2002) 49 ze dne 17. 6. 2002. Norma se skládá ze 7 částí – A- Bezpečnostní dohoda, B - Základní principy a minimální standardy bezpečnosti, C- Personální bezpečnost, D - Fyzická bezpečnost, E - Bezpečnost informací (administrativní bezpečnost), F - INFOSEC (bezpečnost informačních systémů) , G – Průmyslová bezpečnost.

Tyto předpisy stanoví minimální obecné standardy pro jednotlivé oblasti ochrany utajovaných informací, které musí splňovat národní právní úpravy a praxe v oblasti ochrany utajovaných informací jednotlivých členských zemí. Splnění těchto standardů

je základní podmínkou pro zapojení dané země do výměny utajovaných informací Organizace Severoatlantické smlouvy a jejich dodržování je předmětem pravidelných kontrol v jednotlivých členských zemích. Za oblast ochrany utajovaných informací odpovídá NATO Office of Security (Bezpečnostní úřad NATO).

Vstupem České republiky do Evropské unie byly, pro účely výměny utajovaných informací v rámci tohoto společenství, přijaty směrnice EU v oblasti ochrany utajovaných informací. Jedná se o dva předpisy, a to ROZHODNUTÍ RADY ze dne 19. března 2001, kterým se přijímají bezpečnostní předpisy Rady ve znění pozdějších novelizací (2001/264/ES) a ROZHODNUTÍ KOMISE ze dne 29. listopadu 2001, kterým se mění její jednací řád *(oznámeno pod číslem K(2001) 3031)* (2001/844/ES, ESUO, Euratom) a jeho další novelizace, které je poměrně obsáhlým předpisem, jenž stanoví obecné zásady v oblasti ochrany utajovaných informací.[3]

Systém ochrany utajovaných informací EU je kordinován Bezpečnostním výborem Rady a Bezpečnostní kancelář generálního sekretariátu Rady zajišťuje, řídí a kontroluje opatření v oblasti ochrany utajovaných informací EU. Vedoucí bezpečnostní kanceláře GSR řídí aktualizaci bezpečnostních předpisů a koordinuje bezpečnostní opatření s příslušnými orgány členských států.

V podstatě lze konstatovat, že předpisy Organizace Severoatlantické smlouvy a Evropské unie v oblasti ochrany utajovaných informací nevykazují žádné zásadní disproporce. Obě oblasti předpisů stanoví minimální obecné zásady práce a ochrany utajovaných informací pro členské státy za účelem zajištění jednotných postupů v oblasti ochrany utajovaných informací.

Přijetím České republiky jako členského státu do výše zmíněných mezinárodních organizací se význam oblasti utajovaných informací a jejich ochrany v naší zemí dostal kvalitativně na zcela odlišnou a vyšší úroveň.

[3]www.nbu.cz - právní předpisy – předpisy EU v oblasti ochrany utajovaných informací

3.1 STRUČNÝ HISTORICKÝ VÝVOJ PRÁVNÍ ÚPRAVY UTAJOVANÝCH INFORMACÍ V ČESKÉ REPUBLICE

První českou právní kodifikaci v současné době užívaného pojmu utajované informace, je možno nalézt v podobě "státního tajemství" v zákoně č. 50/1923 Sb., na ochranu republiky. Zákon měl za úkol postihnout činnosti, které závažným způsobem mohly ohrozit Československou republiku. Mezi tyto bylo zařazeno i ohrožení státního tajemství.

Pojem státního tajemství byl definován poměrně široce, jako "skutečnost, opatření nebo předmět, jež vláda tají v takovém zájmu, mají zůstati utajeny před cizí mocí".[4] Bližšího vymezení se pak dostalo ještě státnímu tajemství v oblasti vojenství. Zákon rozlišuje zradu státního tajemství, vojenskou zradu,[5] nedovolené zpravodajství [6] a ohrožování obrany republiky.[7] Tato norma odděluje ve všech uvedených trestných činech úmysl a nedbalost.

Citovaný zákon představoval poměrně silný zásah do demokratických práv občanů nově vzniklé republiky, a to zejména v oblasti svobody projevu a svobody tisku. Zákon byl v letech 1933, 1934, 1935, 1939 a 1945 novelizován.

Nahrazen byl zákonem ze 6. října 1948 na ochranu lidově demokratické republiky, který byl vydán pod č. 231/1948 Sb. Do této normy se plně projevily politické změny po únorovém převratu v roce 1948. Jedná se o právní normu, která "legalizovala "represivní opatření proti jakémukoli projevu demokratické opozice. Zákon používá termín "státní tajemství", a to v souvislosti s ustanovením o vyzvědačství.[8] Současně se zde objevuje nedbalé uchování státního tajemství[9] jako

[4] § 5 z.č. 50/1923 Sb., na ochranu republiky
[5] § 6 z.č. 50/1923 Sb., na ochranu republiky
[6] § 23 z.č. 50/1923 Sb., na ochranu republiky
[7] § 24 z.č. 50/1923 Sb., na ochranu republiky
[8] § 5 z.č.231/1948 Sb., na ochranu lidově demokratické republiky
[9] § 7 z.č. 231/1948 Sb., na ochranu lidově demokratické republiky

trestný čin a trestný čin ohrožení republiky, který měl spočívat ve vyzvídání "státního tajemství v úmyslu vyzraditi jej nepovolané osobě".[10] Pokud jde o oblast obrany státu objevuje se zde v ustanovení § 12 trestný čin nedovoleného zpravodajství, které se vztahovalo ke zveřejnění údajů o jakémkoli subjektu důležitém pro obranu republiky nebo jejího spojence za podmínky, že mohl vědět, že uveřejněním ohrožuje zájmy státu.

Další kodifikaci se oblasti státního tajemství v trestním právu dostalo s přijetím trestního zákona ze dne 29. listopadu 1961 (vydán z.č. 140/1961 Sb.) , v § 89 odst. 11 je definováno státní tajemství jako "vše co v důležitém zájmu republiky, zejména zájmu politickém, vojenském a hospodářském, má zůstat utajeno před nepovolanou osobou". Stejné ustanovení zákona obsahuje i vymezení pojmu hospodářského a služebního tajemství. V hlavě I. - trestné činy proti republice je pak obsahžena i oblast porušení ochrany státního tajemství, a to v oddílu 2., ustanovení § 105 vyzvědačství , § 106 ohrožení státního tajemství, § 107 nedbalostní vyzrazení státního tajemství a § 108, který je vztažen na vyzvědačství a ohrožení státního tajemství ke škodě státu světové socialistické soustavy.

Vzhledem k absenci právní úpravy státního tajemství došlo v roce 1971 k přijetí zákona o ochraně státního tajemství (z.č. 102/1971 Sb. ze dne 8. října 1971). Státní tajemství je zde vymezeno § 2 zcela identicky jako v trestním zákonu. Vláda ČSSR stanovila základní skutečnosti tvořící předmět státního tajemství a ministr vnitra ČSSR vydával a doplňoval seznamy skutečností tvořících státní tajemství pro jednotlivé obory či odvětví.

Tuto právní normu pak, po listopadové změně režimu, nahradil zákon č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů, ve znění pozdějších předpisů. Následně došlo k úpravě ustanovení § 105 - 107 trestního zákona, tak aby odpovídaly novému chápání ochrany informací.

[10] § 8 z.č. 231/1948 Sb., na ochranu lidově demokratické republiky

V současné době se kromě z.č. 415/2009 Sb., oblast ochrany utajovaných informací, respektive porušení ochrany utajovaných informací, vyskytuje v novém trestním zákonu č. 40/2009 Sb., a to konkrétně v ustanovení § 316 – Vyzvědačství, § 317 – Ohrožení utajované informace a § 318 – Ohrožení utajované informace z nedbalosti.

Jak již bylo v úvodu této práce konstatováno, po celou historii lidstva představovaly a představují získání informace, přístup k nim a využití moc. K tomu abychom mohli skutečnost, a dnes již podle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, informaci považovat za utajovanou, je vhodné si vymezit, co opravdu takovouto skutečností je. Tedy definovat základní pojmy.

V textu této práce je použita řada pojmů z oblasti ochrany utajovaných informací a je proto vhodné vymezit a stručně charakterizovat některé z těchto užitých základních pojmů.

3.2 ZÁJEM ČESKÉ REPUBLIKY[11]

Je zachování ústavního pořádku, svrchovanosti a územní celistvosti, zajištění vnitřního pořádku a bezpečnosti, zajištění ochrany zájmů k nimž se Česká republika zavázala v rámci uzavřených mezinárodních dohod a smluv, ochrana zdraví a života osob a ochrana ekonomiky.

3.3 UTAJOVANÁ INFORMACE[12]

V předchozí právní úpravě "utajovaná skutečnost" dříve "státní tajemství". Jedná se o jakoukoli informaci, tedy v jakékoli podobě a zaznamenané na jakémkoli nosiči, která splňuje následující podmínky :

[11] § 2, 3 z.č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů
[12] § 2 zák.č.412/2005 Sb.

1. vyzrazení nebo zneužití této informace může způsobit újmu zájmu České republiky nebo může být pro zájem České republiky nevýhodné
2. informace musí být označena jako utajovaná v souladu se zákonem č. 412/2005 Sb.
3. informace musí být uvedena v seznamu utajovaných informací.

Je tedy zřejmé, že informace musí naplňovat všechny tři výše uvedené znaky současně, aby ji bylo možno označit za utajovanou informaci a v souladu s platnými předpisy s ní pak nakládat.

Pokud jde o první podmínku, tedy o možný dopad na zájmy České republiky v případě vyzrazení nebo zneužití informace, je tato současně kritériem pro stanovení vlastního stupně utajení, a to v přímé závislosti na míru škod, které neoprávněná manipulace s utajovanou informací může způsobit.

Zákon rozlišuje mimořádně vážnou újmu zájmů České republiky[13] a informace, jejichž vyzrazení či zneužití by mělo tento dopad, jsou klasifikovány stupněm Přísně tajné. Do této oblasti patří informace, jejíž zneužití může mít za následek bezprostřední ohrožení svrchovanosti, území celistvosti nebo demokratických základů České republiky, rozsáhlé ztráty na lidských životech nebo rozsáhlé ohrožení zdraví obyvatel, mimořádně vážné nebo dlouhodobé poškození ekonomiky České republiky, značné narušení vnitřního přádku a bezpečnosti, mimořádně vážné ohrožení významných bezpečnostních operací nebo činnosti zpravodajských služeb, mimořádně vážné ohrožení činnosti nebo existence Organizace Severoatlantické smlouvy, Evropské unie nebo členského státu, mimořádně vážné ohrožení bojeschopnosti ozbrojených sil České republiky, Organizace severoatlantické smlouvy nebo jejího členského státu nebo členského státu Evropské unie, nebo mimořádně vážné poškození diplomatických

[13] § 3 zák.č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů

nebo jiných vztahů České republiky k Organizaci Severoatlantické smlouvy, Evropské unii nebo členského státu.

Stupněm Tajné jsou klasifikovány informace, jejichž vyzrazení nebo zneužití má za následek vážnou újmu České republiky. Do této kategorie patří ohrožení svrchovanosti, územní celistvosti a demokratických základů České republiky, značné škody České republiky ve finanční, měnové nebo hospodářské oblasti, ztráty na lidských životech nebo ohrožení zdraví obyvatel, narušení vnitřního pořádku a bezpečnosti České republiky, vážné ohrožení bojeschopnosti ozbrojených sil České republiky, Organizace Severoatlantické smlouvy nebo jejího členského státu nebo členského státu Evropské unie, vážné ohrožení významných bezpečnostních operací nebo činnosti zpravodajských služeb, vážné ohrožení činnosti Organizace Severoatlantické smlouvy, Evropské unie nebo členského státu, vážné narušení diplomatických vztahů České republiky k Organizaci Severoatlantické smlouvy, Evropské unii nebo členskému státu nebo jinému státu nebo vážné zvýšení mezinárodního napětí.

Stupněm Důvěrné jsou klasifikovány informace, jejichž vyzrazení nebo zneužití má za následek prostou újmu zájmů České republiky, která vzniká jestliže dojde k neoprávněné manipulaci s utajovanou informací, s dopadem na zhoršení vztahů České republiky s cizí mocí, ohrožení bezpečnosti jednotlivce, ohrožení bojeschopnosti ozbrojených sil České republiky, Organizace Severoatlantické smlouvy nebo jejího členského státu nebo členského státu Evropské unie, ohrožení bezpečnostních operací nebo činnosti zpravodajských služeb, ohrožení činnosti či existence Evropské unie nebo jejího členského státu, zmaření, ztížení anebo ohrožení prověřování nebo vyšetřování zvlášť závažných trestných činů nebo usnadnění jejich páchání, vznik nezanedbatelné škody České republice nebo závazné narušení ekonomických zájmů České republiky.

Nejnižším stupněm utajení, tedy Vyhrazené, jsou označovány informace jejichž vyzrazení či zneužití je pro zájmy České republiky nevýhodné. Do této skupiny spadají informace, které v případě neoprávněného nakládání s nimi mají za následek narušení

činnosti ozbrojených sil České republiky, Organizace Severoatlantické smlouvy nebo Sjejího členského státu nebo členského státu Evropské unie, zmaření, ztížení a nebo ohrožení prověřování nebo vyšetřování ostatních trestných činů mimo zvlášť závažných trestných činů nebo usnadnění jejich páchání, poškození významných ekonomických zájmů České republiky nebo Evropské unie nebo jejího členského státu, narušení důležitých obchodních nebo politických jednání České republiky s cizí mocí nebo narušení bezpečnostních nebo zpravodajských operací.

Označením informace podle zákona se rozumí zejména vyznačení názvu původce informace, stupně utajení, evidenční označení a data zniku (viz. dále administrativní bezpečnost).

Třetím znakem utajované informace je její uvedení v seznamu utajovaných informací.[14] Jedná se o seznam, který zpracovává Národní bezpečnostní úřad a je vydáván vládou České republiky ve formě nařízení. Obsahuje obecnou přílohu a jednotlivé přílohy podle ministerstev, ústředních orgánů státní správy a dalších institucí.[15]

Tento třetí znak utajované informace byl poměrně velmi diskutovanou otázkou při tvorbě nové právní úpravy a původní předložený návrh jej vynechal. Podle úvahy zpracovatele návrhu zákona měly být seznamy utajovaných informací zrušeny jako nadbytečné. Předkladatel zákona, tedy Národní bezpečnostní úřad se chtěl přiklonit k praxi běžné v zemích Západní Evropy, které tyto seznamy nemají. V průběhu připomínkového řízení k zákonu však na žádost většiny rezortů byly seznamy utajovaných informací zařazeny zpět.[16]

Přístup k utajované informaci

[14] § 139 z.č.412/2005Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů

[15] Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací, ve znění nařízení vlády č. 240/2008 Sb.

[16] www.transparency.cz – projekty-realizované projekty-utajování informací-dokumenty

Respektive oprávněný přístup k utajované informaci nebo-li seznámení se s utajovanou informací je umožněn v případě naplnění dvou následujících podmínek :

- nezbytnost osoby seznámit se s utajovanou informací, tzn. osoba tuto informaci nezbytně potřebuje pro výkon funkce, pracovní či jinou činnost,
- osoba musí být **osobou "oprávněnou",** tzn. je držitelem osvědčení fyzické osoby pro přístup k utajované informaci odpovídajícího stupně (v případě utajované informace stupně Vyhrazené je držitelem oznámení o splnění podmínek pro přístup k utajované informaci stupně Vyhrazené) nebo je osobou, která disponuje zvláštním přístupem k utajované informaci[17] a současně je osobou "poučenou", tzn. byla proškolena a poučena o právech a povinnostech v oblasti ochrany utajovaných informací a o následcích jejich porušení.[18]

Zákon definuje osoby, které mají možnost zvláštního přístupu k utajované informaci, aniž by u nich došlo k provedení bezpečnostního řízení a vydání odpovídajícího osvědčení. Jedná se v prvé řadě o osoby, které vykonávají funkci – prezident republiky, poslanci a senátoři Parlamentu, členové vlády, Veřejný ochránce práv a zástupce Veřejného ochránce práv, soudci, prezident, viceprezident a členové Nejvyššího kontrolního úřadu. V tomto případě je přístup k utajovaným informacím umožněn po dobu výkonu funkce v rozsahu nezbytném pro její výkon. Další skupinu osob představují "lidské informační zdroje" využívané bezpečnostním a zpravodajským aparátem České republiky. Poslední skupinou osob jsou osoby, které tento přístup potřebují v rozsahu nezbytném pro uplatnění svých práv a plnění povinností v trestním řízení, občanském soudním řízení a soudním řízení správním. Zákon umožňuje ještě jednu možnost přístupu k utajované informaci bez splnění podmínky držení osvědčení fyzické osoby pro daný stupeň utajované informace. Jedná se o tzv. jednorázový přístup k utajované informaci, který byl převzat z předpisů Severoatlantické aliance a v přechozí právní úpravě neexistoval. V podstatě tento institut umožňuje osobě, která je držitelem platného osvědčení fyzické osoby pro přístup k utajované informaci stupně

[17] § 58, 59 z.č. 412/2005Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů
[18] § 2 písm. i) z.č. 412/2005 Sb.

Důvěrné, se po vydání souhlasu Národního bezpečnostního úřadu seznámit s utajovanou informací stupně Tajné.

Původce utajované informace[19]

Orgán státu, právnická osoba či podnikající fyzická osoba, u které konkrétní utajovaná informace byla vytvořena (v případě ochrany průmyslového vlastnictví – např. přihláška vynálezu, užitného vzoru je původcem Úřad průmyslového vlastnictví[20])

Odpovědná osoba[21]

(v předchozí právní úpravě "statutární orgán") je osoba, která je v obecné rovině odpovědná za dodržování povinností stanovených zákonem v daném subjektu. Zákon vymezuje okruh odpovědných osob v ustanovení § 2 písm. d), jedná se převážně o nejvyšší vedení, např. ministři, ředitelé zpravodajských služeb, guvernér České národní banky. Odpovědná osoba má ze zákona řadu povinností, mimo jiné zajistit poučení fyzických osob a jejich pravidelné proškolení, schválit informační systém do provozu, kontrolovat dodržování povinností stanovených zákonem.

Ochrana utajovaných informací

je systém, který zajišťuje aby k informacím, které jsou klasifikovány jako utajované byl umožněn kontrolovaný přístup pouze oprávněným osobám. Jedná se o systém tvořený šesti subsystémy, a to :

1. personální bezpečnost

   cílem tohoto subsystému ochrany utajovaných informací je zajistit, aby přístup k utajovaným informacím měly pouze osoby oprávněné, tedy ty osoby, které splňují podmínky stanovené zákonem pro přístup k utajované informaci, a to po celou dobu platnosti osvědčení fyzické osoby pro přístup k utajované informaci. Nedílnou součástí systému je i řádný výběr osob, které by měly mít přístup k utajované informaci, jejich výchova a ochrana.

[19] § 2 písm. f) z.č.412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů
[20] § 70 z.č. 412/2005 Sb.
[21] § 2, 67 z.č. 412/2005 Sb.

2. průmyslová bezpečnost

je oblastí, která v sobě zahrnuje opatření k zjištění a ověřování splnění podmínek pro přístup k utajované informaci podnikatele včetně zajištění řádného nakládání s utajovanou informací ze strany podnikatele.

3. fyzická bezpečnost

je souborem opatření, která mají zamezit nebo ztížit neoprávněné osobě přístup k utajované informaci, popřípadě přístup nebo pokus o tento přístup ze strany neoprávněné osoby zaznamenat.

4. administrativní bezpečnost

je systém opatření při tvorbě, zpracování, manipulaci včetně ukládání a skartace či archivace utajovaných informací.

5. ochrana informačních a komunikačních systémů

cílem tohoto subsystému ochrany utajovaných informací je zajištění důvěrnosti, integrity a dostupnosti utajované informace v informačních či komunikačních systémech včetně stanovení odpovědnosti správy a uživatelů při práci v těchto sytémech.

6. kryptografická ochrana

je systém opatření pro ochranu utajovaných informací za použití kryptografických metod a materiálů při procestu tvorby, manipulace či ukládání utajovaných informací.

Zpravodajské služby

pro účely této práce pojem zahrnuje české zpravodajské služby, a to Bezpečnostní informační službu, Úřad pro zahraničí styky a informace a Vojenské zpravodajství.

4 REŽIM UTAJOVANÝCH SKUTEČNOSTÍ V ČR VÝHRADNĚ V PŮSOBNOSTI NBÚ

V předlistopadovém Československu byl režim ochrany utajovaných informací upraven zákonem č. 102/1971 Sb., o ochraně státního tajemství. Tento zákon rozlišoval státní, hospodářské a služební tajemství, a za metodické řízení a výkon kontroly a dozoru odpovídalo Federální ministerstvo vnitra ČSSR. Osoby, které měly přístup ke státnímu tajemství byly vedeny Státní bezpečností ve zvláštní evidenci a vztahovala se na ně různá omezení a určitý systém kontroly.

Po revoluci v listopadu 1989 vyvstala záhy potřeba změny stávajícího systému, který neodpovídal aktuálním požadavkům a nárokům na ochranu utajovaných informací a nebyl akceptovatelný v rámci mezinárodní výměny utajovaných informací. Po poměrně dlouhé odborné debatě o vlastním konceptu systému ochrany utajovaných informací, tedy zda vytvořit samostatnou instituci nebo posílit kompetence jiné organizace o tuto oblast, kdy nejčastěji byla v této souvislosti zvažována varianta začlenění ochrany utajovaných informací do Bezpečnostní informační služby, byla nakonec přijata verze vytvoření samostatného ústředního orgánu státní správy, tj. Národního bezpečnostního úřadu (NBÚ).

Uvedený model zaštítění ochrany utajovaných informací formou samostatného správního orgánu státu byl přijat zákonem č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů, dne 2. července 1998 s účinností od 1. listopadu 1998. Na tomto právním základě byl vytvořen nový úřad a postupně uváděl v praxi zákon. Zde je třeba zdůraznit, že přes využití některých pojmů jako např. určení, seznamy utajovaných skutečností, které znal zákon č. 102/1971 Sb., se jednalo o zcela nové pojetí problematiky utajovaných informací, které reflektovalo jak demokratické a společenské změny v zemi, tak rozšiřování a využívání nových

technologií a technických vybavení, zejména výpočetní techniky a komunikačních zařízení pro přenos dat a informací.

NBÚ se stal jediným garantem ochrany utajovaných informací v České republice a z tohoto postavení pak vyplynula řada povinností, odpovědnosti a pravomocí.[22] Zákon č. 412/2005 Sb., pak přinesl v této oblasti řadu zpřesnění a doplnění, tak jak si je vyžádala praxe a zkušenosti z ní získané.

NBÚ je pověřen výkonem státní správy v oblasti ochrany utajovaných informací v celém souhrnu, s určitými výjimkami v oblasti ochrany utajovaných informací ve zpravodajských službách a velmi úzkém okruhu ochrany utajovaných informací u Ministerstva vnitra a Policie ČR. V čele NBÚ je ředitel , kterého jmenuje a odvolává, po projednání ve výboru pro věci bezpečnostní Poslanecké sněmovny, vláda ČR. Ředitel NBÚ je odpovědný předsedovi vlády nebo pověřenému členovi vlády.

NBÚ je iniciátorem a tvůrcem legislativních návrhů a změn v oblasti ochrany utajovaných informací a vykonává metodickou činnost, do které patří mj. poskytování odborných konzultací, výklad prováděcích předpisů a provádění různých typů školení podle potřeb ostatních orgánů státní a veřejné správy či jiných subjektů. Mimo metodické činnosti je odpovědný za provádění kontrolní činnosti v oblasti dodržování právních předpisů na úseku ochrany utajovaných informací. Jedná se o výkon tzv. "státního dozoru". Při této činnosti se NBÚ řídí jak předpisy z oblasti ochrany utajovaných informací, tak zákonem č. 552/1991 Sb., o státní kontrole, ve znění pozdějších předpisů. Pracovníci NBÚ, kteří kontrolu provádějí mají oprávnění přístupu k utajovaným informacím v rozsahu nezbytném pro řádný výkon kontroly.[23] V této oblasti se již prolíná otázka mezinárodní spolupráce na poli výměny utajovaných informací a zákon stanoví oprávnění účasti zahraničního subjektu na prováděné kontrole, pokud tento poskytl České republice utajovanou informaci. Právo účasti na kontrole ze strany úřadu cizí moci musí vyplývat z mezinárodní smlouvy. Nejčastější

[22] § 7-8 z.č.148/1998 Sb., §136-139 z.č. 412/2005 Sb.
[23] blíže kapitola Aktuální problémy ochrany utajovaných informací v ČR

praxí je účast na kontrole ze strany Bezpečnostního úřadu Organizace Severoatlantické smlouvy nebo Evropské unie. Česká republika, respektive pracovníci NBÚ se pak může reciprocně účastnit kontrol neboli výkonu státního dozoru v zahraničí. Státnímu dozoru nepodléhá činnost zpravodajských služeb a ve vybraných případech činnost ministerstva vnitra. Cílem státního dozoru je zjištění skutečného stavu věci a jeho porovnání s platnými předpisy za účelem ověření, že ochrana utajovaných informací je řádně a v plném rozsahu prováděna a dodržována. Zjištěné porušení ochrany utajovaných informací je pak podle závažnosti předmětem přestupkového řízení, které s daným subjektem, tedy fyzickou či právnickou osobou, vede NBÚ. Zákon č. 412/2005 Sb. přinesl v této oblasti zcela nové doplnění a poměrně široce definuje jednotlivé správní delikty na úseku ochrany utajovaných informací. Značně diskutabilní je však otázka sankcí, respektive výše finančních pokut, u některých přestupků, kde je možnost uložit u fyzické osoby či podnikatele pokutu až 5.000.000,- Kč. , což jsou částky, které se pohybují vysoce nad hranicí peněžitých trestů ukládaných za spáchaný trestný čin. Tato změna zákona byla vyvolána naprosto nedostatečným zpracováním problematiky porušení ochrany utajovaných informací a přestupků v zákoně č. 148/1998 Sb., kde např. byla definována řada povinností, avšak bez stanovení dopadu či sankce za porušení dané povinnosti.

Výkon státního dozoru představuje jednu z nejvýznamnějších činností NBÚ a mimo represivní úlohu má svou silnou preventivní stránku v oblasti ochrany utajovaných informací.

NBÚ je garantem za oblast ochrany utajovaných informací v souladu se závazky vyplývajícími z mezinárodní spolupráce a členství České republiky v Evropské unii a Organizaci Severoatlantické smlouvy. V praxi tato úloha znamená, že NBÚ se podílí na tvorbě mezinárodních dohod a smluv v oblasti výměny a ochrany utajovaných informací. Je vstupním místem pro utajované informace přicházející ze zahraničí, s dílčí výjimkou pro informační výměnu mezi zpravodajskými službami, a odpovídá tedy za jejich další distribuci a kontrolu řádného zacházení s nimi. Jak již bylo výše

zmíněno v této souvislosti se podílí na kontrolní činnosti dodržování ochrany utajovaných informací.

V současné době jsou uzavřeny smlouvy či dohody celkem s 21 státy, jejich rozsah a úroveň spolupráce je individuální od prosté výměny utajovaných informací přes uznávání bezpečnostních oprávnění. Jedná se o tyto země: Švédské království, Portugalská republika, Lotyšská republika, Litevská republika, Estonská republika, Spolková republika Německo, Francouzská republika, Italská republika, Ruská federace, Polská republika, Slovenská republika, Bulharská republika, stát Izrael, Spojené státy americké, Spojené království Velké Britanie a Severního Irska, Ukrajina, Finsko, Norsko, Makedonie, Slovinsko a Gruzie. Mimo těchto mezinárodních dohod a smluv jsou ještě uzavírány smlouvy cestou ministerstva obrany, vztahující se k oblasti ochrany utajovaných informací z vojenské problematiky. Do současné doby byly uzavřeny smlouvy s těmito státy – Jihoafrická republika, Norsko, Rumunsko, Švédsko, Spolková republika Německo.

Mimo činnost v oblasti legislativy v rámci mezinárodní výměny se NBÚ zaměřuje na další oblasti spolupráce, a to jak na možnost výměny zkušeností a odborné konzultace k jednotlivým systémům ochrany utajovaných informací, tak na poskytování různého druhu pomoci zemím, které jsou ve fázi přístupu ke členství v Evropské unii nebo Organizaci Severoatlantické smlouvy. Aktuálně je tato pomoc poskytována Srbsku, Makedonii a Chorvatsku.

V rámci mezinárodní spolupráce dále existuje součinnost při schvalování a vzájemném uznávání vydaných osvědčení. NBÚ je jediným oprávněným orgánem v České republice, který může uznat bezpečnostní oprávnění vydané cizí mocí pro účely seznamování se s utajovanými informacemi České republiky. Toto uznávání se děje na základě žádosti dané fyzické či právnické osoby. NBÚ v případě, že existuje mezinárodní dohoda o vzájemném uznávání bezpečnostního oprávnění, toto následně

uzná. V případech hodných zvláštního zřetele, kde neexistuje mezinárodní dohoda, lze ze strany NBÚ uznat bezpečnostní oprávnění, avšak toto musí být nezbytné a v souladu se zahraničními a bezpečnostními zájmy České republiky.

Samostatnou agendu tvoří povolování zahraničních návštěv, za kterou NBÚ odpovídá. Oblast zahraničních návštěv se řídí bezpečnostními předpisy Organizace Severoatlantické smlouvy a mezinárodními dohodami. Jedná se o umožnění přístupu určitého režimového zařízení na území ČR. Souhlas NBÚ vydává na základě žádosti, jejíž přílohou jsou odpovídající potvzení bezpečnostního úřadu cizí moci, který vydal bezpečnostní oprávnění osobám, jenž mají návštěvu uskutečnit. Tento mechanismus platí také opačným směrem, tedy že NBÚ vydá odpovídající potvrzení pro český subjekt, který žádá o návštěvu v zahraničí.

Poslední zmíněnou sférou mezinárodní spolupráce je možnost podílu na provádění bezpečnostních řízení či dožádání informací k fyzické osobě či podnikateli k němuž je prováděno řízení. Toto nové oprávnění NBÚ bylo vyvoláno potřebou možnosti samostatné komunikace s parterskými bezpečnostními úřady v zahraničí. Předchozí praxe tento postup neumožňovala a NBÚ byl nucen nadbytečně zatěžovat zpravodajské služby pro účely ověření běžného údaje v zahraničí. Současně byla tato praxe zavedena z důvodu uvolnění podmínky českého státního občanství u osoby žádající o vydání osvědčení, která byla stanovena v přechozí právní úpravě.

Oblast mezinárodní spolupráce představuje další z hlavních pilířů činnosti NBÚ a je mimořádně důležitá pro systém ochrany utajovaných informací.

Další z úkolů NBÚ je poměrně silně svázán s mezinárodní spoluprací a jedná se o vedení ústředního registru utajovaných informací[24] a schvalování zřízení registrů u orgánů státu a podnikatelů.

[24] § 79 z.č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů

Pod pojmem "ústřední registr" lze spatřovat systém evidence, odeslání či uložení utajovaných informací stupňů Důvěrné, Tajné a Přísně tajné, které jsou poskytovány v mezinárodním styku. Tuto agendu pro Českou republiku zajišťuje NBÚ, tedy evidenci, další distribuci uvnitř státu a v případě odesílání českých utajovaných informací odeslání zahraničnímu adresátovi. S tímto souvisí i povolování poskytování utajovaných informací do zahraničí ze strany NBÚ a oprávnění vydávat kurýrní listy k přepravě utajovaných informací v rámci mezinárodní informační výměny a v odůvodněných případech též zajištění přepravy utajovaných informací do zahraničí. Současně se zřízením registru a jeho vedením odpovídá NBÚ za schvalování registrů vytvořených u ostatních subjektů a jejich kontrolu.

NBÚ je také odpovědný za seznam utajovaných informací. Provádí jeho aktualizaci a případné opravy na základě vlastní iniciativy např. ze zkušenosti výkonu státního dozoru nebo reaguje na adekvátní podnět jiného subjektu, a to formou návrhu, který je předkládán ke schválení vládě ČR a vydán formou nařízení.

V oblasti kryptografické ochrany a ochrany informačních a komunikačních systémů je garantem za činnost Národního střediska komunikační bezpečnosti, Národního střediska pro distribuci kryptografického materiálu, Národního střediska pro měření kompromitujícího elektromagnetického vyzařování a Národního střediska pro bezpečnost informačních systémů. Všechna tato střediska jsou součástí NBÚ. V souvislosti s touto úlohou je NBÚ odpovědný za zajištění výzkumu, vývoje a výroby národních kryptografických prostředků. Vyvíjí a schvaluje národní šifrové algoritmy a vytváří národní politiku kryptografické ochrany. Zjišťuje kompromitující elektromagnetické vyzařování v místech, kde mají být uloženy nebo vytvářeny utajované informace, popř. v místech, která jsou již takto využívána. V návaznosti na uvedené činnosti NBÚ provádí certifikace informačních systémů, kryptografických prostředků a pracovišť, stínících komor a technických prostředků.

Pro potřeby jednotlivých subsystémů ochrany utajovaných informací vydává NBÚ bezpečnostní standardy, které jsou určeny zejména pro postup v daných oblastech na odborných pracovištích v jednotlivých rezortech.

Jednpou z posledních činností technického charakteru, které NBÚ zajišťuje je součinnost se zpravodajskými službami a policií při ověření podmínek a stavu jednacích oblastí, ve smyslu odhalení a zabránění umístění technických prostředků určených k neoprávněnému získání utajovaných informací a jejich úniku.

V oblasti rozhodovacích procesů ve vztahu k veřejnosti je NBÚ odpovědný za provádění řízení a vydání rozhodnutí I. a II. stupně ve věci žádosti fyzických osob a podnikatele o vydání osvědčení a o zrušení platnosti osvědčení (viz. blíže část bezpečnostní řízení). Dále provádí přestupkové řízení ve věci správních dekliktů a přestupků na úseku ochrany utajovaných informací.

Vydává Věstník Úřadu, v němž jsou zveřejňovány seznamy certifikovaných technických prostředků, seznam orgánů státu a podnikatelů, s nimiž byla uzavřena smlouva o zajištění činnosti,[25] a dále pak odborné informace k problematice ochrany utajovaných informací.

Všechny výše zmíněné působnosti NBÚ jako ústředního správního úřadu mají vazbu na oprávnění, která jsou v této souvislosti NBÚ dána zákonem.[26]

NBÚ je pro účely plnění úlohy garanta ochrany utajovaných informací v ČR oprávněn zpracovávat osobní údaje v rozsahu nezbytném pro potřeby plnění úkolů ze zákona a vést odpovídající spisovou agendu.

[25] § 52 z.č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů
[26] § 138 z.č. 412/2005 Sb.

Pro účely prováděných bezpečnostních řízení má oprávnění požadovat bezplatné poskytnutí informací od orgánů státu, právnických osob či podnikajících fyzických osob a tyto informace využívat a evidovat. Dále je oprávněn požadovat od policie a zpravodajských služeb informace získané podle jejich zákonů, zejména podle zákona č. 153/1994 Sb. NBÚ je oprávněn vyžadovat opis z evidence Rejstříku trestů a nahlížet do trestních spisů. Současně pro účely bezpečnostních řízení má NBÚ oprávnění spolupracovat s bezpečnostním úřadem cizí moci, zejména ve věci dožádání informací k účastníkovi řízení. NBÚ v nové právní úpravě získal nově oprávnění poskytnout v nezbytném rozsahu orgánu státu, právnické osobě nebo podnikající fyzické osobě potřebné osobní údaje vztahující se k vyžádané informaci. Všechna tato výše uvedená oprávnění byla proti z.č. 148/1998 Sb. v reakci na zkušenosti z praxe doplněna a přesněji formulována, tak aby umožnila zefektivnit průběh vlastního bezpečnostního řízení.

Z obecných oprávnění je třeba zmínit právo uchovávat v informačních systémech údaje získané v rámci plnění úkolů podle zákona a právo vést evidence a to osob a podnikatelů, kteří mají přístup k utajovaným informacím, bezpečnostních ředitelů, pracovníků kryptografické ochrany, kurýrů kryptografického materiálu, držitelů osvědčení o zvláštní odborné způsobilosti a porušení ochrany utajovaných informací.

V úvodu této kapitoly bylo zmíněno vyjmutí zpravodajských služeb a části agendy ministerstva vnitra z působnosti NBÚ na úseku ochrany utajovaných informací. K této výjimce je třeba v prvé řadě podotknout, že zákon a prováděcí předpisy jsou plně závazné pro všechny subjekty zainteresované do oblasti ochrany utajovaných informací, tedy i pro zpravodajské služby a ministerstvo vnitra. Výjimky, které byly v zákoně zpravodajským službám a ministerstvu vnitra uděleny, jsou poměrně úzké a mají své opodstatnění ve vlastní specifické pracovní náplni zpravodajských služeb a vybraném okruhu činností na ministerstvu vnitra. Zákon těmto složkám umožňuje samostatné

provádění bezpečnostních řízení a dává v tomto postavení ředitel NBÚ, jednotlivým ředitelům zpravodajských služeb a ministrovi vnitra (viz. blíže kapitola Bezpečnostní řízení), dále je vyjímá z kompetence výkonu státního dozoru a stanoví výjimku při poskytování utajovaných informací v rámci mezinárodní spolupráce zpravodajských služeb. Zpravodajské služby jsou však povinny vést odpovídající evidence, a v případě porušení povinností ochrany utajované informace Organizace Severoatlantické smlouvy nebo Evropské unie, musí tuto skutečnost hlásit NBÚ.

Zpravodajské služby a Ministerstvo vnitra plně podléhá NBÚ v oblasti systému certifikací technických prostředků, informačních systémů a kryptografických prostředků a pracovišť. V oblastech, kde mají tyto subjekty zákonem umožněnou výjimku, tedy zejména v personální bezpečnosti, je používána identická metodika a konzultovány postupy, tak aby se zamezilo možnosti jakýchkoli rozdílů, vzhledem k mechanismu vzájemné akceptace vydaných osvědčení pro přístup k utajovaným informacím.[27]

Všechny výše popsané kompetence NBÚ se určitým způsobem průřezově prolínají do jednotlivých oblastí ochrany utajovaných informací,které tvoří jednolitý celek.

4.1 NBÚ A ADMINISTRATIVNÍ BEZPEČNOST

Jak již bylo zmíněno, NBÚ je zřizovatelem a správcem ústředního registru a schvalovatelem ostatních dalších zřizovaných registrů. Ústřední registr se člení na centrální spisovny pro poskytování utajovaných dokumentů v mezinárodním styku mezi Českou republikou a Organizací Severoatlantické smlouvy, Českou republikou a Evropskou unií, Českou republikou a ostatními subjekty cizí moci. Centrální spisovny ústředního registru zastávají též funkci hlavního přijímacího a odbavovacího místa. Pro ukládání utajovaných informací poskytovaných v mezinárodním styku platí princip evidenčního i fyzického oddělení od ostatních utajovaných informací. Samostatně

[27] § 56a z.č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů

se tedy evidují a ukládají utajované informace Evropské unie, Organizace Severoatlantické smlouvy a ostatních subjektů cizí moci včetně samostatně vedených jednacích protokolů[28] podle stupňů utajení. Ústřední registr vede seznam všech registrů na území České republiky včetně jmenných seznamů jejich vedoucích a zástupců s podpisovými vzory.

Tato působnost je nedělitelnou součástí tzv. administrativní bezpečnosti, která v sobě zahrnuje stanovení postupů pro označování písemnosti, způsobu jejich evidence, manipulace a přepravy, ukládání, archivaci a skartaci utajovaných informací. Zákon tuto oblast vymezuje hlavou IV. Ustanovení § 21 - §23 a v řadě ustanovení odkazuje na prováděcí předpis, jmenovitě vyhlášku č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací. Prováděcí předpis podrobně stanoví postupy pro práci s utajovanou informací v celém jejím životním cyklu. Současně definuje základní administrativní pomůcky pro účely manipulace s utajovanými informacemi, přičemž dává i dostatečný prostor pro vlastní specifické postupy uvnitř jednotlivých subjektů. Vymezuje postavení a náplň ustředního registru a ostatních registrů utajovaných informací. Stanoví postupy pro nestadardní situace, např. zánik právnické osoby, orgánu státu, personální změny. Určuje postupy pro manipulaci s technickým zařízením. Vyhláška prošla doposud jedinou novelizací v roce 2008, která byla mimo jiné vyvolána obavami z nadměrného přísunu utajovaných informací stupně Vyhrazené v době předsednictví České republiky v Evropské unii a odlišností české národní úpravy ochrany této úrovně utajovaných informací v porovnání s praxí Evropské unie a Organizace Severoatlantické smlouvy. Tato disproporce, kdy národní úprava jde nad rámec společných standardů Evropské unie a Organizace Severoatlantické smlouvy, zde zůstala i po novelizací vyhlášky, nicméně přijaté změny přinesly určité zjednodušení praxe, které prosazovalo zejména ministerstvo zahraničních věcí jako adresát a zpracovatel této agendy.

[28] Administativní pomůcka pro evidenci utajovaných informací viz. § 3 vyhláška č. 529/2005 Sb.

NBÚ pro účely administrativní bezpečnosti prováděl posuzování bezpečnostní dokumentace a v rámci bezpečnostních řízení uskutečnil dohlídky u podnikatelů za účelem ověření stavu podmínek pro práci s utajovanými informacemi.

Početní přehled: [29]

	2006	2007	2008
Bezpečnostní dokumentace	280	173	136
Uskutečněné dohlídky	161	121	123

4.2 FYZICKÁ BEZPEČNOST A NBÚ

Oblast fyzické bezpečnosti zahrnuje systém opatření, ať již nasazení technických prostředků či zabezpečení formou fyzické ostrahy, režimových opatření, které mají primárně zabránit neoprávněným osobám v přistupu k utajované informaci. Pokud již k překonání systému opatření dojde, pak by měl systém v maximální možné míře přístup k utajované informaci ztížit a popř. pokus o neoprávněný přístup zaznamenat.

Zákon vymezuje fyzickou bezpečnost v hlavě V., a to ustanoveními § 24 až § 33. Prováděcí předpis, tedy vyhláška č. 328/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, byl v roce 2008 kompletně novelizován. Úloha NBÚ v této oblasti se pohybuje především v odpovědnosti za certifikaci technických prostředků a posuzování projektů fyzické bezpečnosti včetně poskytování konzultační a metodické činnosti při jejich tvorbě. Projekt fyzické bezpečnosti je rozpracování systému opatření na konkrétní objekt, ve kterém jsou buď ukládány nebo zde vznikají či jsou projednávány utajované informace. Podle úrovně stupně utajovaných informací se pak odvíjí míra zabezpečení a opatření nezbytných pro zajištění ochrany utajovaných

[29]Údaje převzaty z výročních zpráv NBÚ za r. 2006, 2007, 2008

informací. Projekt standardně obsahuje určení objektu a vymezení hranic pro jednací oblasti nebo zabezpečených oblastí s vymezením kategorií a tříd, vyhodnocení rizik, provozní řád, plán zabezpečení objektu a zabezpečených oblastí nebo jednací oblasti v krizových siutacích, způsob použití opatření fyzické bezpečnosti. Při posuzování projektu fyzické bezpečnosti je aplikován bodový systém, kterým jsou načítány body podle úrovně zabezpečení v dané kategorii opatření (např. ostraha a zařízení elektrické zabezpečovací signalizace, systém kontroly vustupu do zabezpečené oblasti nebo objektu a systém návštěv). Změny v projektu fyzické bezpečnosti je povinností hlásit a podle jejich případného dopadu na ochranu utajovaných informací podléhají posouzení a schválení NBÚ.

Přehled přijatých žádostí a posouzených projektů fyzické bezpečnosti

	2007	2008
Přijaté žádosti	164	148
Schválené projekty	215	147

Certifikace technického prostředku představuje proces, v rámci něhož jsou posuzovány technické parametry zařízení či výrobků používaných k ochraně utajovaných informací a následné vystavení certifikátu na základě odborného posudku odborného pracoviště. Pro tyto účely má NBÚ sjednánu spoluprací s řadou odborných pracovišť (zkušebny, laboratoře atd.) na základě smlouvy o spolupráci při zajištění činnosti.[30]

[30] § 46 odst. 15 a § 52 z.č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů

Přehled počtu vydaných certifikátů technických prostředků

Technické prostředky	2006	2007	2008
1. Mechanické zábranné prostředky	239	554	133
2. Elektrická zámková zařízení, systémy pro kontrolu vstupů	397*)	411**)	24
3. Zařízení el. zabezp. signalizace a tísňové systémy	199	-	201
4. speciální tv. systémy	-	-	64
5. zařízení el. požární signalizace	46	27	8
6. zařízení sloužící k vyhledávání nebezp. látek nebo předmětů	0	12	4
7. zařízení fyzického ničení nosičů informací	127	83	84
8. zařízení proti pasiv. /aktiv. odposlechu utaj. informace	-	2	2
celkem	1008	1089	520

*) statistika NBÚ uvádí v r. 2006 pouze souhrnný počet za položky 2 + 4

**) statistika NBÚ uvádí v r. 2007 pouze souhrnný počet za položky 2 až 4

4.3 BEZPEČNOST INFORMAČNÍCH A KOMUNIKAČNÍCH SYSTÉMŮ A NBÚ

Zákon bezpečnost informačních a komunikačních systémů vymezuje v hlavě VI., jmenovitě v ustanoveních § 34 – 35, a problematiku procesu certifikace pak stanoví v hlavě IX., konkrétně v ustanoveních § 46 – 53. Prováděcí předpis je pro obě oblasti

identický, jedná se o vyhlášku č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor.

V obou těchto úzce spjatých oblastech ochrany utajovaných informací má NBÚ úlohu spočívající zejména v posouzení, certifikaci informačního systému a v případě komunikačního systému pak schválení projektu komunikačního systému. Tímto způsobem NBÚ garantuje udržení jednotných standardů pro zajištění utajovaných informací, které jsou zpracovávány, přenášeny a ukládány v informačních nebo komunikačních systémech. Vzhledem k dnešní praxi se jedná o převážnou většinu utajovaných informací, a proto jde o oblast velmi citlivou a důležitou. Orgán státu, právnická osoba nebo podnikající fyzická osoba, fyzická osoba může nakládat s utajovanou informací pouze v informačním systému, který splňuje zákonem stanovené podmínky, a to že byl certifikován NBÚ a schválen do provozu odpovědnou osobou. Odpovědná osoba je povinna hlásit NBÚ uvedení systému do provozu. Prováděcí předpis následně stanoví požadavky kladené na informační systém a podmínky jeho provozu, které jsou odvislé od úrovně stupně utajení informací, s nimiž se má v systému nakládat. Současně je stanoven bezpečnostní provozní modus a obsah bezpečnostní dokumentace vedené k informačnímu systému.

Obdobně pak provozovatel komunikačního systému, který má být využíván pro nakládání s utajovanými informacemi a za který je dle zákona považován systém zajišťující přenos utajovaných informací mezi koncovými uživateli včetně koncového komunikačního zařízení, přenosového prostředí, kryptografických prostředků, obsluhy, provozních podmínek a postupů, je povinen předložit projekt bezpečnosti komunikačního systému ke schválení NBÚ. Komunikační systém lze provozovat až po schválení projektu bezpečnosti komunikačního systému. Projekt musí obsahovat bezpečnostní politiku komunikačního systému, organizační a provozní postupy provozování komunikačního systému a provozní směrnice pro bezpečnostní správu a uživatele komunikačního systému.

Přehled počtů certifikací informačních systémů za r. 2006 - 2008[31]

	2006	2007	2008	celkem
Přijaté žádosti	135	115	103	358
U/ státní správa*)	9	6	5	20
U/ podnikatel	8	17	5	30
V/ státní správa**)	35	47	57	139
V/podnikatel	50	54	50	154

*) řízení ukončeno bez vydání certifikátu

**) vydané certifikáty

4.4 KRYPTOGRAFICKÁ OCHRANA A NBÚ

Je systémem opatření na ochranu utajovaných informací za pomoci využití kryptografických metod a kryptografických materiálů při tvorbě, manipulaci a archivaci či ukládání utajovaných informací. Zákon ji vymezuje v hlavě č. VIII., jmenovitě v ustanoveních § 37 – 45. Je dále upravena dvěma prováděcími předpisy, a to vyhláškou č. 524/2005 Sb., o zajištění kryptografické ochrany utajovaných informací, a vyhláškou č. 525/2005 Sb., o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací. NBÚ je garantem v této oblasti plně a bez výjimky. Je orgánem odpovědným za chod Národního střediska pro distribuci kryptografického materiálu a provádí certifikace kryptografických prostředků, pracovišť a stínících komor. Zajišťuje odborné zkoušky pro účely zvláštní odborné způsobilosti pracovníka kryptografické ochrany a vydává pro tyto účely osvědčení o zvláštní odborné způsobilosti. Uděluje povolení pro vývoz certifikovaného kryptografického prostředku mimo území České republiky a vede evidenci udělených povolení. V případě, že dojde ke kompromitaci kryptografického material, je povinností tuto skutečnost hlásit NBÚ.

[31]Údaje převzaty z Výročních zpráv NBÚ za r. 2006, 2007. 208

V oblasti ochrany utajovaných informací před kompromitujícím elektromagnetickým vyzařováním je NBÚ certifikační autoritou a zajišťuje též provedení odpovídajících měření jak elektrických a elektronických zařízení, tak objektů v rámci procesu certifikace. V případě ochrany utajovaných informací prostřednictvím stínící komory, ktedy uzavřeného elektromagneticky stíněného prostoru zabraňujícího šíření elektromagnetického vyzařování mimo tento proctor, je NBÚ opět v pozici certifikační autority a bez vydání odpovídající certifikace nelze stíněnou komoru využívat pro účely ochrany utajovaných informací.

Přehled certifikací kryptografických prostředků za období 2006 - 2008[32]

	2006	2007	2008
Přijaté žádosti	19	19	20
Rozpracované certifikáty – st. správa	4	2	2
Rozpracované certfikáty – podnikatelé	6	8	10
Ukončeno bez vydání certifkátu – st. správa	0	1	0
Ukončeno bez vydání certifikátu - podnikatelé	2	0	1
Vydané certifikáty – st. správa	15	14	9
Vydané certifikáty - podnikatelé	2	6	3
Vydané certifikáty pro NATO	16	18	7
Vydané certifikáty pro EU	15	15	6

4.5 CERTIFIKACE A NBÚ

Jak již bylo v oblasti fyzické bezpečnosti, bezpečnosti informačních a komunikačních systémů a kryptografické ochrany uvedeno NBÚ je v těchto problematikách jedinou certifikační autoritou. Z toho vyplývá, že technické prostředky, informační systémy

[32]Využito údajů z Výročních zpráv NBÚ za r. 2006, 2007, 2008.

a kryptografické prostředky lze používat pro účely ochrany utajovaných informací pouze po udělení odpovídající certifikace ze strany NBÚ.

Certifikací rozumíme proces či postup, kterým je ověřována způsobilost k ochraně či nakládání s utajovanými informacemi u daného technického prostředku nebo informačního systému. V případě kryptografické ochrany je certifikace rozšířena jak na kryptografický prostředek tak kryptografické pracoviště, kdy je certifikací zkoumána a posuzována způsobilost pracoviště pro výkon činnosti a dále je ověřována způsobilost stínící komory k ochraně utajovaných informací.

NBÚ ověří a posoudí daný stav a v případě, že zjistí danou způsobilost pro ochranu utajovaných informací, pak certifikát vydá. Certifikáty jsou, stejně jako osvědčení pro přístup k utajovaným informacím, veřejnou listinou a zákon stanoví jejich náležitosti. Proces certifikace je určitým druhem správního řízení. Zákon a prováděcí předpisy stanoví způsob podání žádosti, její náležitostí a přílohy včetně dokumentace, postup při posuzování způsobilosti, dobu platnosti certifikátu, důvody zániku certifikátu, mechanismus opakování žádosti po uplynutí doby platnosti certifikátu atd.

4.6 PERSONÁLNÍ BEZPEČNOST A NBÚ

Jde o oblast ochrany utajovaných informací, která patří k základním, a pravděpodobně ji lze charakterizovat jako nejvýznamnější pilíř v systému ochrany utajovaných informací. Důvody jsou nasnadě, neboť chybné technické zařízení či špatné nastavení informačního systému je problémem řešitelným nahrazením novou technikou nebo opravou chyby, ale v případě selhání lidského faktoru, z důvodu nesprávného výběru osoby, která se seznámila s utajovanou informací, je třeba konstatovat, že ztráta dispozice nad utajovanou informací a její ochrana se dostává mimo kontrolu, byť by byl systém ochrany utajovaných informací sebelepší. Proto personální bezpečnost není pouhým prováděním bezpečnostních řízení, ale především výběrem vhodných osob

pro přístup k utajovaným informacím, jejich další vzdělávání a poskytování odpovídající ochrany nositelům utajovaných informací, zejména v případě cíleného zájmu ze strany neoprávněných osob.

Oblast personální bezpečnosti je upravena hlavou II. zákona, jmenovitě ustanoveními § 6 až § 14, a hlavou X., jmenovitě ustanoveními § 54 - § 64, hlavou XI., jmenovitě ustanoveními § 65 - § 72, částí IV – bezpečnostní řízení, jmenovitě ustanoveními § 89 – 95, § 101 – 135 a prováděcím předpisem, vyhláškou č. 527/2005 Sb., o stanovení vzorů v oblasti personální bezpečnosti a bezpečnostní způsobilosti a o seznamech písemností přikládaných k žádosti o vydání osvědčení fyzické osoby a k žádosti o doklad o bezpečnostní způsobilosti fyzické osoby a o způsobu podání těchto žádostí (vyhláška o personální bezpečnosti).

NBÚ poskytuje v této oblasti metodickou a konzultační činnost a zjišťuje, zda jsou dodržovány povinnosti stanovené osobám, které mají přístup k utajovaným informacím. Zákon nově rozlišuje povinnosti osob do tří kategorií, a to na obecné povinnosti, kam spadá povinnost odevzdat nalezenou utajovanou informaci nebo utajovanou informaci získanou v rozporu se zákonem. Dále stanoví povinnost odevzdat nalezené osvědčení pro přístup k utajovaným informacím či osvědčení pro cizí moc, a to buď NBÚ nebo policii a v případě zahraničí na zastupitelském úřadu České republiky. Mezi obecné povinnosti dále patří povinnost dodržovat mlčenlivost o utajovaných informacích, k nimž měl nebo má přístup, a zákaz umožnit přístup k utajované informaci neoprávněné osobě. Zákon stanoví nově povinnost hlášení změn v údajích u žadatelů o vydání osvědčení. Toto ustanovení je opět reakcí na negativní zkušenosti z předchozí praxe a pro účely prováděného řízení je bezpochyby pozitivem. Poslední obecnou povinností je plnit pokyny vydané kontrolním pracovníkem, který provádí výkon státního dozoru a které jsou nutné při provádění neodkladných opatření.

Druhou kategorií povinností jsou povinnosti osoby, která je držitelem osvědčení pro přístup k utajované informaci, avšak v nemá k těmto informacím přístup. Osoby

splňující tuto podmínku jsou povinny hlásit změny údajů NBÚ, odevzdat osvědčení vydávajícímu subjektu ve lhůtě do 5 dnů v případě, že zanikla jeho platnost z důvodu změny údajů či poškození, neprodleně hlásit vydávajícímu subjektu ztrátu či odcizení osvědčení.

Třetí kategorií povinností jsou povinnosti osoby, která je držitelem osvědčení pro přístup k utajované informaci a má současně přístup k utajovaným informacím. Zde se k povinnostem již výše uvedeným přidávají následující: dodržovat povinnosti při ochraně utajovaných informací, neprodleně oznamovat porušení povinností stanovených zákonem tomu, kdo provedl její poučení, a účastnit se pravidelně jedenkrát ročně proškolení z právních předpisů v oblasti ochrany utajovaných informací. Povinnost odborného školení jedenkrát ročně byla do zákona opět vtělena po zkušenostech z praxe, kdy byla velmi často zjišťována absence základních znalostí zásad v oblasti ochrany utajovaných informací u držitelů osvědčení pro přístup k utajovaným informacím.

Novým prvkem v oblasti personální bezpečnosti je tzv. personální project,[33] který byl taktéž iniciován na základě výsledků a statistických rozborů v oblasti požadovaných počtů bezpečnostních prověrek různé úrovně. Řada subjektů nebyla schopna definovat reálné požadavky, a počty prováděných bezpečnostních prověrek byly jak z pohledu kvantitativního tak z pohledu rozložení úrovně požadovaného stupně utajení pro nějž mělo být osvědčení vydáno, naprosto neúměrné. Tento stav bránil efektivnímu výkonu a představoval nadbytečné výdaje pro státní rozpočet. NBÚ proto zvolil variantu personálního projektu jako určitého regulátoru a korektivu pro požadavky na personální bezpečnost ze strany ministerstev a ostatních ústředních orgánů státní správy. Tito musí do personálního projektu zhodnotit stav v personální bezpečnosti za uplynulý rok a uvést předpokládaný počet fyzických osob, u kterých bude nutno provádět v roce následujícím bezpečnostní řízení, a to včetně rozlišení

[33] § 72 z.č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů

požadovaného stupně utajení. NBÚ personální projekty posoudí a zpracuje vyjádření. Oba dokumenty pak předkládá NBÚ vládě ke schválení. Podle vyjádření NBÚ ve výroční zprávě za r. 2008 přineslo zavedení personálních projektů zpřesnění a mělo i dopad na snížení počtu požadovaných bezpečnostních řízení, nicméně i podle vyjádření samotného NBÚ bude třeba iniciovat další změny.[34]

NBÚ v rámci personální bezpečnosti odpovídá za vydávání osvědčení fyzické osoby či podnikatele pro cizí moc. Tato oblast je plně v kompetenci NBÚ a proti předchozí právní úpravě ztratily zpravodajské služby oprávnění vydávat tato osvědčení pro své potřeby. Osvědčení je vydáváno na žádost dané osoby jako veřejná listina, a to na dobu nezbytně nutnou, maximálně však na dobu platnosti osvědčení pro přístup k utajovaným informacím.

[34]Návrh tzv. "Velké novely" z.č. 412/2005 Sb. předložený do parlamentu v 11.prosinci 2008 – tisk č. 683

Přehled vydaných osvědčení pro cizí moc za r. 2006 – 2008[35]

typ	2006	2007	2008	celkem
COSMIC TOP SECRET	274	216	208	698
COSMIC TOP SECRET ATOMAL	41	51	48	140
NATO SECRET	1718	1883	1501	5102
NATO SECRET ATOMAL	32	12	1	45
NATO CONFIDENTIAL	746	693	631	2070
NATO CONFIDENTIAL ATOMAL	1	1	1	3
WEU FOCAL TOP SECRET	54	61	24	139
WEU SECRET	188	105	35	328
WEU CONFIDENTIAL	82	17	8	107
EU TOP SECRET	321	123	*)	444
EU SECRET	1215	411	*)	1626
EU CONFIDENTIAL	583	209	*)	792
CELKEM	5255	3782	2457	

*) zavedením nového vzoru osvědčení v r. 2008 a jeho akceptaci ze strany orgánů EU došlo k ukončení vydávání zvláštních osvědčení pro EU.

NBÚ je dále v oblasti personální bezpečnosti jediným orgánem, který je oprávněn uznat bezpečnostní oprávnění vydané úřadem cizí moci a umožnit tak přístup k utajované informaci (viz. výše).

Do oblasti personální bezpečnosti lze zařadit i uplatnění institutu zproštění povinnosti mlčenlivosti.[36]

[35] Výroční zprávy NBÚ za r. 2006, 2007, 2008.
[36] § 63 z.č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů

V této oblasti má NBÚ, konkrétně ředitel NBÚ, oprávnění zprostit mlčenlivosti v případě, že došlo k zániku orgánu státu bez právního nástupce. Obecně ke zproštění mlčenlivosti dochází na žádost orgánu státu pro účely řízení před orgánem státu. Zproštění mlčenlivosti provádí odpovědná osoba orgánu státu, do jehož působnosti utajovaná informace spadá. Zproštění mlčenlivosti je vztaženo pouze na konkrétní utajovanou informaci, a to v nezbytně nutném rozsahu a na dobu nezbytně nutnou. Je prováděno vždy písemnou formou a stupeň utajení není zproštěním mlčenlivosti u dané utajované informace dotčen.

4.7 PRŮMYSLOVÁ BEZPEČNOST A NBÚ

Představuje 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. Oblast průmyslové bezpečnosti je upraven hlavou III. zákona, jmenovitě ustanoveními § 15 až § 20, a dále pak hlavou X., jmenovitě ustanoveními § 54 – 57, hlavou XI., jmenovitě ustanoveními § 68 - § 69, částí IV., jmenovitě ustanoveními § 89 - § 93, § 96 – 98, § 101 – 135. Zásadní úlohou NBÚ v oblasti průmyslové bezpečnosti je provádění bezpečnostích řízení podnikatele a průběžné ověřování aktuálního stavu věci, tak aby byla zajištěna ochrana utajovaných informací, s nimiž podnikatel přichází do styku. NBÚ zveřejňuje na svých internetových stránkách a ve věstníku NBÚ přehled podnikatelů, kteří disponují platným osvědčením. Zákon stanoví povinnosti podnikatele, které obdobně jako u personální bezpečnosti, rozčleňuje podle existence přístupu k utajovaným informacím. Podnikatel, který nemá aktuálně přístup k utajovaným informacím, je povinen hlásit změny údajů, ztrátu nebo odcizení osvědčení, vrátit osvědčení v případě vydání pravomocného rozhodnutí o zrušení platnosti, zabezpečit ochranu utajovaných informací při zániku platnosti osvědčení podnikatele. V případě podnikatele s přístupem k utajované informaci jsou tyto povinnosti rozšířeny o řadu dalších, a to zajistit ochranu utajovaných informací podle zákona a mezinárodních smluv,

zpracovávat a vést přehled míst nebo funkcí u kterých je nezbytný přístup k utajovaným informacím, neprodleně oznámit NBÚ skutečnost, která může mít vliv na vydání nebo platnost osvědčení fyzické osoby nebo podnikatele, zajistit vytvoření podmínek pro administrativní bezpečnost, provozovat pouze certifikovaný a schválený informační systém, v případě nesplnění podmínky stanovené v certifikační zprávě zastavit provoz informačního systému, zajistit ochranu utajovaných informací a neprodleně informovat NBÚ. Dodržovat zásady kryptografické ochrany včetně vedení evidence fyzických osob s přístupem ke kryptografickému materiálu atd., hlásit porušení ochrany utajovaných informací NBÚ, zřídit registr poskytovaných utajovaných informací a dodržovat povinnosti vztahující se k vedení registru včetně provádění pravidelné kontroly, předat utajovanou informaci poskytnutou cizí mocí nebo zahraničním parterem k zaevidování NBÚ, zasílat utajované informace prostřednictvím ústředního registru, zajistit písemné pověření fyzické osoby k přístupu k utajované informaci se zvláštním režimem nakládání označované "ATOMAL", zřídit funkci bezpečnostního ředitele, zajistit poučení fyzických osob a jejich pravidelné každoroční proškolení k právním předpisům z oblasti ochrany utajovaných informací, zajistit ověřování splnění podmínek pro stupeň Vyhrazené, schválit informační systém do provozu a tuto skutečnost nahlásit NBÚ a pověřit fyzickou osobu k činnosti nebo výkonu kryptografické ochrany a kontrolovat dodržování povinností stanovených zákonem.

Oblast průmyslové bezpečnosti v sobě zahrnuje v podstatě všechny subsystémy ochrany utajovaných informací.

5 BEZPEČNOSTNÍ ŘÍZENÍ

Jednou ze zásadních změn, které do oblasti ochrany utajovaných informací přinesla nová právní úprava je institut bezpečnostního řízení, který je používán pro oblast personální a průmyslové bezpečnosti. Na tomto místě je vhodné zmínit krátce postupy užívané v předchozím období, tedy před nabytím platnosti zákona č. 412/2005 Sb. V odborné terminologii byl užíván pojem "bezpečnostní prověrky" navrhované osoby nebo organizace. V rámci této bezpečnostní prověrky byla prováděna opatření bezpečnostní prověrky, jejichž rozsah byl odstupňován v závislosti na požadovaném stupni utajovaných skutečností, k nimž měla mít osoba či organizace přístup. V případě personální bezpečnosti pak osoba, která se podrobovala bezpečnostní prověrce, neměla v probíhající proceduře odpovídající postavení, a jediný způsob, kterým mohla do této situace vstoupit, bylo odebrání souhlasu s prováděním bezpečnostní prověrky. Toto postavení vycházelo ze stavu, kdy tzv. statutární orgán (nejčastěji zaměstnavatel, popř. osoba, která měla prověřované osobě poskytnout utajovanou skutečnost) provedl výběr vhodného kandidáta pro přístup k utajovaným skutečnostem a následně se tento kandidát stal navrhovanou osobou, která udělila souhlas s prováděním bezpečnostní prověrky. Statutární orgán podával u Národního bezpečnostního úřadu žádost o provedení bezpečnostní prověrky, jejíž přílohou byly tzv. podkladové materiály, které dodala navrhovaná osoba. Tento stav se v průběhu praxe neosvědčil a proto při tvorbě nového zákona byly zvažovány různé možnosti včetně využití z.č. 500/2004 Sb., správního řádu (dále jen "správní řád"), ale vzhledem k velmi specifickému účelu a užívaným prostředkům v proceduře bylo přistoupeno k vytvoření vlastního typu řízení - "bezpečnostní řízení" a vyloučení správního řádu v této oblasti. Jak již bylo výše uvedeno, důvodem pro tento postup byl specifický účel a užívané prostředky, neboť se jedná o řízení, kdy správní orgán na základě zjištění skutečného stavu věci a ověření pravdivosti a úplnosti údajů poskytnutých žadatelem, vydává rozhodnutí, kterým je žadateli umožněn či zamítnut přístup k utajovaným informacím. Tedy správní orgán ze zjištěného stavu věci konstatuje, zda žadatel splňuje podmínky stanovené zákonem č. 412/2005 Sb. pro vydání osvědčení fyzické či právnické osoby pro přístup k utajovaným informacím.

Základem bezpečnostního řízení je ověření splnění podmínky bezpečnostní spolehlivosti neboli vyloučení bezpečnostních rizik u žadatele. Ve zjednodušeném pohledu zde vzniká stav, kdy správní orgán posuzuje na základě zjištěných informací z minulosti, zda je žadatel způsobilý k tomu, aby mu mohly být v budoucnu svěřeny utajované informace, a dovozuje tak z chování žadatele v minulosti, jak se bude či může chovat k utajovaným informacím a jaké může mít toto chování vliv na ochranu utajovaných informací, pokud k nim bude mít žadatel přístup. Pro tyto účely má správní orgán právo ověřit poskytnuté informace u oprávněných subjektů, vyžádat si ověření údajů a zjištění stavu věci prostřednictvím zpravodajských služeb atd. Dalším důvodem pro samostatnou právní úpravu "bezpečnostního řízení" jsou zmíněné "užívané prostředky", tedy možnosti správního orgánu ověřit a získat informace ke zjištění stavu věci v rámci provádění úkonů řízení. Důsledkem použití některých úkonů bezpečnostního řízení, tím je míněno především využití zpravodajských služeb nebo postoupení informací ze strany specializovaných policejních útvarů (např. Národní protidrogová centrála), vzniká stav, kdy správní orgán obdrží utajované informace k žadateli, které dokládají zjištění bezpečnostního rizika u jeho osoby, a současně nelze žadatele s těmito skutečnostmi seznámit. Důkazní material, z něhož správní orgán při rozhodnutí bude vycházet, není žadateli zpřístupněn, a to ani v případě přezkumného řízení či projednávání v rámci soudního řízení.

Nová právní úprava definuje účastníka řízení, jeho postavení a práva v řízení včetně možnosti uplatnit námitku podjatosti, požadovat přerušení řízení či provedení důkazního řízení podle jeho návrhu. Současně zavedla institut lhůt pro provedení řízení, čímž dala účastníkovi řízení určitou právní jistotu a narovnala oprávněně kritizovanou předchozí praxi. Na straně druhé rozšířila a přesně vymezila oprávnění správního orgánu požadovat informace a údaje k ověření pravdivosti a úplnosti poskytnutých údajů (např. možnost dožadovat údaje chráněné povinností mlčenlivosti od finančních a bankovních ústavů, finančních úřadů a správců daně), zavedením institutů řízení jako je svědek, znalec, přerušení řízení, zastavení řízení a povinnosti hlášení změn údajů

v průběhu řízení umožnila zefektivnit, zrychlit a snížit náklady na řízení v porovnání s předchozí procedurou.

5.1 ÚČEL A TYPY ŘÍZENÍ

Bezpečnostní řízení je process, jehož účelem je zjistit, zda žadatel (fyzická osoba či podnikatel) splňuje podmínky stanovené zákonem č. 412/2005 Sb., pro vydání osvědčení fyzické osoby nebo podnikatele pro přístup k utajovaným informacím. Správní orgán v rámci tohoto procesu provádí úkony řízení v rozsahu vymezeném zákonem č. 412/2005 Sb. za účelem zjištění skutečného stavu věci a ověření pravdivosti informací a údajů poskytnutých žadatelem pro účely bezpečnostního řízení. Bezpečnostní řízení je používáno pro fyzické osoby a podnikatele za účelem naplnění personální a průmyslové bezpečnosti jako nedílných součástí systému ochrany utajovaných informací. V rámci bezpečnostních řízení podnikatele a fyzických osob lze rozlišit tři typy bezpečnostních řízení a to:

1. bezpečnostní řízení ve věci vydání osvědčení (do této skupiny lze řadit též tzv. "následná bezpečností řízení", tedy provádění opakovaného prověření osoby či podnikatele, který je již držitelem osvědčení)
2. bezpečnostní řizení ve věci zrušení platnosti osvědčení
3. řízení o vydání osvědčení pro přístup k utajovaným informacím cizí moci

5.2 ŽÁDOST A PŘÍLOHY

Obdobně jako průběh bezpečnostního prověření doznaly zásadní změny podklady, které jsou pro účely bezpečnostního řízení vyžadovány. Fyzická osoba nebo-li žadatel podává žádost, dotazník, prohlášení osobnostní způsobilosti, prohlášení o způsobilosti k právním úkonům, fotografii a dále uvedené přílohy. Základním zdrojem údajů je dotazník, který žadatel vyplňuje v elektronické formě, kterou následně vytiskne a pro účely řízení předává tak ve dvojí formě. Rozsah poskytovaných údajů je pro všechny požadované stupně, na které má být osvědčení vydáno, téměř identický.

V oblasti bezpečnostního řízení fyzické osoby se jedná o:

1. osobní údaje – jméno, příjmení (včetně všech předchozích) a akademické tituly, datum a místo narození, rodné číslo a státní občanství včetně předchozích, rodinný stav, data k průkazu totožnosti
2. údaje o studiu po ukončení povinné školní docházky a profesní kariéře, tedy uvedení jednotlivých zaměstnání včetně identifikačních údajů o zaměstnavateli s určením pracovní pozice či uvedením vykonávané činnosti,
3. údaje o vazbách do zahraničí, jak o pobytech v zahraničí s dobou nad 30 dnů tak o kontaktech s cizími státními příslušníky,
4. informace o finanční i majetkové situaci a podnikatelské činnosti a členství v orgánech právnických osob
5. příslušnosti ke sdružením, nadacím a obecně prospěšných společnostech,
6. místech trvalého bydliště a adresách, kde se žadatel zdržoval,
7. předchozím bezpečnostním řízení,
8. informace o době výkonu vojenské služby, příslušnosti, spolupráci či kontakty s předlistopadovými bezpečnostními a zpravodajskými službami nebo současnými bezpečnostními službami cizí moci
9. údaje o trestním stíhání a vztahu k návykovým látkám, alkoholu či jiného typu závislosti
10. údaje k rodinným příslušníkům žadatele, jejichž rozsah je odlišen podle věku.

Nedílnou součástí dotazníku je životopis a prohlášení o pravdivosti a úplnosti údajů v dotazníku. Při provádění prvního bezpečnostního řízení k žadateli jsou tyto údaje požadovány v kompletním rozsahu včetně příloh dokládajících tyto údaje. [37]

Jako přílohy žadatel dokládá :

a) rodný nebo křestní list, popřípadě další obdobné doklady,
b) doklad o nejvyšším dosaženém vzdělání,

[37] §94-95 z.č.412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů

c) potvrzení o studiu v zahraničí včetně doby trvání studia,
d) rozhodnutí orgánů činných v trestním řízení v trestních věcech,
e) potvrzení zaměstnavatele o příjmech s uvedením jejich výše, v případě jiného druhu příjmu daňové přiznání nebo jiný doklad potvrzující tento příjem, a to 5 let zpětně v případě první žádosti o vydání osvědčení nebo za období, které uplynulo od posledního předložení těchto dokladů v bezpečnostním řízení,
f) doklady o právech třetích osob zatěžujících vlastnictví žadatele,
g) doklady dokumentující rozdíl mezi zápisem ve veřejném seznamu soudu nebo jiného státního orgánu a skutečností
h) rozhodnutí příslušného orgánu o nařízení výkonu rozhodnutí. [38]

Při provádění následných řízení dokládá žadatel mimo základních identifikačních dat pouze ty údaje, u kterých došlo ke změně, a tyto změny ještě správnímu orgánu v rámci ohlašovací povinnosti nedoplnil. Lze tedy konstatovat, že následná řízení kladou na žadatele minimální nároky z hlediska předkládaných údajů, za podmínky, že si řádně plní ohlašovací povinnost danou zákonem.[39]

V oblasti bezpečnostního řízení podnikatele jsou dokládány obdobně jako u fyzické osoby – žádost podnikatele, dotazník, bezpečnostní dokumentaci podnikatele a přílohy. Dotazník podnikatele obsahuje identifikační údaje podnikatele (údaje z obchodního, živnostenského či obdobného rejstříku), údaje o majetkové a finanční situaci – tedy o bankovních účtech, výši čistého obchodního majetku, údaje z provedených ročních účetních závěrek, poskytnuté půjčky, úvěry, zastavený majetek, obchodní partneři, identifikace daňového poradce, podání návrhu na konkurs nebo vyrovnání, rozhodnutí o konkursu nebo vyrovnání, údaje o zrušení a plnění závazků vůči státu, smlouvy, jejichž předmět plnění obsahuje utajované informace, identifikaci cizich státních příslušníků, kteří jsou v pracovněprávním, členském nebo obdobném

[38] Vyhláška č. 527/2005 Sb., § 4
[39] § 66 z.č. 412/2005 Sb.

vztahu k podnikateli, údaje o vlastních nebo pronajatých nemovitostech a nebytových prostorech podnikatele, ve kterých se vyskytuje tzv. "zabezpečená oblast".[40]

Jako přílohy jsou požadovány :

a) úplný výpis z obchodního rejstříku,

b) doklady o rozhodnutích orgánů podnikatele obsahující změny, které se zapisují do obchodního rejstříku a nejsou v něm dosud zapsány,

c) výpis z evidence emise nebo čestné prohlášení podnikatele obsahující seznam osob, jejichž podíl na základním kapitálu nebo na hlasovacích právech je vyšší než 10 %, pokud je akcionářem,

d) výpis z katastru nemovitostí týkající se nemovitostí uvedených v § 97 písm. d) a h) zákona,

e) smlouvy o pronájmu prostor, budov a pozemků uvedených v § 97 písm. d) zákona,

f) roční účetní závěrky a daňová přiznání za posledních 5 let,

g) ovládací smlouvu nebo písemnou zprávu o vztazích,[41] pokud je podnikatel ovládající nebo ovládanou osobou, za posledních 5 let,

h) písemné zprávy auditora o ověření účetních závěrek za posledních 5 let, pokud tak stanoví zvláštní právní předpis,[42]

i) potvrzení finančního úřadu o stavu osobních účtů podle jednotlivých daní, ke kterým je na území České republiky registrován,

[40] § 96-98 z.č. 412/2005 Sb.
[41] § 66a obchodního zákoníku.
[42] Zákon č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů.

j) potvrzení správy sociálního zabezpečení a všech zdravotních pojišťoven, že podnikatel nemá vůči těmto institucím žádné splatné nedoplatky, včetně penále

k) přehled závazků z podnikatelské činnosti, od kterých konec sjednané lhůty splatnosti přesáhl více než 180 dnů, s uvedením jednotlivých věřitelů a důvodu nezaplacení, potvrzený odpovědnou osobou podnikatele

l) potvrzení bank nebo dalších věřitelů o plnění úvěrových smluv nebo smluv o půjčce podnikatelem

m) výpis z účtu vlastníka nebo čestné prohlášení podnikatele, s uvedením přehledu všech účastí na akciových společnostech a majetkového podílu v procentech,

n) čestné prohlášení podnikatele s uvedením přehledu ostatních investičních cenných papírů,[43] vkladů do společností s ručením omezeným, členských vkladů v družstvech, vkladů a podílů ve veřejných obchodních společnostech a komanditních společnostech

o) potvrzení insolvenčního soudu dokládající neexistenci skutečností uvedených v § 17 odst. 1 zákona

p) seznam osob v orgánech podnikatele a v prokuře podnikatele s uvedením jejich rodných čísel a souhlasu[44] k jejich využití pro účely bezpečnostního řízení.

Podnikající fyzická osoba k žádosti podle § 96 odst. 2 písm. c) zákona přiloží

a) živnostenské listy, koncesní listiny, nebo je-li osobou podnikající na základě jiného

[43] § 21 zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění pozdějších předpisů.

[44] § 219 insolvenčního zákona.

než živnostenského oprávnění[45] nebo osobou provozující zemědělskou výrobu[46], výpis z obdobné evidence

b) je-li osobou zapsanou do obchodního rejstříku, úplný výpis z obchodního rejstříku

c) výpis z katastru nemovitostí, týkající se nemovitostí uvedených v § 97 písm. d) a h) zákona

d) smlouvy o pronájmu prostor, budov a pozemků uvedených v § 97 písm. d) zákona

e) roční účetní závěrky a daňová přiznání za posledních 5 let

f) písemné zprávy auditora o ověření ročních účetních závěrek za posledních 5 let, pokud tak stanoví zvláštní právní předpis[47]

g) potvrzení finančního úřadu o stavu osobních účtů dle jednotlivých daní, ke kterým je na území České republiky registrován

h) potvrzení správy sociálního zabezpečení a všech zdravotních pojišťoven, že podnikatel nemá vůči těmto institucím žádné splatné nedoplatky, včetně penále

i) přehled závazků z podnikatelské činnosti, od kterých konec sjednané lhůty splatnosti přesáhl více než 180 dnů, s uvedením jednotlivých věřitelů a důvodu nezaplacení, potvrzený odpovědnou osobou podnikatele

j) potvrzení bank nebo dalších věřitelů o plnění úvěrových smluv nebo smluv o půjčce podnikatelem

[45] § 115 insolvenčního zákona.
[46] § 117 insolvenčního zákona.
[47] Zákon č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů.

k) výpis z účtu vlastníka nebo čestné prohlášení podnikatele, s uvedením přehledu všech účastí na akciových společnostech a majetkového podílu v procentech

l) čestné prohlášení podnikatele s uvedením přehledu ostatních investičních cenných papírů,[48] vkladů do společností s ručením omezeným, členských vkladů v družstvech, vkladů a podílů ve veřejných obchodních společnostech a komanditních společnostech

m) potvrzení živnostenského úřadu, že v živnostenském rejstříku není uveden záznam:
1. pozastavení nebo přerušení provozování živnosti,
2. datu zániku živnostenského oprávnění,
3. usnesení o zrušení konkursu, mimo jeho zrušení pro nedostatek majetku,
4. překážkách provozování živnosti podle zvláštního právního předpisu[49],
5. přehledu o uložených pokutách včetně sankčních opatření uložených jinými správními orgány v souvislosti s podnikáním

n) potvrzení podle odstavce 1 písm. o). Písemnosti uvedené v odstavci 1 písm. a), c), d) a i) až p) a v odstavci 2 písm. b), c) a g) až n) nesmí být starší 60 dnů od data vystavení. Zahraniční osoba, která je podnikatelem podle zvláštního právního předpisu[50], doloží písemnosti uvedené v odstavci 1 nebo odstavci 2 formou obdobných dokladů z příslušných evidencí podle země původu.

5.3 PROVÁDĚNÍ ŘÍZENÍ, OPRÁVNĚNÍ, POUŽÍVANÉ INSTITUTY

Jak již bylo výše uvedeno, účelem bezpečnostního řízení je zjistit úplně a přesně stav věci v rozsahu, který je nezbytný pro vydání rozhodnutí. K dalším obecným zásadám bezpečnostního řízení patří, že řízení je neveřejné, správní orgán musí při

[48] § 21 zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění pozdějších předpisů.
[49] § 134 insolvenčního zákona.
[50] § 136 insolvenčního zákona.

řízení šetřit osobní čest a důstojnost všech osob řízením dotčených. Řízení je obdobně jako správní řízení vedeno v českém jazyce, a pokud žadatel dokládá písemnosti v cizím jazyce, je povinen zajistit a předložit jejich úřední překlad do českého jazyka. Účastník řízení je oprávněn dát se zastupovat zmocněným zástupcem, avšak v případě osobních úkonů, tedy jmenovitě pohovoru, je zastoupení vyloučeno.

Rozsah řízení respektive úkonů prováděných v rámci řízení je upraven v závislosti na úrovni stupně utajované informace pro který má být vydáno osvědčení. Jsou rozlišovány 3 stupně – Důvěrné, Tajné, Přísně tajné.[51]

5.4 BEZPEČNOSTNÍ ŘÍZENÍ K ŽÁDOSTI O VYDÁNÍ OSVĚDČENÍ FYZICKÉ OSOBY PRO PŘÍSTUP K UTAJOVANÉ INFORMACI STUPNĚ DŮVĚRNÉ

Jak již bylo uvedeno jedná se o bezpečnostní řízení s nejnižším rozsahem povinných úkonů v řízení. Správní orgán provádějící řízení ověřuje pravdivost poskytnutých údajů a zjišťuje výskyt bezpečnostních rizik cestou vyžádání potřebných informací od příslušných orgánů státu, právnické osoby nebo podnikající fyzické osoby, pokud s ní nakládají. Vzhledem k charakteru těchto úkonů se toto řízení dá nazvat "evidenčním prověřením" a v porovnáním s předchozí praxí bezpečnostních prověrek lze konstatovat, že rozdíl je v podstatě ve dvou oblastech, a to v rozsahu ověřovaných údajů a oslovovaných subjektů. Původní praxe neumožňovala, bez dalších opatření, ověření údajů k ostatním osobám tvořící společnou domácnost s žadatelem a taktéž nedovolovala správnímu orgánu požadovat informace od právnických osob nebo podnikajících fyzických osob. Tyto změny přímo reflektují problémy, které přinášela přechozí praxe a lze konstatovat, že je v dostatečné míře též odstranily. Doba stanovená k provedení řízení odpovídá tedy rozsahu úkonů a je v současné době stanovena na 3 měsíce.

[51] U přístupu k utajovaným informacím stupně Vyhrazené není prováděno bezpečnostní řízení a proto jej zpracovatel v této části nezmiňuje.

5.5 BEZPEČNOSTNÍ ŘÍZENÍ K ŽÁDOSTI O VYDÁNÍ OSVĚDČENÍ FYZICKÉ OSOBY PRO PŘÍSTUP K UTAJOVANÉ INFORMACI STUPNĚ TAJNÉ

Jedná se o druhou úroveň bezpečnostního řízení, která v sobě zahrnuje úkony nižšího stupně, tedy Důvěrného, a současně správní orgán ověří identitu žadatele, přičemž k tomuto úkonu může požádat o ověření příslušnou zpravodajskou službu nebo policii. Pokud získané informace nepostačují pro zjištění skutečného stavu věci, může správní orgán požádat příslušné zpravodajské služby nebo policii o provedení šetření k žadateli a osobám starším 18 let žijícími s žadatelem ve společné domácnosti. Jak vyplývá z rozsahu úkonů jedná se již o řízení, jehož součástí je možnost využití "šetření", tedy aktivní získávání informací k osobě žadatele či osobám, které sdílejí s žadatelem společnou domácnost. Lhůta pro zpracování žádosti je stanovena na 9 měsíců ode dne jejího podání.

5.6 BEZPEČNOSTNÍ ŘÍZENÍ K ŽÁDOSTI O VYDÁNÍ OSVĚDČENÍ FYZICKÉ OSOBY PRO PŘÍSTUP K UTAJOVANÉ INFORMACI STUPNĚ PŘÍSNĚ TAJNÉ

Jedná se bezpečnostní řízení pro nejvyšší stupeň utajované informace a proto v sobě mimo úkonů bezpečnostních řízení pro nižší stupně zahrnuje jako povinný úkon šetření příslušné zpravodajské služby k výskytu bezpečnostních rizik v prostředí, ve kterém se žadatel pohybuje. Dalším povinným úkonem je provedení pohovoru[52] s osobou, která má být držitelem osvědčení pro přístup k nejvyššímu stupni utajení. Lhůta k provedení bezpečnostního řízení je vzhledem k rozsahu úkonů stanovena na dobu 12 měsíců.

[52] Institut "Pohovoru" je vymezen ustanovením § 105 z.č.412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů

Požadavky na zpravodajské služby:
Bezpečnostní informační služba [53]
r. 2008 – bezpečnostní řízení fyzických osob
přijaté žádosti - 373 vyřízené žádosti – 418

r. 2008 – bezpečnostní řízení podnikatele
vyřízené žádosti – 101

Vojenské zpravodajství [54]
r. 2008 – bezpečnostní řizení fyzických osob
vyřízené žádosti – 195

r. 2008 – bezpečnostní řízení podnikatele
vyřízené žádosti – 5

Pro dokreslení objemu rozsahu běžných tzv. evidenčních dotazů, tedy dotazu na výskyt osoby v evidencích vedených oprávněnými subjekty, je uváděn přehled počtů z Výroční zprávy Vojenského zpravodajství za r. 2008. Z uvedených počtů lze dovozovat, že obdobný objem dotazů byl zaslán i na ostatní zpravodajské služby a dalším oprávněným subjektům.

Přehled evidenčních dotazů zaslaných NBÚ v letech 2003- 2008 na Vojenské zpravodajství

	2003	2004	2005	2006	2007	2008	celkem
osoby	17496	24764	27662	47737	34171	30590	182420
podnikatelé	245	480	507	347	427	494	2500

[53]Výroční zpráva BIS za r. 2008
[54]Výroční zpráva VZ za r. 2008

Nová právní úprava řeší i situaci, kdy úkony stanovené pro bezpečnostní řízení požadovaného stupně nejsou dostačující pro zjištění stavu věci. Tento problém byl v předchozím zákoně upraven nedostatečně, a byl proto zdrojem různých problémů. Proto má v současné době správní orgán možnost požádat žadatele o udělení písemného souhlasu s provedením úkonů řízení vyššího stupně, a v případě jeho neudělení, je toto zákonným důvodem pro zastavení řízení.[55]

Lhůty pro provádění bezpečnostních řízení představují další nový prvek v zákonné úpravě a jsou důsledkem stavu, kdy některé bezpečnostní prověrky byly ze strany správního orgánu prováděny neúnosně dlouhou dobu. Tento stav byl dán historickým vývojem a úzce souvisel se situací, která vznikla po nabytí účinnosti zákona č. 148/1998 Sb., kdy byl Národní bezpečnostní úřad doslova nárazově zavalen tisíci žádostmi podanými ve stejné době. Zákon č. 148/1998 Sb. neobsahoval v podstatě žádná překlenovací opatření na řešení situace, která nastala, tedy situace, že bylo potřeba pro řadu osob zajistit přístup k utajovaným skutečnostem v době, než došlo k provedení bezpečnostní prověrky a vydání osvědčení. Tato absence v zákoně č. 148/1998 Sb. vytvářela komplikované situace a mnohdy znesnadňovala dosud běžně prováděné pracovní činnosti. Je třeba si uvědomit, že na rozdíl od nové právní úpravy, zákon č. 148/1998 Sb. stanovil vydání osvědčení jako podmínku pro výkon nebo ustanovení do funkce. Zákon č. 148/1998 Sb. umožňoval pouze jednu variantu přístupu k utajovaným skutečnostem bez vydaného osvědčení, jednalo se o tzv. souhlas s přístupem k utajovaným skutečnostem podle § 40 a bylo jej možno udělit na žádost statutárního ogránu se souhlasem navrhované osoby na dobu 2 měsíců, a to pouze u žádostí stupně Tajné a Přísně tajné, pokud byla provedena některá opatření bezpečnostní prověrky s kladnými výsledky. Vyjimka však neřešila přístup k utajovaným skutečnostem cizí moci, a tak bylo její využití, zejména v oblasti rezortů ministerstva zahraničních věcí a obrany, značně svazující.

[55] § 113 odst. 1 písm. e) z.č.412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů

Neúměrné množství žádostí o vydání osvědčení, limitované možnosti nově vzniklého Národního bezpečnostního úřadu a tlak na vydání osvědčení ze strany statutárních orgánů, vzhledem k jejich potřebám řešit personální obsazení, bylo velmi kolizní a přineslo negativní zkušenost s délkou prováděných prověrek natolik silnou, že při tvorbě zákona byla podmínka stanovení lhůt pro řízení jako jednou ze základních ze strany připomínkujících subjektů.

Zavedením lhůt byla dána účastníkovi řízení právní jistota, což je bezesporu kladem jak pro samotné účastníky řízení tak i pro odpovědné osoby při jejich přípravě personálních projektů, a v případě přijetí navrhované "velké novely" budou uvedené lhůty dále zkráceny.

Správní orgán může lhůtu prodloužit, a to vždy maximálně o dobu, která je stanovena pro provedení řízení v daném stupni. Toto prodloužení se žadateli oznamuje písemnou formou včetně odůvodnění.

V souvislosti s institutem lhůt je třeba zmínit instituty přerušení a zastavení řízení.[56] Jedná se opět o nově zavedenou možnost, která je reakcí na předchozí nedostatečnou právní úpravu. Správní orgán má možnost řízení přerušit z důvodu předběžné otázky, při výzvě k odstranění nedostatků v žádosti, v případě, že není možno vyslechnout nepominutelného svědka, byl-li stanoven znalec pro vypracování znaleckého posudku a pokud o přerušení řízení požádal sám žadatel. Využití tohoto institutu znamená, že správní orgán se v řízení dostal do situace, kdy již dále nemůže konat a musí řízení přerušit. Řízení je přerušováno rozhodnutím a v řízení je pokračováno dnem, kdy pominou důvody, které byly příčinou přerušení řízení nebo dnem uplynutí lhůty stanovené správním orgánem pro přerušení. V době přerušení řízení pak lhůta stanovená pro provádění řízení neběží.

[56] §112-113 z.č.412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů

Pokud jde o zastavení řízení, pak mimo zpětvzetí žádosti ze strany žadatele správní orgán řízení zastaví, jestliže žadatel neodstranil ve stanovené lhůtě nedostatky žádosti nebo se opakovaně nedostavil bez řádné omluvy k pohovoru. Dále správní orgán řízení zastaví, pokud zjistí, že žadatel nesplňuje základní podmínky věku 18 let, způsobilosti k právním úkonům a trestní bezúhonnost.

Správní ográn v případě, že nastane situace, která naplňuje některou z uvedených důvodů pro zastavení řízení,[57] vydá rozhodnutí o zastavení řízení. Pro doplnění je třeba ještě dodat, že po vyjasnění potřeb ze strany orgánů veřejné správy a samosprávy došlo k přeskupení požadavků v počtech držitelů osvědčení, a tak je z hlediska počtu prováděných bezpečnostních řízení pro osvědčení stupně Důvěrné hlavní skupinou s počtem kolem 64% z celkového objemu prováděných bezpečnostních řízení. Pokud jde o objem počtu bezpečnostních řízení pro osvědčení stupně Tajné pohybuje se zhruba na 33% z celkového objemu a v případě bezpečnostních řízení stupně Přísně Tajné lze hovořit o objemu do 3% [58] z celkového počtu.

Pro ilustraci počtů v oblasti personální bezpečnosti – tj. podané žádosti, vydaná osvědčení, rozhodnutí o nevydání a zastavená řázení (viz. níže tabulka). Disproporce mezi počty přijatých a vyřízených žádostí je vytvořena převodem nezpracovaných žádostí z předchozího roku. Podíváme-li se na uvedená čísla, je třeba konstatovat, že jde stále o vysoké počty, uvědomíme-li si, že délka platnosti vydávaných osvědčení pro jednotlívé stupně byla prodloužena, a celkově by mělo docházet k průběžnému poklesu počtů podávaných žádostí.

[57] §113 z.č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů

[58] Výpočet z údajů poskytnutých NBÚ ve výročních zprávách za r. 2006, 2007, 2008

Bezpečnostní řízení fyzických osob - přehled počtů žádostí, vydaných osvědčení, rozhodnutí o nevydání a zastavení r. 2006 - 2008

rok/stupeň	2006/ D	2007/ D	2008/ D	2006/ T	2007/ T	2008/ T	2006/ PT	2007/ PT	2008/ PT	celkem
Žádosti	6789	4695	4059	3765	3267	2930	210	200	343	26258
vydáno	9460	5043	4097	4376	3668	2612	257	230	189	29932
nevydáno	142	45	31	30	17	11	4	0	1	281
zastaveno	223	110	115	69	93	72	9	11	8	710
celkem	16614	9293	8302	8240	7045	5625	480	441	541	

Pokud jde o stav počtů v oblasti průmyslové bezpečnosti, pak poměrně vyrovnaný objem tvoří žádosti na stupeň Vyhrazené (45%) a Důvěrné (42%), pak následují žádosti na stupeň Tajné (12,5%) a u stupně Přísně tajné je počet minimální (0,3%).

5.7 BEZPEČNOSTNÍ ŘÍZENÍ PODNIKATELE

Přehled počtu žádostí, vydaných osvědčení, rozhodnutí o nevydání a zastavení v období 2006 - 2008

rok/stupeň	06/ V	07/ V	08/ V	06/ D	07/ D	08/ D	06/ T	07/ T	08/ T	06/ PT	07/ PT	08/ PT	celkem
žádosti	95	90	99	78	85	102	33	21	25	1	1	0	630
vydáno	203	117	82	157	117	97	38	44	27	1	2	1	886
nevydáno	-	-	-	-	3	1	-	-	-	-	-	-	4
zastaveno	-	5	6	-	2	5	-	1	-	-	-	-	20*)
celkem	298	212	187	235	207	205	71	66	52	2	3	1	

*) nevydání v r. 2006 nebyla rozlišena podle stupňů – celkový počet – 12

5.8 ÚKONY A ZAJIŠTĚNÍ ÚČELU V PRŮBĚHU ŘÍZENÍ

5.8.1 INSTITUT SVĚDKA

Zcela novou praxí je zavedení institutu svědka. Zákon umožňuje správnímu orgánu předvolat svědka za účelem zjištění skutečného stavu věci a posouzení výskytu bezpečnostních rizik. Osoba, která má podat svědeckou výpověď, je povinna se dostavit a musí vypovídat pravdivě a úplně. Pokud tak neučiní vystavuje se možnosti sankce peněžitého trestu, a to až do výše 50.000 Kč.[59] Výpověď svědka je protokolována, a tato písemnost je pak součástí bezpečnostního spisu. Jedná se v podstatě o obdobu provedení důkazu svědeckou výpovědí, tak jak jej aplikuje zákon č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů (dále jen "správní řád"), avšak s tou výjimkou, že by účastník řízení byl v časovém předstihu o provedení svědecké výpovědi informován a byla mu dána možnost přítomnosti u této výpovědi.

5.8.2 INSTITUT POHOVORU[60]

Jedná se o úkon převzatý z předchozí praxe, avšak se zákonem více vymezenými pravidly pro jeho provádění. Správní orgán provádí pohovor s účastníkem řízení pokud, se vyskytnou skutečnosti, které je třeba objasnit pro zjištění skutečného stavu věc,i a vždy v případě účastníka řízení, který žádá o vydání osvědčení pro přístup k nejvyššímu stupni utajení, tedy Přísně Tajné. K pohovoru je účastník řízení předvoláván písemně a jedná se o nezastupitelný úkon v řízení. To znamená, že účastník řízení může mít s sebou zmocněného zástupce či advokáta, ale ten není oprávněn do průběhu pohovoru zasahovat. Pohovor je protokolován a může být zaznamenán na zvukový nebo obrazový nosič, ale pouze se souhlasem účastníka řízení. Zákon umožňuje i variantu pohovoru ve formě písemného vyjádření, a to v případech, kdy je účastník řízení dlouhodobě v zahraničí. Pohovor lze tedy definovat jako řízenou

[59] § 104, 116 z.č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů

[60] § 105 z.č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů

komunikaci mezi správním orgánem a účastníkem řízení, která má objasnit skutečný stav věci a současně dát možnost účastníkovi řízení vyjádřit se ke zjištěným skutečnostem, pokud se nejedná o utajované informace.

Jedná se o velmi silný institut, který lze nalézt téměř v každém evropském systému bezpečnostního prověřování, pochopitelně v různých formách a s odlišným zákonným vymezením, které vyplývá z postavení personální bezpečnosti v dané zemi, respektive z postavení subjektu oprávněného tuto činnost provádět.

Jak již bylo uvedeno, bezpečnostními řízením je ověřováno, zda účastník řízení splňuje zákonem stanovené podmínky pro vydání osvědčení. Podmínky jsou v případě fyzických osob stanoveny v hlavě II. zákona a jedná se o tyto:

- věk 18 let (u této podmínky došlo ke změně proti předchozí právní úpravě, která stanovila věkovou hranici 21 let pro přístup k utajovaným informacím stupně Přísně Tajné)
- způsobilost k právním úkonům v plném rozsahu (tato podmínka v předchozí právní úpravě nebyla)
- bezúhonnost (za osobu bezúhonnou je považována ta, která nebyla pravomocně odsouzena za spáchání úmyslného trestného činu nebo trestného činu vztahujícího se k ochraně utajovaných informací, pokud se na ni nehledí, jako by odsouzena nebyla. U této podmínky došlo pouze k určitému zpřesnění pojmu bezúhonnosti v porovnání se zák.č. 148/1998 Sb.)
- státní občanství České republiky nebo státní občanství členského státu Evropské unie nebo Organizace Severoatlantické smlouvy (u této podmínky došlo k zásadnímu posunu proti předchozí právní úpravě. Zákon č. 148/1998 Sb., stanovil podmínku českého státního občanství a výjimku z této podmínky musela schvalovat vláda ČR, což představovalo poměrně značné komplikace v praxi)
- osobnostní způsobilost, kterou se rozumí, že osoba netrpí poruchou nebo

obtížemi, které mohou mít vliv na její spolehlivost či schopnost utajovat informace (u této podmínky došlo ke změně proti z.č.148/1998 Sb. a navazujících vyhlášek, neboť místo speciálních akreditovaných odborných pracovišť, která prováděla vyšetření pro osoby, u kterých bylo žádáno o vydání osvědčení pro přístup k utajovaným informacím stupně Tajné nebo Přísně Tajné, bylo zavedeno posouzení na základě znaleckého posudku. Znalecký posudek je však vyžadován pouze v odůvodněných případech. Účastník řízení standardně vyplňuje prohlášení k osobnostní způsobilosti, které je součástí žádosti a pouze v případech, kdy je zjištěna skutečnost vyvolávající pochybnost o osobnostní způsobilosti, pak správní orgán ustanoví znalce. Toto ustanovení § 13 a § 106 zákona doznalo novelizace, neboť původní text zákona stanovil pro osoby požadující osvědčení pro přístup k utajovaným informacím stupně Přísně Tajné znalecký posudek. Tato podmínka se stala předmětem kritiky a jako neadekvátní byla následně novelou odstraněna. U této podmínky je třeba zmínit, že zde je samostatné ustanovení § 13 odst. 3 zákona, kterým se určuje odlišný postup pro posuzování podmínky osobnostní způsobilosti pro příslušníky, zaměstnance, uchazeče o zaměstnání u zpravodajských služeb a Ministerstva vnitra ve zvláštních případech. (viz. dále)

- bezpečnostní spolehlivost[61]
- jedná se o stěžejní podmínku pro udělení osvědčení a lze jednoznačně konstatovat, že ověření a posouzení bezpečnostní spolehlivosti je skutečným předmětem bezpečnostního řízení. Správní orgán při posuzování bezpečnostní spolehlivosti zkoumá zjištěný stav, poskytnuté údaje a informace ze strany účastníka řízení v jednotlivostech i v souhrnu, za účelem vyloučení výskytu bezpečnostních rizik, tak jak jsou stanovena zákonem.

[61] § 14 z.č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů

Bezpečnostní rizika lze rozdělit na :

- tzv. nepřekročitelná,[62] tedy taková rizika, která jsou-li jsou u účastníka řízení zjištěna, je vždy konstatováno nesplnění podmínky bezpečnostní spolehlivosti. Jedná se o závažnou nebo opakovanou činnost proti zájmům České republiky a o činnost spočívající v potlačování základních práv a svobod a nebo podpora takové činnosti. Tato rizika jsou u účastníka řízení zjišťována zpětně za období od 15 let jeho věku.
- tzv. překročitelná,[63] tedy taková rizika, která jsou posuzována v dalším kontextu, zejména do jaké míry může zjištěná skutečnost ovlivnit schopnost utajovat informace, k době výskytu, rozsahu, charakteru a k chování účastníka řízení ve zkoumaném období. Zkoumaným obdobím je v případě žádosti o vydání osvědčení pro stupeň Důvěrné – 10 let, Tajné – 15 let, Přísně Tajné – 20 let, nebo za období od 15 let věku podle toho, které z nich je kratší. Tento časový limit se nevzahuje na tzv. historické riziko, tedy ustanovení § 14 odst. 3 písm. a) zákona, jmenovitě zařazení do složky bývalé Státní bezpečnosti s rozvědným nebo kontrarozvědným zaměřením, zpravodajské správy Generálního štábu Československé lidové armády anebo odboru vnitřní ochrany Sboru nápravné výchovy anebo prokazatelnou spolupráci s bývalou Státní bezpečností nebo zpravodajskou správou Generálního štábu Československé lidové armády nebo odborem vnitřní ochrany Sboru nápravné výchovy. V tomto případě je riziko posuzováno od věku 15 let účastníka řízení. Za "překročitelná" bezpečnostní rizika je považováno užívání jiné identity, pokud nesouvisela s užíváním jiné identity ze zákonných důvodů, úmyslné porušení právních předpisů, na jehož základě může nastat újma zájmu České republiky, chování, které má vliv na důvěryhodnost nebo ovlivnitelnost osoby a může ovlivnit její schopnost utajovat informace, styky s osobou, která vyvíjí nebo vyvíjela činnost proti zájmům České republiky, pravomocné odsouzení pro trestný čin, uvedení nepravdivé informace nebo zamlčení informace

[62] § 14 odst. 2 z.č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti
[63] § 14 odst. 3 z.č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů

rozhodné pro objektivní zjištění skutečného tavu věci v řízení podle části čtvrté nebo nenahlášení změny údajů uvedených v příloze k žádosti o vydání osvědčení fyzické osoby nebo v jiném materiálu poskytnutém správnímu orgánu v příloze žádosti, porušení povinnosti při ochraně utajovaných informací nebo zřejmě nepřiměřené finanční nebo majetkové poměry vzhledem k řádně přiznaným příjmům fyzické osoby. Všechny tyto výše uvedené zjištěné skutečnosti mohou představovat bezpečnostní riziko a nesplnění podmínky bezpečnostní spolehlivosti. Zde musí správní orgán uvážit jak zjištěné skutečností tak všechny další okolnosti a souvislosti ve vztahu k možným bezpečnostním rizikům.

Ustanovení § 14 zákona obsahuje odst. 7, který stanoví odlišný postup pro zpravodajské služby (viz. dále)

Podmínky pro přístup podnikatele k utajovaným informacím stanoví hlava III. zákona a jsou to tyto: [64]

- ekonomická stabilita,

podnikatel nesplňuje tuto podmínku pokud byl zrušen, byla mu povolena ochranná lhůta, na jehož majetek byl prohlášen konkurs nebo návrh na prohlášení konkursu byl zamítnut pro nedostatek majetku, popř. byl konkurs zrušen pro nedostatek majetku, u kterého bylo soudem povoleno nucené vyrovnání nebo na něhož byl soudem návrh na nucené vyrovnání zamítnut nebo u kterého byla zavedena nucená správa. Podnikatel může být za ekonomicky nestabilního považován, pokud má splatný nedoplatek na pojistném na sociální zabezpečení, na příspěvku na státní politiku zaměstnanosti nebo na pojistném na veřejném zdravotním pojištění včetně penále. Dále podnikatel, který má splatný nedoplatek na dani z příjmů, na dani z přidané hodnoty či na jiných daních včetně příslušného penále z dlužné částky, popř. na vyměřeném clu, včetně případných úroků, nebo podnikatel, který trvale či opakovaně neplní finanční povinnosti

[64] § 16 z.č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů

vůči státu, fyzickým nebo právnickým osobám a podnikatel, u něhož bylo rozhodnuto v exekuci o majetek.

- bezpečnostní spolehlivost

nebo vyloučení bezpečnostních rizik. Za tzv. "nepřekročitelné" bezpečnostní riziko je zjištěná činnost statutárního orgánu nebo jeho člena, člena kontrolního orgánu nebo prokuristy proti zájmům České republiky. Za ostatní tzv. "překročitelná" rizika lze považovat uvedení nepravdivé informace nebo zamlčení informace rozhodné pro objektivní a úplné zjištění skutečného stavu věci při ověřování podmínek pro vydání osvědčení podnikatele nebo nenahlášení změny údajů uvedených v žádosti nebo v jiném materiálu poskytnutém správnímu orgánu k žádosti, kapitálové, finanční nebo obchodní vztahy k jiným fyzickým nebo právnickým osobám anebo k cizí moci, které vyvíjejí nebo vyvíjely činnost proti zájmům České republiky, personální nestabilitu ve statutárním nebo kontrolním orgánu nebo v osobách prokuristů, je-li podnikatel akciovou společností s jinou formou akcií než jsou akcie znějící na jméno, je-li společníkem, který má rozhodující vliv na volbu nebo jmenování statutárního nebo kontrolního orgánu podnikatele akciová společnost s jinou formou akcií, než jsou akcie znějící na jméno, porušení povinností při ochraně utajovaných informací, pravomocné odsouzení fyzické osoby, která je společníkem podnikatele, pro úmyslný trestný čin, úmyslné porušení právních předpisů osobami oprávněnými jménem podnikatele nebo za podnikatele jednat, na jehož základě může nastat újma zájmu České republiky nebo vztah cizího státního příslušníka zaměstnaného podnikatelem k fyzickým osobám nebo právnickým osobám nebo k cizí moci, které vyvíjely nebo vyvíjejí činnost proti zájmům České republiky.

Stejně jako v oblasti bezpečnostní spolehlivosti u personální bezpečnosti, vychází vymezení bezpečnostních rizik u právnických osob, tedy podnikatelů, a změny provedené proti předchozí právní úpravě z praxe při aplikaci zákona č. 148/1998 Sb. a jsou v úzké návaznosti na novelizaci právních předpisů v podnikatelské činnosti.

- schopnost zabezpečit ochranu utajovaných informací,

touto podmínkou se rozumí, že podnikatel je schopen zabezpečit a dodržovat jednotlivé druhy ochrany utajovaných informací na požadované úrovni pro příslušný stupeň utajovaných informací

- zajištění personální bezpečnosti u odpovědné osoby a prokuristů

tato podmínka úzce souvisí s předchozí podmínkou a vymezuje povinnost odpovědné osoby a prokuristů disponovat platným osvědčením fyzické osoby minimálně pro stupeň utajovaných informací, pro které má být vydáno osvědčení podnikatele.

Pro rozsah splnění podmínek pro vydání osvědčení podnikateli je zásadní forma přístupu, pro kterou má být osvědčení vydáno. Zákon rozlišuje dvě varianty, buď jde o přístup podnikatele k utajované informaci, která u něho bezprostředně vzniká nebo je mu poskytnuta – pak musí být splněny všechny podmínky stanovené § 16 zákona, nebo jde o přístup podnikatele k utajované informaci, která u něj nevzniká ani mu není poskytována, ale ke které mají přístup zaměstnanci podnikatele nebo osoby jednající jménem podnikatele, a to v souvislosti s výkonem pracovní nebo jiné činnosti pro podnikatele na základě smlouvy. V druhém případě je postačující naplnění podmínky § 16 odst. 1 písm. c) zákona, tedy splnění personální bezpečnosti.

Správní orgán pro účely bezpečnostního řízení zakládá bezpečnostní svazek.[65] Jedná se o soubor písemností a materiálů vztahujících se k řízení a hlášení změn, který je členěn na část neutajovanou a utajovanou. Tento svazek je veden správním orgánem a je vyřazen po 20leté lhůtě od data posledního pravomocného rozhodnutí, které obsahuje. V průběhu řízení, až do vydání rozhodnutí má žadatel právo nahlédnout do neutajované části svazku, pořídit si výpis či vyžádat kopii některé z písemností.

Správní orgán je při provádění řízení vázán obecnou zásadou postupovat tak, aby byl úplně a přesně zjištěn stav věci v rozsahu, který je nezbytný pro vydání rozhodnutí. V praxi to znamená, že jakmile správní orgán po provedení zákonem stanovených

[65] §124 z.č. 412/205Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů

úkonů řízení v daném rozsahu zjistí, že žadatel splňuje podmínky pro vydání osvědčení, rozhodne o jeho vydání. Pokud správní orgán zjistí, že žadatel nesplňuje dané podmínky, pak je vydáno též rozhodnutí, a to buď o nevydání osvědčení nebo o zastavení žádosti.

5.8.3 KLADNÉ ROZHODNUTÍ ŘÍZENÍ

V případě, že žadatel splňuje zákonem stanovené podmínky je místo "kladného rozhodnutí" vydáváno Osvědčení o přístupu fyzické osoby či podnikatele k utajované informaci požadovaného stupně. Dokument osvědčení je veřejnou listinou a jeho platnost je omezena v závislosti na úrovni stupně utajované informace, k níž má mít jeho držitel přístup - Důvěrné – 9 let, Tajné – 7 let, Přísně Tajné – 5 let.[66] Správní orgán zašle Osvědčení jeho budoucímu držiteli a kopii založí do odpovídajícího bezpečnostního svazku.

5.8.4 NEGATIVNÍ ROZHODNUTÍ ŘÍZENÍ

Pokud správní orgán zjistí, že žadatel, jako fyzická osoba, nesplňuje podmínku pro vydání osvědčení v oblasti způsobilosti k právním úkonům v plném rozsahu, věku 18 let nebo bezúhonnosti, pak vydá rozhodnutí o zastavení řízení. [67]

V případě nesplnění ostatních podmínek pro vydání osvědčení je správním orgánem vydáváno rozhodnutí o nevydání osvědčení. Rozhodnutí se vydává vždy v písemné formě a musí obsahovat jak výrokovou část tak řádné odůvodnění, které obsahuje jak konkrétní důvody, které vedly správní orgán k zamítavému stanovisku, tak uvedení podkladů a informací, z nichž správní orgán při rozhodování vycházel. Jedinou výjimkou z tohoto postupu je situace, kdy správní orgán vycházel při rozhodnutí

[66] § 54-56 z.č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů

[67] §113 odst. 1 písm. a) z.č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů

z utajované informace, a nelze ji tedy do rozhodnutí uvést. V tomto případě správní orgán pouze na utajovanou informaci v rozhodnutí odkáže, bez dalšího.

Žadatel má právo proti tomuto rozhodnutí podat rozklad ve lhůtě do 15 dnů ode dne převzetí rozhodnutí. Rozklad podává k vyššímu stupni správního orgánu, tedy v případě Národního bezpečnostního úřadu k řediteli úřadu. Podání rozkladu má v tomto případě odkladný účinek.

Rozklad je podáván písemnou formou a má stanovené náležitosti. Mimo identifikačních údajů žadatele je třeba v rozkladu uvést zejména proti kterému rozhodnutí je směřován, čeho se žadatel domáhá a v čem spatřuje rozpor s právními předpisy či nesprávnost napadeného rozhodnutí.

Správní orgán, který rozhodnutí vydal, může o rozkladu rozhodnout v případě, že mu plně vyhoví a původní rozhodnutí zruší. Tento postup bývá uplatňován zejména v případě, že dojde k pochybení při vydání rozhodnutí nebo je zjištěn rozpor s právními předpisy.

Pokud správní orgán neshledá důvody k zrušení rozhodnutí předává spisový materiál včetně rozkladu a stanoviska k němu rozkladové komisi. Rozkladová komise přezkoumá spisový materiál, postup správního orgánu a posoudí rozklad. Následně zpracuje návrh pro ředitele (Národního bezpečnostního úřadu, zpravodajské služby) nebo ministra vnitra, podle toho jaký správní orgán žádost projednává. Ředitel nebo ministr vnitra pak následně vydá rozhodnutí v řízení o rozkladu. Pokud shledá důvody k vyhovění rozkladu, vydá rozhodnutí, kterým se ruší původní rozhodnutí správního orgánu, a věc jde do dalšího projednání. Pokud není rozkladu vyhověno, je vydáno rozhodnutí o zamítnutí rozkladu, které je pravomocné. Žadatel má možnost proti tomuto výsledku podat žalobu u soudu, jejíž podání však nemá odkladný účinek pravomocného rozhodnutí.

Přehled rozkladů v období let 2006 – 2008

rok	Dosud nerozhodnuto	Vyhověno rozkladu	Rozklad zamítnut	zastaveno	celkem
2006	0	59	86	0	145
2007	0	17	36	1	54
2008	4	9	17	0	30
celkem	4	85	139	1	

Žaloby proti rozhodnutí ředitele NBÚ

	v jednání	zastaveno	vyhověno	zamítnuto	odmítnuto	celkem
Dle z.č.148/1998Sb. - Městský soud v Praze	7	14	12	40	5	78
Kasační stížnost – rozh. o zamítnutí žaloby - NSS Brno	5	2	3	7	0	17
Kasační stížnost NBÚ proti rozh. o vyhovění žalobě - NSS Brno	1	1	0	1	0	3
Žaloba dle 412/2005 Sb.- Městský soud v Praze	27	5	5	9	0	46
Kasační stížnost – 412/2005 Sb. - proti rozh. o zamítnutí žaloby – NSS Brno	2	0	0	2	0	4
Kasační stížnost NBÚ – 412/2005 Sb. - proti rozh. o vyhovění žalobě – NSS Brno	0	0	1	0	0	1
celkem	42	22	21	59	5	

Jak již bylo výše uvedeno k obecným zásadám bezpečnostního řízení, je toto řízení neveřejné. Vzhledem k citlivosti soustředěných osobních dat a údajů k žadateli byla jako nové speciální ustanovení včleněna do zákona povinnost mlčenlivosti

pro zaměstnance,[68] kteří řízení provádějí nebo se s nimi seznámili v souvislosti s ním. Dále je zákonem stanoveno, že údaje z bezpečnostního svazku lze používat pouze pro účely zákona a zproštění mlčenlivosti v této oblasti je možné jen na žádost orgánů činných v trestním řízení. Ochrana údajů na straně jedné a jednoznačně vymezená možnost jejich dalšího použití byla do zákona zapracována nově, a to opět na základě předchozích zkušeností a potřeby.

- bezpečnostní řízení – možnosti po vydání osvědčení
- po vydání osvědčení mohou v praxi nastat dvě varianty, kdy je prováděno další řízení a to :
  vydání osvědčení pro přístup k utajovaným informacím cizí moci,
  řízení o zrušení platnosti osvědčení

Pro vydání osvědčení pro přístup k utajovaným informacím cizí moci někdy bývá v praxi užíván pojem "certifikát pro cizí moc". Tato procedura je uplatňována v případě osob či podnikatelů, kteří mají mít přístup k utajovaným informacím cizí moci, tím jsou jmenovitě myšleny utajované informace NATO a WEU. Původně do této skupiny patřily ještě utajované informace Evropské unie, ale po zavedení nového vzoru osvědčení (česko-anglicko-francouzská verze textu) je pro přístup k utajovaným informacím EU postačující vlastní osvědčení bez dalšího. Osoba či podnikatel pro přístup k utajovaným informacím NATO a WEU musí disponovat odpovídajícím osvědčením pro přístup k utajovaným informacím cizí moci a toto je vydáváno Národním bezpečnostním úřadem na žádost. Národní bezpečnostní úřad po přezkoumání splnění podmínek u osoby či podnikatele a provedení některých úkonů řízení vydá požadované osvědčení pro cizí moc. V případě utajovaných informací NATO jsou vystavovány typy osvědčení – NATO CONFIDENTIAL, NATO SECRET, NATO COSMIC TOP SECRET a speciální skupina osvědčení pro skupinu utajovaných informací s označením ATOMAL. V případě osvědčení pro přístup k utajovaným

[68] § 124 odst. 4 z.č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů

informacím WEU – tzn. Západoevropské unie jsou vydávána osvědčení WEU CONFIDENTIAL, WEU SECRET, WEU FOCAL TOP SECRET. Pokud při provádění úkonů správní orgán zjistí, že podmínky nejsou u držitele osvědčení splněny, osvědčení pro cizí moc není vydáno a je zahájeno řízení o zrušení platnosti osvědčení.

5.9 ŘÍZENÍ O ZRUŠENÍ PLATNOSTI OSVĚDČENÍ

Řízení o zrušení platnosti osvědčení je v podstatě bezpečnostním řízením, které je zahajováno z moci úřední, a to na základě zjištění důvodné pochybnosti o splnění podmínek pro vydání osvědčení u osoby či podnikatele, který je držitelem osvědčení. Podnětem pro zahájení řízení tedy mohou být různé informace či zjištění při ověřování splnění podmínek[69] v době platnosti osvědčení či výsledek porovnání skutečného stavu věci s hlášenými údaji ze strany držitele osvědčení. Správní orgán za pomoci úkonů řízení ověřuje aktuální stav věci a posuzuje zda nevznikl stav, kdy držitel osvědčení přestal splňovat některou z podmínek stanovených zákonem pro vydání osvědčení. O zahájení řízení správní orgán informuje držitele osvědčení a současně odpovědnou osobu, na jejíž odpovědnosti je následně zvážit míru a rozsah přístupu k utajovaným informacím držitele osvědčení v době, kdy je prováděno řízení o zrušení platnosti osvědčení. Jakmile má správní orgán dostatečný rozsah podkladů pro posouzení stavu, posoudí zjištěné skutečnosti v jednotlivosti a souhrnu a vydá rozhodnutí ve věci. Pokud je zjištěno, že držitel splňuje zákonem stanovené podmínky, je vydáno rozhodnutí o zastavení řízení a celá věc je uzavřena. Pokud je však zjištěno, že držitel přestal splňovat některou z podmínek pro vydání osvědčení, je vydáno rozhodnutí o zrušení platnosti osvědčení. Rozhodnutí má stejnou formu jako rozhodnutí o nevydání osvědčení s tím, že nabývá právní moci převzetím, tedy platnost osvědčení je zrušena a jeho držitel má povinnost jej vrátit vydávajícímu správnímu orgánu. Uplatnění opravného prostředku je stejné jako v případě nevydání osvědčení, avšak s již uvedenou výjimkou, že podání opravného prostředku nemá odkladný účinek a osvědčení tedy pozbylo platnosti a osoba tak ztratila oprávnění přístupu k utajovaným informacím.

[69] § 110 odst. 1 z. č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů

Tato odlišnost má zcela jasné opodstatnění, neboť v případě žadatele o osvědčení nemá tato osoba přístup k utajovaným informacím, zatímco v případě zrušení platnosti osvědčení jde o osobu s přístupem, a v souladu se zásadami ochrany utajovaných informací je nezbytné zabránit přístupu k utajovaným informacím osobě, která nesplňuje podmínky stanovené zákonem.

5.10 ODLIŠNOSTI PRO ZPRAVODAJSKÉ SLUŽBY

Zpravodajské služby mají v oblasti bezpečnostního řízení dvě postavení. Vzhledem k zaměření této práce bude pozornost věnována postavení zpravodajské služby jako správního orgánu oprávněného k provádění bezpečnostních řízení a to u vybrané kategorie osob, jmenovitě příslušníků a zaměstnanců zpravodajských služeb a uchazečů o přijetí do služebního či zaměstnaneckého poměru u těchto složek.[70] Stejné postavení má i ministerstvo vnitra České republiky, a to v případě přísluníků policie vybraných v zájmu plnění závažných úkolů policie ministrem vnitra.[71] V praxi toto ustanovení znamená, že personální bezpečnost v oblasti ochrany utajovaných informací spadá plně do kompetence dané zpravodajské služby a tato má postavení Národního bezpečnostního úřadu v uvedené oblasti ochrany utajovaných informací. Vzhledem k specifickým činnostem zpravodajských služeb bylo do zákona vtěleno několik odlišností, které zpravodajské služby při provádění bezpečnostních řízení uplatňují. Podíváme-li se detailně na tyto odlišnosti zjistíme, že jdou v podstatě nad rámec úkonů řízení a lze konstatovat, že jsou určitým zpřísněním celé procedury.

Jedná se o oblast posouzení osobnostní způsobilosti žadatele.[72] kdy je tato podmínka posuzována prohlášením žadatele nebo psychologickým vyšetřením psychologického pracoviště zpravodajské služby a v případě žádosti o vydání osvědčení

[70] § 140 z.č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů
[71] § 141 z.č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů
[72] § 13 z.č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů

na stupeň utajení Přísně tajné je osobnostní způsobilost ověřována na základě psychologického vyšetření.

Druhou oblastí je posuzování bezpečnostní spolehlivosti, kde je zpravodajským službám umožněno při posuzování bezpečnostního rizika provést fyziodetekční vyšetření, pokud zjištěné skutečnosti vyvolávají pochybnosti o schopnosti osoby utajovat informace.[73] Toto ustanovení je z hlediska použití fyziodetekčního vyšetření [74] ve zpravodajských službách průlomové, neboť dosavadní zákonné normy upravující činnost a postavení zpravodajských služeb tuto možnost neznaly. O přínosu použití tohoto druhu vyšetření v oblasti zpravodajských služeb je vedena stálá diskuse a je otázkou, nakolik se v českém prostředí osvědčí. Existuje řada států, kde je tato metoda, zejména v prostředí zpravodajských služeb, hojně využívána, např. USA, Kanada,[75] avšak ve většině případů je brána pouze jako podpůrný prostředek pro ověření informací.

5.11 PROBLÉMY APLIKACE " BEZPEČNOSTNÍHO ŘÍZENÍ" V PROSTŘEDÍ ZPRAVODAJSKÝCH SLUŽEB

Přesun prověřování osoby do systému určitého typu správního řízení, tak jak jej definuje zákon a vymezení postavení zpravodajské služby jako správního orgánu přineslo na jedné straně "unifikaci" bezpečnostních řízení prováděných různými subjekty, ale na straně druhé velice zúžilo prostor zpravodajským službám při prověřování, pro ochranu identit osob, které jsou jejími příslušníky, zaměstnanci nebo se o práci ve zpravodajských službách ucházejí. V případě osob, u kterých je příslušnost ke zpravodajské službě utajovanou informací, je pak provedení bezpečnostního řízení tak jak jej stanoví zákon, téměř nerealizovatelné. Důvody daného stavu vyplývají ze skutečnosti, kdy vzhledem k existenci jednotného posuzování utajovaných informací jsou dány jednotné podmínky pro přístup, a z toho vyplývají i jednotné postupy

[73] § 14 odst. 7 z.č. 412/2005 Sb.
[74] J. Kohout - Fyziodetekční vyšetření v procesu objasňování trestné činnosti, Kriminalistika 3/2008, Kriminalistický ústav Praha
[75] např. www.csis.gc.ca

a procedury včetně bezpečnostního řízení. Pro potřeby zpravodajských služeb by bylo pravděpodobně vhodnější do zákona vtělit odkaz na samostatnou právní normu řešící oblast personální bezpečnosti, popř. i některé další problematické otázky z oblasti ochrany utajovaných informací tak, aby ochrana utajovaných informací byla zajištěna minimálně v rozsahu stanoveném zákonem, a na druhé straně byla zohledněna odlišnost činností a ochrana citlivých údajů zpravodajské služby v dostatečném rozsahu.

6 PRAKTICKÉ PROBLÉMY REŽIMU UTAJOVANÝCH INFORMACÍ V ČR

Na základě údajů obsažených v pramenech, z nichž čerpala tato práce,[76] lze oblast problémů režimu utajovaných informací vymezit na dva hlavní okruhy. První okruh je otázka aplikace zákona v praxi z pohledu dodržování zásad ochrany utajovaných informací a druhým je stav legislativní úpravy a její dopad na výkon činnosti zpravodajských služeb.

V obecné rovině, tedy ze stavu, který pokrývá oblast výkonu státního dozoru ze strany NBÚ, a to konkrétně z výsledků[77] zjištěných při prováděných kontrolách, lze shledat opakovaně stejné typy vyskytovaných nedostatků a pochybení při ochraně utajovaných informací. Obecně je to nestanovení stupně utajení utajované informace, neopodstatněné vyznačení stupně utajení na dokument, který utajovanou informaci neobsahoval, ztráta dokumentů obsahujících utajované informace, rozpory vnitřních předpisů s obecně platnými předpisy tzn. zákon a prováděcí předpisy, špatné nastavení systému, které neumožnilo zajistit ochranu utajovaných informací v plné míře. V jednotlivých oblastech ochrany utajovaných informací se objevují o následující nedostatky; personální bezpečnost - přístup k utajovaným informacím u osob, které nesplňovaly podmínky, neaktuálnost přehledů pracovních míst nebo funkcí,u kterých je nezbytný přístup k utajovaným informacím a vedení evidence osob s přístupem

[76] Zvláště Výroční zprávy NBÚ a zpravodajských služeb
[77] Výroční zprávy NBÚ r. 2006, 2007, 2008

k utajovaným informacím. U průmyslové bezpečnosti jsou nejčastější nedostatky ve zpracování bezpečnostní dokumentace, konkrétně provádění její průběžné aktualizace, nehlášení změn údajů v žádosti o vydání osvědčení podnikatele. Administrativní bezpečnost má nejčetněji zastoupeny nedostatky ve vedení evidence utajovaných dokumentů (nezaevidování utajovaných informací, chybné nebo neúplné zápisy, špatně prováděné opravy v administrativních pomůckách) a chybná manipulace s utajovanými dokumenty včetně neevidování pohybu utajovaných informací. V oblasti fyzické bezpečnosti byly shledány nedostatky ve zpracování projektu fyzické bezpečnosti, zejména nesoulad skutečného stavu s projektem, dále nesprávné nastavení opatření fyzické bezpečnosti, absence požadovaných technických prostředků při zajištění objektů a zabezpečených oblastí a nedostatečná úroveň opatření (nesplnění minimálních požadavků). Bezpečnost informačních systémů shledává obdobně jako předchozí oblasti rozpor mezi bezpečnostní dokumentací a skutečným stavem; nejsou dodržována stanovená režimová opatření, provoz informačního systému je v rozporu s certifikační zprávou a existují nedostatky ve správě uživatelských účtů informačního systému. U kryptografické ochrany bylo zjištěno nedodržování instalačních podmínek kryptografických prostředků, nedodržování režimových opatření na kryptografických pracovištích, nedostatky v označování kryptografického materiálu a nesplnění požadavků pro jeho ukládání. Tyto výše uvedené nedostatky se ve výsledcích kontrol státního dozoru stabilně opakují.

Podle údajů z výroční zprávy v r. 2008 bylo z celkového počtu kontrolovaných subjektů pouze 27% bez nedostatků. Toto zjištění je poměrně znepokojivé a dokladuje, že stav ochrany utajovaných informací je nezbytné zlepšit.

V uvedené oblastibylo z pohledu řešených přestupků, zjištěno, že projednávaných přestupků či podaných oznámení bylo v r. 2006 podáno celkem 118 oznámení o porušení zákona, 2007 – 107 oznámení, 2008 – 80 oznámení. V oblasti porušení ochrany utajovaných informací byl stav následující :

(PO – právnická osoba, FO – fyzická osoba)

oblast	FO /2006	FO/2007	FO/2008	PO/2006	PO/2007	PO/2008	celkem
Adm. bez	19	21	22	0	1	1	64
Info-syst.	14	12	4	-	0	-	30
Fyz.bez	1	2	2	1	-	1	7
Prům.bez	-	-	-	4	4	6	14
Pers.bez	30	36	26	-	-	-	92
Příst.neopr. osoby k UI	-	-	3	-	-	-	3
celkem	64	71	57	5	5	8	

Přestože se jedná o dílčí údaje je zřejmé, že nejčastější oblastí porušení ochrany utajovaných informací je personální bezpečnost, za ní následuje administrativní bezpečnost a bezpečnost informačních a komunikačních systémů. V roce 2008 také narostla celková částka udělených peněžitých pokut, což lze pravděpodobně přičítat již plné aplikaci zákona v praxi a z ní vyplývající zpřísnění (pro srovnání – r. 2006 – 32.000 Kč, r. 2007 – 77.500 Kč, r. 2008 - 135.500 Kč).

Z výše uvedených přehledů a čísel je zcela zřejmé, že hlavní podíl při porušení ochrany utajovaných informací mají fyzické osoby. Naprosto jednoznačně převládá problém rozporu mezi prováděnou praxí a právním předpisem, což vede k otázce zda je na vině skutečně pouze nedbalost, neznalost či neodpovědnost ze strany osob, které mají k utajovaným informacím přístup, nebo zda právní předpisy nepředstavují nadměrné zatížení při výkonu vlastní činnosti a jejich nepružnost a komplikovanost jsou vlastním důvodem jejich nedodržování.

Po zvážení daného stavu lze dojít k závěru, že příčiny jsou na obou uvedených stranách problému. Výběr osob pro přístup k utajovaným informacím ze strany odpovědné osoby nedosahuje odpovídajících kvalit. Úroveň odborných znalostí v oblasti ochrany utajovaných informací ze strany běžných uživatelů, tedy osob s přístupem k utajovaným informacím je stále velmi nízká. Oblast ochrany utajovaných informací není považována za "odbornost", kterou by pro výkon své běžné činnosti skutečně potřebovali a proto i zákonem stanovená pravidelná školení bývají v řadě organizací čistě formálním úkonem. Je poměrně častým jevem, že školení jsou prováděna společně pro všechny zaměstnance s přístupem k utajovaným informacím aniž by došlo k jejich rozdělení a zaměření školení k oblasti ochrany utajovaných informací, která je pro jejich výkon činnosti prioritní a měla by pro praxi skutečné využití.

Je paradoxem, že při vlastním výkonu činnosti je běžně uplatňován kariérní postup, v rámci něhož se průběžně posuzují a vyhodnocují schopnosti a výsledky, zatímco při stanovení úrovně přístupu k utajovaným informacím se bez znalosti a ověření schopností řádného nakládání s utajovanými informacemi dané osoby se tento postup téměř nezvažuje. Tímto je myšlena existence bezpečnostních zásad v rámci organizace ve smyslu, kdy přístup k utajované informaci vyššího stupně je umožněn až po určité době práce s utajovanými informacemi nižšího stupně. V předchozí právní úpravě se objevila snaha určitým způsobem, regulovat přístup k utajovaným skutečnostem u nejvyššího stupně; jednalo se omezení pro provedení bezpečnostní prověrky na stupeň Přísně tajné od věkové hranice 21 let žadatele. Nová právní úprava se však cestou regulace postupného přístupu k utajovaným informacím nevydala a ponechala vše na odpovědné osobě.

Pokud se jedná o problém složitosti právní úpravy je třeba konstatovat, že nová právní úprava je poměrně komplikovaná (z.č. 412/2005 Sb. má v porovnání s předchozím zákonem č. 148/1998 Sb. téměř dvojnásobný počer paragrafů) a lze říci, že je pro běžného uživatele i nepřehledná a těžce srozumitelná. Přidáme-li k tomu

prováděcí předpisy, a v řadě organizací pak vlastní interní normy, a již zmíněné často formální školení k právním předpisům z oblasti utajovaných informací, pak se nízké úrovni odborných znalostí u běžných uživatelů nelze podivovat.

Zcela transparentním příkladem je rozdíl v nakládání s utajovanou informací stupně Vyhrazené v prostředí české právní úpravy a zahraničí. Zde se česká varianta odlišuje ve všech oblastech ochrany utajovaných informací a to ve smyslu "přísnější ochrany" (nadbytečné ověřování splnění podmínek pro přístup k utajované informaci stupně Vyhrazené u fyzické osoby, bezpečnostní řízení u podnikatele pro stupeň Vyhrazené atd.). Vzhledem ke skutečnosti, že utajované informace stupně Vyhrazené tvoří velkou část z celkového počtu utajovaných informací, dostává se, touto právem kritizovanou disproporcí, celý systém ochrany utajovaných informací do nepříznivého hodnocení.

NBÚ si je této skutečnosti vědom, a proto se daný stav snaží průběžně narovnat. Jak již bylo dříve uvedeno, zák. č. 412/2005 Sb. prošel do současné doby již sedmi novelami a v současné době je připravena a ve výborech poslanecké sněmovny leží k projednání tzv. "Velká novela", která by měla zejména zjednoudšit a zpřehlednit právní úpravu ochrany utajovaných informací pro běžného občana – účastníka řízení – a napravit zjištěné nedostatky. V oblasti personální bezpečnosti se jedná zejména o snahu zkrátit lhůty stanovené pro provedení bezpečnostních, řízení a to u stupně Důvěrné na 2 měsíce, Tajné na 6 měsíců a Přísně tajné na 9 měsíců. Zúžit množství informací poskytovaných účastníkem řízení, které předkládá pro účely bezpečnostního řízení, a upřesnit rozsah hlášení změn údajů, rozšíření důvodů pro zastavení řízení, umožnit vyloučení neodůvodněně podávaných žádostí, zakotvit princip držení pouze jednoho osvědčení pro přístup k utajované informaci, možnost vrácení osvědčení a zavedení důvodu zániku platnosti v souvislosti s tímto vrácením, posílení pravomoci bezpečnostních ředitelů v oblasti regulace počtů žádostí a zavedení institutu schvalování přehledu míst nebo funkcí, na nichž je nezbytné mít přístup k utajované informaci.

Výše uvedené navrhované změny jsou s výjimkou posílení pravomoci bezpečnostního ředitele a možnosti omezení podávání neoprávněných žádostí pouze technikáliemi, které bezesporu přinesou větší komfort účastníkovi řízení, ale ke kvalitě vlastní procedury bezpečnostního řízení či zlepšení úrovně odborného vědomí v oblasti ochrany utajovaných informací téměř nepřispějí.

Na úseku průmyslové bezpečnosti je připravována změna zásadní, která pokud bude realizována, odstraní již zmiňovaný nepoměr mezi českou a zahraniční legislativou v oblasti stupně Vyhrazené, a to tím, že dojde ke zrušení ověřování podmínek přístupu podnikatelů k utajované informaci stupně Vyhrazené. Dále bude zrušena obecná podmínka držitelství osvědčení pro prokuristy, která nereflektovala skutečnou potřebu přístupu k utajované informaci. Stejně jako u personální bezpečnosti i zde se objevuje návrh na zkrácení lhůt pro bezpečnostní řízení podnikatele, a to u stupně utajení Tajné na 8 měsíců a Přísně tajné na 10 měsíců. Objevuje se opakovaně návrh na zpoplatnění bezpečnostního řízení podnikatele správním poplatkem ve výši 5.000,- Kč a 10.000,- Kč.

Novelou by mělo být taktéž stanoveno rozčlenění objektů pro zabezpečení ochrany utajovaných informací do kategorií a umožněno zpracování utajované informace v objektu příslušné kategorie bez toho, aby zde byla umístěna zabezpečená oblast příslušné kategorie.

Další disproporcí, která se stala zdrojem kritiky zahraničních partnerů a která je v určitém rozporu s minimálními bezpečnostními standardy Organizace Severoatlantické smlouvy a Evropské unie, je oblast přístupu osob bez prověření k utajovaným informacím.[78] Podle těchto standardů je přístup k utajovaným informacím determinován provedením bezpečnostní prověrky, kterou bylo ověřeno, že osoba splňuje podmínky pro přístup k utajovaným informacím. Nová právní úprava by měla

[78] § 57 zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů

zúžit okruh osob, které mohou mít přístup k utajovaným informacím, aniž by splňovaly podmínky stanovené zákonem proti původnímu z.č. 148/1998 Sb. Výsledný efekt je však zcela opačný, počet osob byl rozšířen (např. byla zrušena podmínka osvědčení pro členy kontrolních orgánů parlamentu podle zvláštních zákonů) a zatímco v předchozí úpravě byla obsažena alespoň dílčí povinnost o poučení osob, které se budou seznamovat s utajovanou skutečností, pak toto opatření ,u osob stanovených v § 58 odst. 1 z.č. 412/2005 Sb., v novém zákonu zcela chybí. Z hlediska systému ochrany utajovaných informací a mezinárodní výměny a spolupráce v této oblasti se jedná o velmi problematický a z odborného hlediska i neopodstatněný zásah do celého konceptu ochrany.

Zaměříme-li se na problémy zpravodajských služeb v oblasti režimu ochrany utajovaných informací, pak je třeba tyto rozdělit na dva okruhy, a to v souvislosti s úlohou či postavením, které zpravodajské služby v oblasti ochrany utajovaných informací mají. V prvé řadě jsou subjektem, který utajované informace získává a dále s nimi manipuluje, a tato jeho činnost je vymezena právními předpisy v oblasti ochrany utajovaných informací, s určitými výjimkami, jako pro každou jinou právnickou osobu. V druhé řadě jsou zpravodajské služby součástí systému ochrany utajovaných informací, a to zejména v oblasti provádění úkonů řízení pro potřeby NBÚ a ostatních oprávněných subjektů.

Pokud jde o oblast ochrany utajovaných informací v rámci zpravodajské služby, existují zde vedle sebe dva instituty povinnosti mlčenlivosti, a to jeden vyplývající ze zákona č. 412/2005 Sb. a druhý vyplývající ze zvláštních zákonů, které upravují působnost a oprávnění činnosti jednotlivých zpravodajských služeb. Řada problémů, které s aplikací zákonů v oblasti ochrany utajovaných informací ve zpravodajských službách byly, vznikla ze situace, kdy do relativně funkčních interních systémů zpravodajských služeb vstoupil v roce 1998, tedy v podstatě po 8 letech činnosti těchto složek, zákon na ochranu utajovaných skutečností. Obecnost právní úpravy, potíže

výkladu některých ustanovení zákona a prováděcích předpisů vyvolávala negativní reakce.

Mimo institutu povinnosti mlčenlivosti, který přinesl zákon na ochranu utajovaných skutečností, ve zpravodajských službách již dříve fungoval institu povinnosti obecné mlčenlivosti. Je třeba si uvědomit, že údaj naprosto běžný a neutajovaný pro jednu organizaci může v prostředí zpravodajské služby představovat informaci, kterou je nezbytné chránit stupněm utajení. Současně však není možné, aby všechny skutečnosti v rámci zpravodajských služeb spadaly do kategorie utajovaných informací, ať již vzhledem k nemožnosti naplnění všech zákonem stanovených atributů pro utajovanou informaci, tak z pohledu následně nutných opatření k zajištění ochrany utajovaných informací. Proto zde paralelně zůstává obecná povinnost mlčenlivosti. Pro přiblížení je vybrána definice ze zákona o Vojenském zpravodajství: "příslušníci Vojenského zpravodajství a každý kdo plní úkoly podle tohoto zákona, jsou povinni zachovávat mlčenlivost o skutečnostech se kterými se seznámili při plnění úkolů Vojenského zpravodajství nebo v souvislosti s nimi".[79] Obdobné omezení mají i ostatní zpravodajské služby, ale vzhledem k jeho obecnosti je velmi sporné prokazování jeho porušení a otázka případného postihu.

Předěl mezi tím, co je a co není ve zpravodajské službě utajovanou informací, je často velmi sporný a snaha ochránit činnost cestou stanovení zvláštní povinnosti obecné mlčenlivosti se nejeví jako optimální řešení.

Dalším sporným bodem je v oblasti personální bezpečnosti přesun od mechanismu bezpečnostní prověrky do systému bezpečnostního řízení, které je v podstatě upraveným typem správního řízení. Zpravodajské služby zde mají minimální výjimky a "zprůhlednění" procedury, které je v případě běžného žadatele pozitivem, může přinášet zpravodajským službám nemalé komplikace v zejména oblasti ochrany identity příslušníků.

[79] § 25 zákon č. 289/2005 Sb., o vojenském zpravodajství

Obdobně nedořešeným bodem zůstala varianta přístupu osob jednajících ve prospěch služby k utajované informaci bez platného osvědčení. Zákon tuto možnost připouští,[80] ale současně stanoví podmínku provedení poučení, kterým se podle zákona rozumí písemný záznam o seznámení fyzické osoby s jejími právy a povinnostmi v oblasti ochrany utajovaných informací a s následky jejich porušení. Tato praxe je však, zejména v případě činnosti zpravodajské služby s vnější působností, jen velmi těžce aplikovatelná.

Další zmíněnou oblastí působení zpravodajských služeb na úseku ochrany utajovaných informací je jejich aktivní role při provádění bezpečnostních řízení a v rámci vlastní působnosti jednotlivých služeb i úloha při ochraně utajovaných informací. Nová právní úprava přinesla některá zlepšení v této oblasti a to zejména v rozsahu oprávnění při ověřování údajů. Na straně druhé představuje určitý problém lhůta stanovená pro provedení řízení, která zpravodajsku službu při provádění šetření limituje. Tento postup pak ve svém důsledku přenáší na zpravodajské služby úkol klást většího důraz na oblast následného ověřování splnění podmínek u držitelů osvědčení a osob, které mají přístup k utajovaným informacím.

Podíváme-li se na účel zřízení, působnost a vykonávané činnosti jakékoli zpravodajské služby vidíme zásadní odlišnost této instituce od běžných orgánů státní správy. Již v současné úpravě mají tyto organizace výjimky v personální bezpečnosti, zahraniční výměně infomací, vynětí z výkonu státního dozoru, v oblasti fyzické bezpečnosti se služby podílí na kontrole zabezpečení jednacích oblastí a pro své potřeby si toto provádí samostatně atd. Je otázkou do budoucna, zda cesta jednoho zákona s četnou řadou výjimek pro oblast zpravodajských služeb je skutečně tím nejvhodnějším řešením. Při hodnocení stavu se nelze ubránit úvaze o vyjmutí celé problematiky zpravodajských služeb z obecné právní úpravy ochrany utajovaných informací

[80] § 58 a §2 písm. i) zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů

a umožnění řešení ochrany utajovaných informací a zvláštní povinnosti obecné mlčenlivosti v rámci jednotlivých zákonů o zpravodajských službách.

7 ZÁVĚR

Téma utajovaných skutečností a dnes již utajovaných informací je širokým tématem, které bývá v dnešním všedním světě často prezentováno i sdělovacími prostředky, a to především ve spojitosti se státními záležitostmi. Ne vždy však bývají tyto informace nestranné. Ve velké většině případů se jedná o informace více či méně zavádějící sloužíci spíše k upoutání pozornosti. Průhlednost a srozumitelnost legislativy pak může napomoci lépe pochopit význam a důležitost institutu utajování a utajovaných informací.

Problémy režimu utajovaných informací můžeme dělit na dvě části. Praktické problémy aplikace zákona v praxi z pohledu zásad ochrany utajovaných informací, které vyplívají nejen z rozdílů aplikace zákona a dále pak stav legislativní úpravy a její nemalý dopad na výkon činnosti zpravodajských služeb. Obě zde citované části jsou důležitými body, které nelze podceňovat a ani opomíjet.

Težištěm práce pak byla nejen komparace legislativy minulé a současné, ale i analýza současného stavu, který není autorem této diplomové práce považován za zcela uspokojivý. Z těchto důvodů jsou zmíněny, nejen v poslední kapitole, možné problémy režimu utajovaných informací, ale i jejich případná možná řešení, která by v budoucnu mohla již zmiňované problémy řešit. Tímto došlo k naplnění cíle práce, která naznačuje cestu řešení již zmiňovaných problémů dotýkajících se nejen legislativy, ale i praxe s touto legislativou tvořící jeden nedílný celek. V současné době již déle než rok leží ve sněmovně novela zákona o ochraně utajovaných informací a bezpečnostní způsobilosti. Bohužel tato novela nenaplňuje jeden z hlavních cílů, a to zestručnění a zjednodušení současné platné právní úpravy. Přesto ale, že ji lze hodnotit

jako dobrou, nemá tato novela, díky současné politické situaci, velkou naději, aby se jí sněmovna zabývala a alespoň částečně tak mohly být řešeny některé i zde zmiňované problémy režimu utajovaných informací.

8 SEZNAM LITERATURY

1. **MAJEROVÁ, V. a MAJER, M.** *Empirický výzkum v sociologii venkova a zemědělství, část II.* Praha : Česká zemědělská univerzita, 2007. str. 274. ISBN: 978-80-213-1671-3. s. 180.

2. **Čarnecký, V.** *Ochrana utajovaných skutečností v českém právním řádu (Diplomová práce).* Praha : ČZU Praha, 2003.

3. *Transparency International - Česká republika, o.p.s.* [Online] http:// www.transparency.cz.

4. **JUDr. Ing. Svatošová, Helena.** Utajování versus základní práva a demokratické standardy včetně problematiky zbraní - Návrh zákona o ochraně. [Online] [Citace: 10. 9 2009.] http://www.transparency.cz/pdf/publikace/studieutajinfo-prosinec04.pdf.

5. *Vyhláška č. 523/2005 Sb., O bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor.*

6. *Vyhláška č. 526/2005 Sb. o stanovení vzorů používaných v oblasti průmyslové bezpečnosti a o seznamech písemností a jejich náležitostech nutných k ověření splnění podmínek pro vydání osvědčení podnikatele a o způsobu podání žádosti podnikatele.*

7. *Vyhláška č. 527/2005 Sb. o stanovení vzorů v oblasti personální bezpečnosti a bezpečnostní způsobilosti a o seznamech písemností přikládaných k žádosti o vydání osvědčení fyzické osoby a k žádosti o doklad o bezpečnostní způsobilosti fyzické osoby.*

8. *Zákon č. 40/1964 Sb., Občanský zákoník.*

9. *Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.*

10. *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.*

11. *Zákon č. 289/2005 Sb., O vojenském zpravodajství.*

12. Výroční zprávy NBÚ r. 2006, 2007, 2008. [Online] [Citace: 16. 11 2009.] http://www.nbu.cz.

13. *Zákon č. 231/1948 Sb., Na ochranu lidově demokratické republiky.*

14. *Zákon č. 50/1923 Sb., Národního shromáždění na ochranu republiky.*

15. *Zákon č. 140/1961 Sb., Trestní zákon.*

16. *Zákon č. 40/2009 Sb., Trestní zákoník.*

17. *Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací, ve znění nařízení vlády č. 240/2008 Sb.*

18. *Vyhláška č. 524/2005 Sb. o zajištění kryptografické ochrany utajovaných informací.*

19. *Vyhláška č. 525/2005 Sb. o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací.*

20. *Vyhláška č. 526/2005 Sb. o stanovení vzorů používaných v oblasti průmyslové bezpečnosti a o seznamech písemností a jejich náležitostech nutných k ověření splnění podmínek pro vydání osvědčení podnikatele a o způsobu podání žádosti podnikatele .*

21. *Vyhláška č. 527/2005 Sb. o stanovení vzorů v oblasti personální bezpečnosti a bezpečnostní způsobilosti a o seznamech písemností přikládaných k žádosti o vydání osvědčení fyzické osoby a k žádosti o doklad o bezpečnostní způsobilosti fyzické osoby.*

22. *Vyhláška č. 528/2005 Sb. o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008 Sb.*

23. *Vyhláška č. 529/2005 Sb. o administrativní bezpečnosti a o registrech utajovaných informací, ve znění vyhlášky č. 55/2008 Sb.*

24. *Národní bezpečnostní úřad.* [Online] [Citace: 24. 10 2009.] http://www.nbu.cz.

25. *ALEX - Historische Rechts- und Gesetzestexte.* [Online] http://alex.onb.ac.at.

26. *Česká asociace bezpečnostních manažerů.* [Online] http://www.cabm.cz.

27. *Canadian Security Intelligence Service.* [Online] http://www.csis.gc.ca.

28. *Úřad pro zahraniční styky a informace (ÚZSI).* [Online] http://www.uzsi.cz.

29. *Vojenské zpravodajství ČR.* [Online] http://www.vzcr.cz.

30. *Bezpečnostní informační služba ČR.* [Online] http://www.bis.cz.

31. *Ministerstvo vnitra ČR.* [Online] http://www.mvcr.cz.

32. *Fyziodetekční vyšetření v procesu objasňování trestné činnosti.* **Kohout, J.** Praha : Kriminalistický ústav, 2008, Sv. 3.

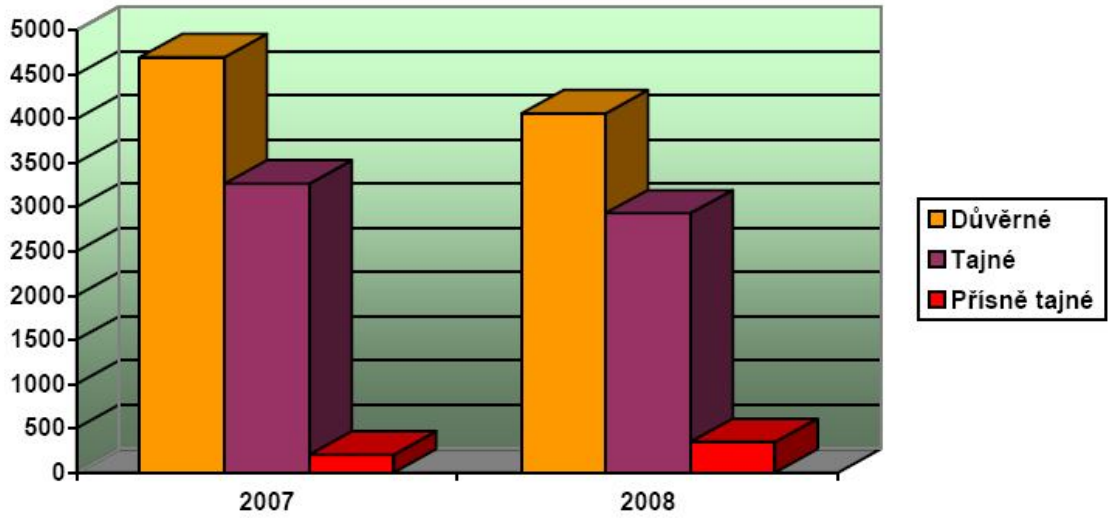
33. **Musil, R.** *Ochrana utajovaných skutečností.* Praha : Eurounion s. r. o., 2001. str.379. ISBN: 80-85858-93-2.

34. **Smejkal, V. a Rais, K.** *Řízení rizik ve firmách a jiných organizacích, 2. vydání.* Praha : Grada, 2006. str. 296. ISBN: 80-247-1667-4.

35. **Fryšar, M. a kolektiv.** *Bezpečnost pro manažery, podnikatele a politiky.* Praha : Public History, 2006. str. 176. ISBN: 80-86445-22-4.

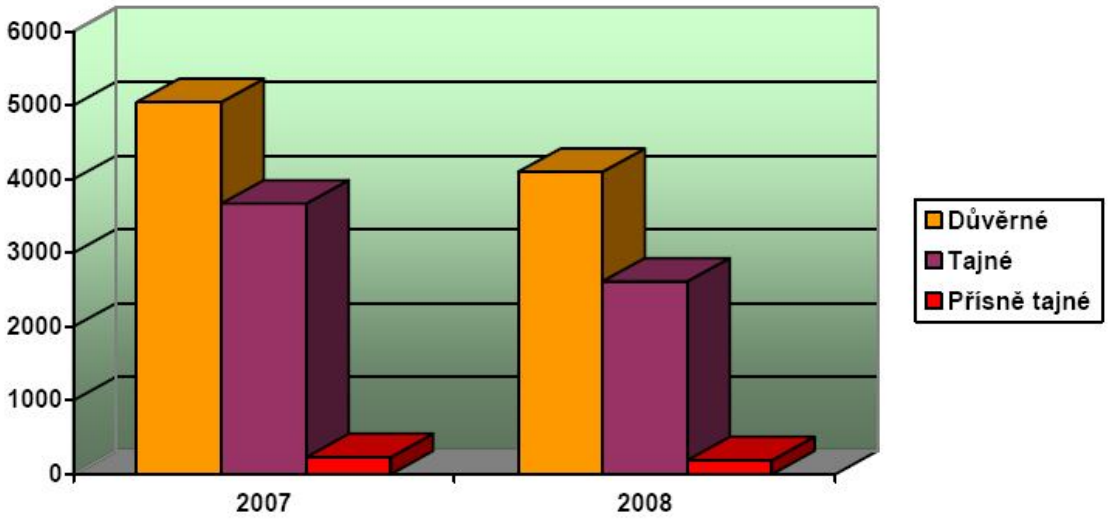
9 PŘÍLOHY

9.1 PRIJATÉ ŽÁDOSTI O VYDÁNÍ OSVEDCENÍ FYZICKÉ OSOBY 2007 A 2008



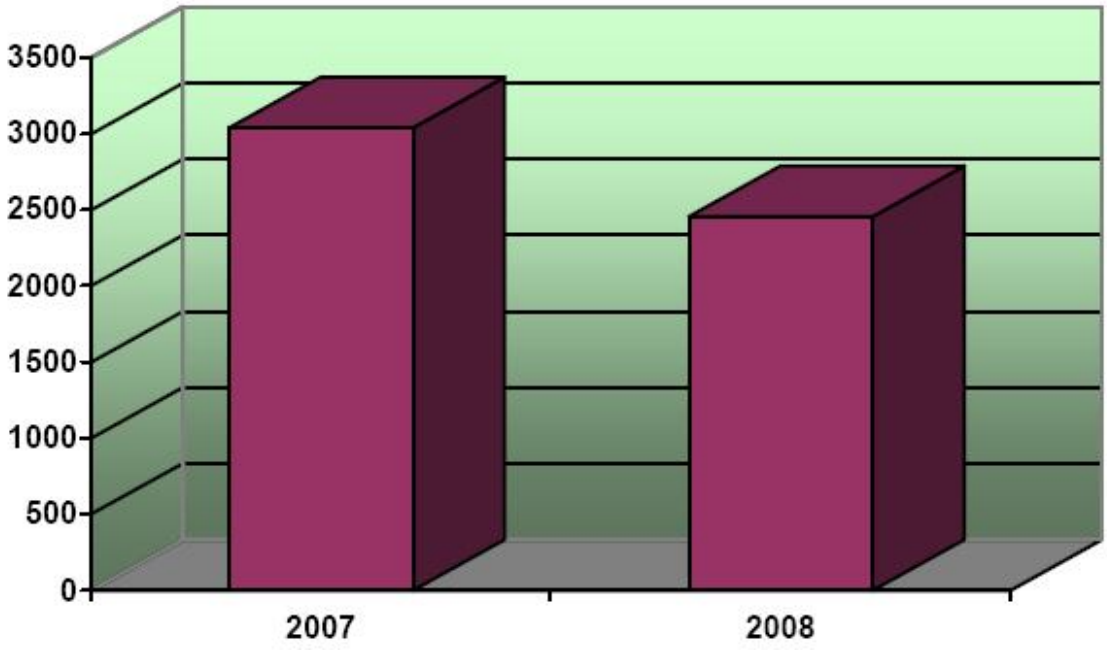
Zdroj: Zpráva o činnosti NBÚ za rok 2008

9.2 VYDANÁ OSVEDCENÍ FYZICKÉ OSOBY 2007 A 2008



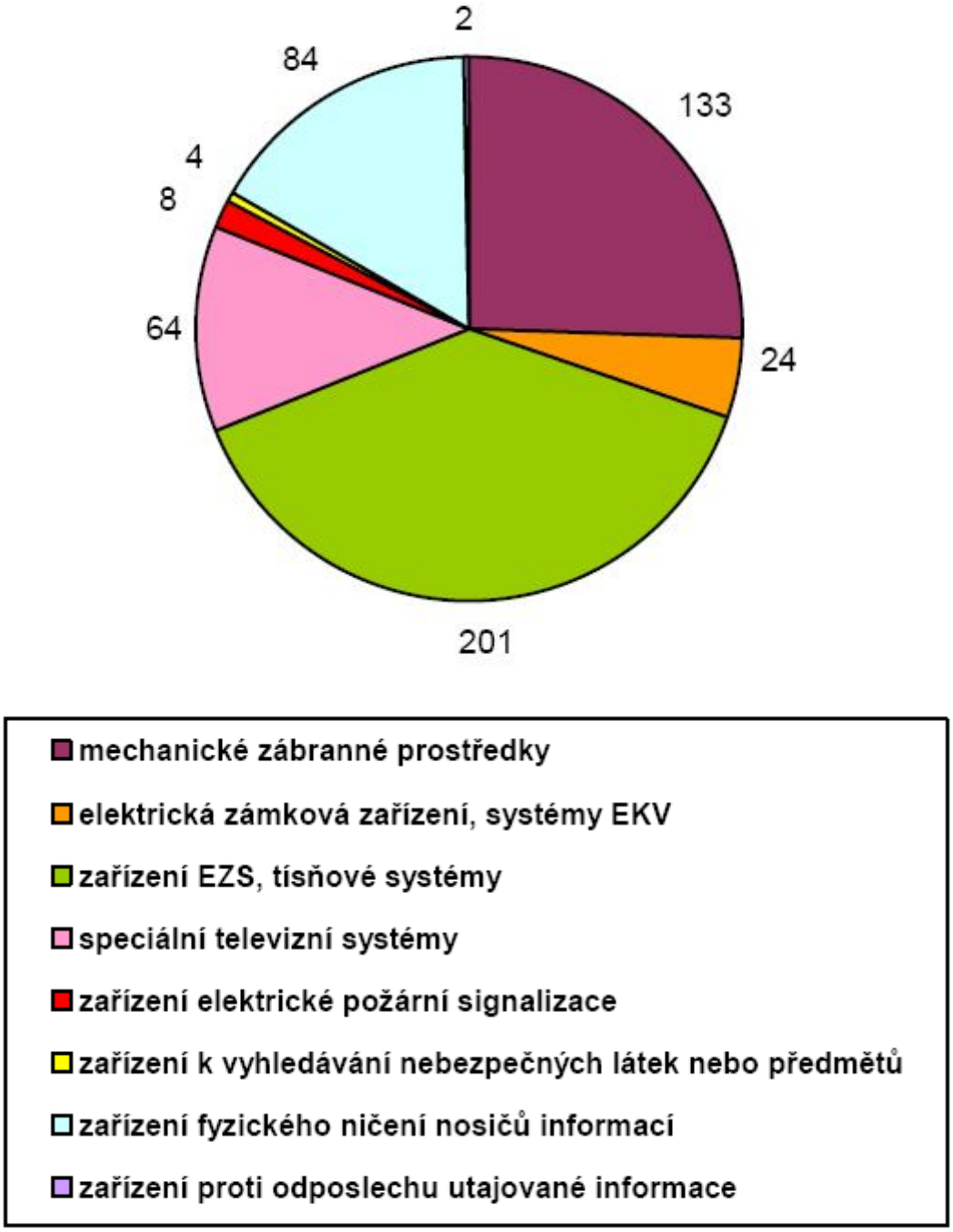
Zdroj: Zpráva o činnosti NBÚ za rok 2008

9.3 VYDANÁ OSVEDCENÍ FYZICKÉ OSOBY PRO CIZÍ MOC 2007 A 2008



Zdroj: Zpráva o činnosti NBÚ za rok 2008

9.4 VYDANÉ CERTIFIKÁTY TECHNICKÝCH PROSTŘEDKŮ V ROCE 2008



Zdroj: Zpráva o činnosti NBÚ za rok 2008