VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, Z. Ú., ČESKÉ BUDĚJOVICE

BAKALÁŘSKÁ PRÁCE

VÝKON STÁTNÍ SPRÁVY V OBLASTI OCHRANY UTAJOVANÝCH INFORMACÍ

Autor práce: Jaroslav Mach

Studijní obor: Bezpečnostně právní činnost ve veřejné správě

Forma studia: Kombinovaná

Vedoucí práce: doc. JUDr., PhDr. Jiří Bílý, CSc.

Katedra: Katedra právních oborů a bezpečnostních studií

2020

SKEN ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v seznamu použitých zdrojů.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce v elektronické podobě ve veřejně přístupné části infodisku VŠERS, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky vedoucího a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce systémem na odhalování plagiátů.

.....

Děkuji vedoucímu bakalářské práce doc. JUDr., PhDr. Jiřímu Bílému, CSc. za cenné rady, připomínky a metodické vedení práce.

ABSTRAKT

MACH, J. *Výkon státní správy v oblasti ochrany utajovaných informací: bakalářská práce.* České Budějovice : Vysoká škola evropských a regionálních studií, 2020. 54 s. Vedoucí bakalářské práce : doc. JUDr., PhDr. Jiří Bílý, CSc.

Klíčová slova: ochrana utajovaných informací, informační bezpečnost, státní správa, ústřední orgány

Bakalářská práce je zaměřena na výkon státní správy v oblasti ochrany utajovaných informací. V této souvislosti je podrobněji analyzována funkce Národního bezpečnostního úřadu, jako ústředního orgánu státní správy vykonávajícího tuto činnost. Následně jsou zmíněny i některé další orgány, které činnost Úřadu suplují či doplňují, nebo mají v této oblasti samostatnou působnost. Nechybí ani vysvětlení pojmu státní správy, která má nezbytnou úlohu při vytváření a fungování všech zmiňovaných orgánů, k čemuž využívá i patřičných právních instrumentů. Výsledkem je ucelený přehled pojednávající z vícera aspektů o dané problematice ochrany utajovaných informací a informační bezpečnosti.

ABSTRACT

MACH, J. *The Execution of state administration in the area of security of classified information: Bachelor Thesis.* České Budějovice : The College of European and Regional Studies, 2020. 54 p. Supervisor : doc. JUDr., PhDr. Jiří Bílý, CSc.

Key words: security of classified information, information security, state administration, central state authorities

This bachelor thesis deals with execution of state administration in the area of security of classified information. In this context, the function of the National Security Authority, as the central state administration body performing this activity, is analyzed in more detail. Then some other state agencies which substitute or complement activities of the National Security Authority or have their own activity in this area are mentioned. The bachelor thesis also defines concept of state administration which is a very important part in creating and functioning all government and state agencies by using of all appropriate law instruments. The result is a comprehensive overview involving more aspects of security of classified information and information security.

Obsah

Úvod

„Informace znamená všechno; za války jako v míru, v politice jako ve finanční sféře.“ — Stefan Zweig

Ne nadarmo se říká, že kdo má informace, má moc. Informace jsou totiž to, co často určuje i samotný ráz dějin. Umět a dokázat pracovat s informacemi je také součástí mnoha profesí dnešní doby, ať už se jedná o burzovní makléře či bezpečnostní analytiky, vědce nebo politiky. Právě kvůli velké záplavě informací, na které se nemalou měrou podílí již řadu let rozvoj internetu a informačních technologií, je kladen důraz i na jejich selekci a snahu o vytřídění těch důležitých od méně potřebných, a s tím spojenou bezpečnost při jejich nakládání.

V souvislosti se získáváním informací a závažnostmi, jež některé z nich obsahují, je potřeba zavádění nejrůznějších opatření, mezi která patří například platná a aktuální legislativa reflektující dění moderní doby, nebo zřizování zvláštních úřadů, které zajišťují spektrum nejrůznějších činností v této oblasti, včetně najímání specializovaných pracovníků a uskutečňování pravidelných školení, a to i pro širokou veřejnost. To má za následek hlubší proniknutí do uvedené problematiky, a to jak z hlediska normativního, tak technického, což obojí vede ke standardizaci postupů při plnění všech aktivit v této oblasti.

Pokud se v současné době hovoří o ochraně utajovaných informací, pak je poukazováno nejen na ochranu vnitřních potřeb státu, ale také na ochranu celku, který tvoří rozsáhlý komplex všech informací proudících mezi Českou republikou a jinými státy či organizacemi, se kterými Česká republika spolupracuje, a které je potřeba chránit před možným zneužitím. K tomu je nutná i patřičná právní úprava, bez které nelze předpokládat dostatečné zabezpečení a ochranu utajovaných informací, včetně výhod a nevýhod z toho plynoucích. Ztráta způsobená podceněním a nedostatečným zabezpečením této ochrany může v konečném důsledku způsobit subjektu, který s ní nakládal, nemalé škody. Na základě těchto důvodů je volba uvedeného tématu velmi aktuální, z čehož vyplývá i potřeba u příslušných subjektů pracujících s těmito informacemi mít aspoň základní povědomí o jejich ochraně a informačním zabezpečení.

1. Cíl a metodika bakalářské práce

Cílem práce je analyzovat a zhodnotit problematiku výkonu státní správy, která je spojena s ochranou utajovaných informací, a to jednak z pohledu ústředních orgánů vykonávajících předmětnou činnost, tak i z pohledu platné legislativy, která vymezuje konkrétní podobu všech prováděných činností a jejich specifikaci. Výsledkem analýzy je navrhnout některá legislativní opatření ke zlepšení výkonu státní správy v dané oblasti. Na základě toho jsou induktivním přístupem prezentovány jednotlivé kapitoly, které se zabývají příslušnými orgány a jejich činnostmi, a to především ve vztahu k zákonu o ochraně utajovaných informací a příslušným prováděcím právním předpisům. Rovněž je proveden rozbor informační bezpečnosti a její specifika, a to i ve vztahu k zabezpečení utajovaných informací.

Pro naplnění vytyčeného cíle bakalářské práce jsou v ní komparativní metodou shrnuta jednotlivá oprávnění a pravomoci orgánů, včetně dalších odlišností nebo podobností při prováděném výkonu jejich působnosti, což bylo i základní premisou při zpracování této práce.

2. Státní správa a její vymezení

Státní správa je součástí systému veřejné správy, kterou členíme na dva subsystémy, a to na státní správu a samosprávu, někdy též územní samosprávu. Z pohledu státní moci patří do moci výkonné (tj. realizuje výkonnou moc státu), která je zakotvena v hlavě třetí Ústavy České republiky[1]. Vykonávají ji orgány veřejné moci, kterými v případě *přímého*[2] výkonu státní správy jsou orgány státu jako vláda, ministerstva a další správní úřady, a při *nepřímém*[3] výkonu státní správy pak obecní nebo krajské úřady územních samosprávných celků (obcí, krajů), které vykonávají tuto činnost v přenesené působnosti. Územní samosprávu vymezuje hlava sedmá Ústavy České republiky, kde je v čl. 105 uvedeno, že *výkon státní správy lze svěřit orgánům samosprávy jen tehdy, stanoví-li to zákon*. Příkladem přenesené působnosti může být například povolování staveb ve stavebním řízení nebo vydávání občanských a řidičských průkazů. V tomto případě se hovoří o decentralizaci státní moci na veřejnoprávní korporace, které jsou zřizovány zákonem a jsou zároveň subjektem veřejného práva.

Státní správu je možné dále členit na *ústřední* a *územní*[4]. Ústřední státní správou jsou ministerstva a jiné ústřední správní úřady stanovené kompetenčním zákonem[5], které mají celostátní působnost. Výčet ministerstev je uveden v ust. § 1 kompetenčního zákona. Výčet ústředních správních úřadů pak v ust. § 2, mezi nimiž je uveden také Národní bezpečnostní úřad nebo Národní úřad pro kybernetickou a informační bezpečnost. Územní státní správou jsou pak územní správní úřady s působností na území správního obvodu, okresu nebo kraje. Jedná se například o finanční nebo katastrální úřad, popř. úřad práce či obvodní báňský úřad. Jednotlivé druhy úřadů, stejně jako další instituce nebo organizace vykonávající činnost státní správy, lze nalézt i ve veřeně dostupných zdrojích[6].

[1] Ústavní zákon č. 1/1993 Sb., Ústava České republiky, ve znění pozdějších ústavních zákonů
[2] BŘEŇ, J., Základní charakteristika státní správy. Praha: Institut pro veřejnou správu Praha, 2017. Skripta (Institut pro veřejnou správu), str. 40-41.
[3] Tamtéž, str. 40-41.
[4] Tamtéž, str. 39-40, str. 60.
[5] Zákon č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy České socialistické republiky, ve znění pozdějších předpisů
[6] *Adresář úřadů* [online]. Říčany: European Business Enterprise [cit. 2020-03-22]. Dostupné z: https://www.statnisprava.cz/rstsp/ciselniky.nsf/druhy_uradu

Státní správa může být rovněž vykonávána *vrchnostensky* a *nevrchnostensky*[7]. V prvním případě se jedná o vztahy nadřízenosti a podřízenosti, kdy státní orgán autoritativně vystupuje vůči ostatním adresátům (něco nařizuje, o něčem rozhoduje), čímž zasahuje do jejich právních poměrů. V druhém případě jde o rovnoprávný vztah, kdy je při zajišťování (obhospodařování) určitých veřejných potřeb vstupováno do různých soukromoprávních vztahů (např. přijímání zaměstnanců nebo nakládání se státním majetkem).

Státní správa je tedy veřejná správa uskutečňovaná státem, která má *výkonný*, *podzákonný* a *nařizovací* charakter, kdy výkonným charakterem je provádění (vykonávání) zákonů, podzákonným se rozumí činnost orgánů státní správy v mezích zákona (vázanost právními předpisy[8]) a nařizovacím pak uplatňování autority státních orgánů za pomoci různých mocenských nástrojů, které zajišťují vynutitelnost normativních správních aktů vůči jejich adresátům.

Z pohledu právních předpisů ovlivňujících výkon státní správy je pak možné zmínit např. zákon č. 82/1998 Sb., o odpovědnosti za škodu způsobenou při výkonu veřejné moci rozhodnutím nebo nesprávným úředním postupem a o změně zákona České národní rady č. 358/1992 Sb., o notářích a jejich činnosti (notářský řád), ve znění pozdějších předpisů. Dále pak např. zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, nebo zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů.

Jako kontrolní prvek státní správy, ale i územní samosprávy, slouží kromě k tomu určených kontrolních orgánů a jiných právních předpisů i zákon č. 106/1999Sb., o svobodném přístupu k informacím, který umožňuje veřejnosti získávat informace z výkonu činnosti těchto orgánů. Při jejich poskytování je ovšem brán zřetel na povahu těchto informací, a proto je v uvedeném zákonu striktně vymezeno v ust. § 7 *je-li požadovaná informace v souladu s právními předpisy označena za utajovanou informaci, k níž žadatel nemá oprávněný přístup, povinný subjekt ji neposkytne.* Tím je docíleno potřeby ochrany informací, jejichž vyzrazení by mohlo způsobit újmu státu.

[7] BŘEŇ, J., Základní charakteristika státní správy. Praha: Institut pro veřejnou správu Praha, 2017. Skripta (Institut pro veřejnou správu), str. 35.
[8] BŘEŇ, J., Základní charakteristika státní správy. Praha: Institut pro veřejnou správu Praha, 2017. Skripta (Institut pro veřejnou správu), str. 43.

3. Národní bezpečnostní úřad

Národní bezpečnostní úřad (dále jen „Úřad“) je institucí zřízenou podle zákona č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy České republiky, ve znění pozdějších předpisů (dále jen „kompetenční zákon“), kde je vymezen v ust. § 2 tohoto zákona. Při svém výkonu se řídí zásadami činnosti ústředních orgánů státní správy uvedenými v části třetí kompetenčního zákona, kde v ust. § 20 je mimo jiné konkretizováno, že *ministerstva a ostatní ústřední orgány státní správy plní v okruhu své působnosti úkoly stanovené v zákonech a v jiných obecně závazných právních předpisech*. Na Úřad se v tomto případě vztahuje především zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů (dále jen „zákon“), a k němu příslušné prováděcí právní předpisy. Úřad jako takový byl zřízen zákonem č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů, který byl nahrazen zákonem. Samotný zákon pak upravuje zásady pro stanovení informací jako informací utajovaných, podmínky pro přístup k nim a další požadavky na jejich ochranu, zásady pro stanovení citlivých činností a podmínky pro jejich výkon a s tím spojený výkon státní správy. Dále se na Úřad vztahuje také Ústavní zákon č. 1/1993 Sb., Ústava České republiky, ve znění pozdějších předpisů (dále jen „Ústava“), konkrétněji článek č. 79, který zajišťuje možnost zřídit správní úřad a stanovit jeho působnost i pravomoci. Ty jsou vymezeny v ust. § 137 zákona, případně v ust. § 138 tamtéž. Jednou z hlavních činností Úřadu je pak například zajišťovat bezpečnostní způsobilost subjektů a organizací pro styk s utajovanými informacemi[9] a ochrana těchto informací před jejich možným zneužitím.

[9] Utajovanou informací se dle definice v ust. § 2 písm. a) zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, rozumí „*informace v jakékoliv podobě zaznamenaná na jakémkoliv nosiči označená v souladu s tímto zákonem, jejíž vyzrazení nebo zneužití může způsobit újmu zájmu České republiky nebo může být pro tento zájem nevýhodné, a která je uvedena v seznamu utajovaných informací*“ (viz Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovanýchinformací).

3.1 Vydávání oznámení, osvědčení nebo dokladu

Jedním z primárních úkolů Úřadu je až na výjimky uvedené v ust. § 140 a § 141 zákona provádět činnosti v souvislosti se žádostmi fyzických osob a podnikatelů o vydání nebo obnovení osvědčení (ust. § 54 zákona). Obdobně provádí tyto činnosti u žádostí fyzických osob o vydání dokladu o bezpečnostní způsobilosti pro výkon citlivé činnosti[10] (dále jen „doklad“). Těmito činnostmi Úřadu se rozumí především vedení bezpečnostního řízení[11] (dále jen „řízení“), v němž se tyto žádosti[12] přezkoumávají. Rovněž je v gesci Úřadu vést řízení o zrušení osvědčení, a to pro všechny tři stupně utajení, tj. Důvěrné, Tajné a Přísně tajné. V omezené míře také rozhoduje o vydání oznámení o splnění podmínek pro přístup k utajované informaci stupně utajení Vyhrazené (dále jen „oznámení“). Jednotlivé stupně utajení (ust. § 4 zákona) jsou řazeny celkem do čtyř kategorií od nejnižšího stupně nebezpečí způsobení újmy z vyzrazení utajovaných skutečností po nejvyšší. K tomuto členění je přistupováno na základě požadavků, které se týkají seznamování osob s utajovanými skutečnostmi, resp. informacemi. Nejnižší stupeň závažnosti co do seznamování se s utajovanými informacemi je spojen s řízením pro stupeň utajení „*Vyhrazené*“. Se zvyšující se mírou závažnosti z ohrožení zájmu České republiky[13] jsou v pořadí další stupně utajení, a to „*Důvěrné*“, „*Tajné*“ a „*Přísně tajné*“. Následné udělení, obnovení nebo zrušení oznámení, osvědčení či dokladu se odvíjí od podmínek stanovených zákonem.

3.1.1 Podmínky pro vydání oznámení

Podmínky pro vydání oznámení fyzické osobě jsou uvedeny v ust. § 6 zákona. Kompetence kontrolovat splnění podmínek podle § 6 odst. 2 (svéprávnost, alespoň 18 let věku, bezúhonnost) a vydávat oznámení je ve většině případů vyhrazena odpovědné (nebo jí určené) osobě u subjektu, u kterého je fyzická osoba požadující vydání oznámení ve služebním, pracovním nebo jiném obdobném poměru stanoveném zákonem. Není-li odpovědné ani jinak určené osoby u subjektu, pak podmínky kontroluje odpovědná (nebo jí pověřená) osoba toho, kdo umožní fyzické osobě přístup

[10] Ustanovení § 80 až § 88 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů
[11] Tamtéž, ustanovení § 89 až § 135
[12] Tamtéž, ustanovení § 94, § 96 a § 99
[13] Tamtéž, ustanovení § 2 písm. b)

k utajovaným informacím. Ten pak oznámení také vydává. Teprve nelze-li splnit výše uvedené, rozhoduje o vydání oznámení Úřad, a to pouze na základě odůvodněné písemné žádosti. Výjimku zde tvoří podnikatel, který se potřebuje seznamovat s utajovanými informacemi stupně utajení Vyhrazené. Tomu postačí doložit písemné prohlášení (viz ust. § 15a zákona) o své schopnosti zabezpečit ochranu utajovaných informací, popř. mít platné osvědčení.

3.1.2 Podmínky pro vydání osvědčení

Podmínky pro vydání osvědčení fyzické osoby jsou oproti podmínkám pro vydání oznámení rozšířeny. Spadají do personální bezpečnosti[14] a jsou stanoveny v ust. § 12 odst. 1 zákona, které stanoví, že *osvědčení fyzické osoby Úřad vydá fyzické osobě, která je státním občanem České republiky nebo státním příslušníkem členského státu Evropské unie nebo Organizace Severoatlantické smlouvy, splňuje podmínky uvedené v § 6 odst. 2* (tj. svéprávnost, alespoň 18 let věku, bezúhonnost), *je osobnostně způsobilá a bezpečnostně spolehlivá*. Vydání takového osvědčení je garancí jistoty u držitele osvědčení ve vztahu k jeho vykonávané činnosti, kdy tím zároveň prokazuje, že splnil veškeré potřebné náležitosti vyplývající ze zákona pro jeho udělení. Toto osvědčení je rovněž možné uplatnit tam, kde je potřeba mít platné oznámení nebo doklad. Naproti tomu však platné oznámení nebo doklad není možné aplikovat pro případy, u kterých je nutné mít platné osvědčení.

Podmínky pro vydání osvědčení podnikatele[15] spadají prozměnu do průmyslové bezpečnosti[16] a jsou stanoveny v ust. § 16 odst. 1 zákona, které stanoví, že *osvědčení podnikatele Úřad vydá podnikateli, který je ekonomicky stabilní, bezpečnostně spolehlivý, je schopen zabezpečit ochranu utajovaných informací, pokud odpovědná osoba je držitelem platného osvědčení fyzické osoby nejméně pro takový stupeň utajení, pro který žádá podnikatel o vydání osvědčení podnikatele a který při podání žádosti o vydání osvědčení podnikatele uhradil správní poplatek podle jiného právního předpisu*.

[14] Ustanovení § 5 písm. a) a ust. § 6 až § 14 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů
[15] Zákonné vymezení podnikatele viz ust. § 420 až § 421 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů
[16] Ustanovení § 5 písm. b) a ust. § 15 až § 20 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů

Pro upřesnění písmene d) a e) tohoto ustanovení je vhodné podotknout, že u podnikatele není vyloučeno, aby za něj jednala jiná osoba. Proto je stanovena tato podmínka, kdy držitelem osvědčení pro stejný nebo nižší stupeň, o jehož udělení podnikatel žádá, je právě jeho odpovědná osoba[17]. Poslední bod tohoto ustanovení pak hovoří o uhrazení správního poplatku dle příslušného zákona o správních poplatcích[18], což však není podmínka, která by vylučovala seznamovat se s utajovanými informacemi nebo byla podnětem k zahájení řízení o odnětí (resp. zrušení) osvědčení[19].

Podmínky, za kterých bylo osvědčení vydáno, musí osoba splňovat po celou dobu platnosti vydaného osvědčení, což platí jak pro fyzickou osobu, tak pro podnikatele. Plnění podmínek v době platnosti osvědčení provádí Úřad v rámci úkonů řízení[20]. Platnost osvědčení stanovují jednotlivé lhůty, které jsou u stupně utajení „Důvěrné“ devět let, „Tajné“ sedm let a „Přísně tajné“ pět let (viz ust. § 55 zákona). Po uplynutí této doby je nutné zahájit nové řízení, ve kterém se bude rozhodovat o obnovení platnosti daného osvědčení. Zákon i v tomto případě stanovuje lhůty, ve kterých je účastník[21] řízení povinen podat žádost o vydání nového osvědčení. Termín pro podání žádosti před vypršením platnosti se liší u osvědčení vydaných pro fyzickou osobu a pro podnikatele a odvíjí se od jednotlivých stupňů utajení (viz ust. § 94 odst. 4 a § 96 odst. 4 zákona). Specifickým druhem osvědčení zůstává osvědčení fyzické osoby a podnikatele pro cizí moc (ust. § 57 zákona), které by mělo zlepšit přístupnost k utajovaným informacím u mezinárodních jednání. Cizí mocí se dle ust. § 2 písm. g) zákona rozumí cizí stát nebo jeho orgán anebo nadnárodní nebo mezinárodní organizace nebo její orgán. Podmínky pro vydání těchto osvědčení jsou však ve shodě s podmínkami pro vydání osvědčení pro fyzickou osobu nebo podnikatele, což je oboustranně výhodné. Uvedená osvědčení fyzické osoby i osvědčení podnikatele jsou veřejnými listinami[22].

Důležité je také zmínit, že dle ust. § 7 zákona č. 106/1999 Sb., o svobodném přístupu k informacím (kapitola. č. 2), *povinný subjekt neposkytne rovněž osobní údaje*

[17] Ustanovení § 2 písm. e) zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů
[18] Zákon č. 634/2004 Sb., o správních poplatcích, ve znění pozdějších předpisů
[19] Ustanovení § 101 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů
[20] Tamtéž, ustanovení § 107 až § 111
[21] Tamtéž, ustanovení § 92
[22] Ustanovení § 567 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů nebo ustanovení § 131 odst. 1 zák. č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů

o osobě, která je držitelem osvědčení fyzické osoby pro přístup k utajovaným informacím pro stupeň utajení Přísně tajné a Tajné, pokud by to mohlo ohrozit ochranu utajovaných informací. Je-li tedy dotaz směřován na osobu, která uvedené oprávnění vlastní, je potřeba postupovat obezřetně a vyvarovat se sdělení uvedených údajů.

3.1.3 Podmínky pro vydání dokladu

Podmínky pro vydání dokladu do jisté míry korespondují s podmínkami pro vydání osvědčení a jsou specifikovány v ust. § 81 zákona, které stanoví, že *doklad Úřad vydá fyzické osobě, která je plně svéprávná, dosáhla alespoň 18 let věku, je bezúhonná, osobnostně způsobilá a spolehlivá*. Vzor dokladu je stanoven v prováděcím právním předpisu[23]. Vydaný doklad je rovněž veřejnou listinou, a to s platností na dobu pěti let. Termín pro podání žádosti o obnovení (vydání nového) dokladu je stanoven v ust. § 99 odst. 4 zákona. Samotný doklad pak může v některých případech suplovat oznámení, ale oznámení již nemůže suplovat doklad. Plnění podmínek v době platnosti dokladu je kontrolováno shodně jako u osvědčení.

3.1.4 Zrušení osvědčení nebo dokladu

O zrušení osvědčení nebo dokladu ještě před vypršením jeho platnosti je vedeno řízení. Toto řízení se podle ust. § 101 zákona zahajuje v případě, kdy existují důvodné pochybnosti o tom, že držitel této veřejné listiny splňuje i nadále veškeré podmínky nutné pro vydání tohoto dokumentu. V případě potvrzení nastalé důvodné pochybnosti Úřad platnost takového dokumentu zruší. Postup v řízení o zrušení platnosti je obdobný jako u řízení o žádosti, nelze ho však až na výjimky přerušit (ust. § 112 zákona) ani zastavit (ust. § 113 zákona). Ukončení řízení se provede vydáním rozhodnutí[24] o zrušení osvědčení nebo dokladu, případně vydáním rozhodnutí o zastavení řízení na základě uvedených výjimek podle ust. § 113 písm. i) nebo j) zákona. Náležitosti samotného rozhodnutí pak stanovuje ust. § 122 zákona.

[23] Vyhláška č. 363/2011 Sb., o personální bezpečnosti a o bezpečnostní způsobilosti, ve znění pozdějších předpisů

[24] Ustanovení § 121 odst. 3 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů

3.2 **Kontrola a metodická činnost**

Má-li Úřad řádně zajišťovat ochranu utajovaných informací, musí provádět i kontrolní činnost u všech dotčených subjektů, na které se taková kontrola vztahuje. Oprávnění Úřadu provádět takové kontroly na dodržování patřičných předpisů je vymezeno v ust. § 137 písm. b) zákona s odkazem na příslušné ustanovení, kterým se kontrolní činnost řídí (tj. ust. § 143 zákona). Dotčenými subjekty jsou pak orgány státu, právnické osoby, podnikající fyzické osoby a fyzické osoby (dále jen „kontrolované osoby"), jak je uvedeno v ust. § 143 odst. 1. Dodržováním právních předpisů v dané oblasti se pak rozumí zejména postup v souladu se zákonem nebo s jednotlivými vyhláškami, např. vyhláškou č. 363/2011 Sb., o personální bezpečnosti a o bezpečnostní způsobilosti, vyhláškou č. 405/2011 Sb., o průmyslové bezpečnosti, vyhláškou č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, nebo vyhláškou č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací. Samotná kontrola se provádí podle zákona č. 255/2012 Sb., o kontrole (kontrolní řád), ve znění zákona č. 183/2017 Sb., nestanoví-li zákon jinak. Jak je z tohoto ustanovení § 143 odst. 2 zákona patrné, využívá zákon pro provádění potřebných úkonů subsidiarity kontrolního řádu. Ten kromě postupu orgánů moci výkonné, které vykonávají předmětnou činnost v sektoru veřejné správy, stanovuje rovněž cíl prováděné kontroly vůči určité osobě a také její celkový průběh. Pracovníci Úřadu provádějící kontrolu[25] (dále jen „kontrolní pracovníci") se obeznamují s utajovanými informacemi v rámci prováděné kontroly pouze v případě, že mají pro požadovaný stupeň utajení platné osvědčení. Neprokáží-li se kontrolní pracovníci tímto osvědčením, se kterým by splňovali podmínky podle ust. § 11 zákona, nebude jim umožněno kontrolu provést, a to ani pro stupeň utajení Vyhrazené[26]. Seznam utajovaných informací pak stanovuje nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací, ve znění pozdějších předpisů.

[25] Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, vymezuje pro své potřeby takové zaměstnance jako „kontrolní pracovníky", ovšem kontrolní řád je vymezuje jako „kontrolující". Kontrolní pracovníci jsou tak užším pojmem než kontrolující.

[26] Osvědčení pro stupeň utajení Vyhrazené neexistuje, avšak pro provedení kontroly u jakéhokoli stupně utajení je vyžadováno platné osvědčení.

Kontroly se může rovněž za splnění určitých podmínek účastnit úřad cizí moci[27], konkrétněji u kontrol týkajících se ochrany utajovaných informací, které byly od takového orgánu České republice poskytnuty, a vyplývá-li to současně z ratifikovaných mezinárodních dohod, kterými je Česká republika vázána.

Jedná-li se o kontrolu ochrany utajovaných informací spadající podle zákona do výkonu působnosti Národního úřadu pro kybernetickou a informační bezpečnost, je podmínkou takové kontroly přizvání jeho zástupce. Pod kontrolu Úřadu naopak nespadají činnosti, které vykonávají zpravodajské služby a také Ministerstvo vnitra v případech uvedených v ust. § 141 zákona (jinak kontrola Úřadu vyloučena není).

Metodickou činnost provádí jednotlivé odbory Úřadu, které zajišťují vydávání metodických pokynů pro danou oblast své správy, někdy i ve spolupráci s věcně příslušnými organizačními celky Úřadu.

3.3 **Plnění závazků z mezinárodních dohod**

V již zmíněném ust. § 20 kompetenčního zákona (kapitola č. 3) se dále uvádí, že ministerstva a ostatní ústřední orgány státní správy plní v okruhu své působnosti také *úkoly vyplývající z členství České republiky v Evropské unii a v ostatních integračních seskupeních a mezinárodních organizacích, pokud jsou pro Českou republiku závazné*. Mezinárodní smlouvy, kterými je Česká republika vázána, jsou vyhlašovány ve sbírce mezinárodních smluv sdělením Ministerstva zahraničních věcí České republiky (dále jen „Ministerstvo zahraničí“). Konkrétní postup pak uvádí příslušný zákon č. 309/1999 Sb., o Sbírce zákonů a o Sbírce mezinárodních smluv, ve znění pozdějších předpisů. Předpisy Evropské Unie jsou naproti tomu vyhlašovány v Úředním věstníku Evropské unie, například rozhodnutí rady ze dne 23. září 2013 o bezpečnostních pravidlech na ochranu utajovaných informací EU (2013/488/EU). Závazkem může být třeba plnění dohody v rámci účasti úřadu cizí moci při provádění kontroly (viz kapitola 3.2).

[27] Definice cizí moci je vymezena v ust. § 2 písm. g) zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů

3.4 Poskytování utajovaných informací v mezinárodním styku

Poskytování utajovaných informací v mezinárodním styku je vymezeno v ust. § 73 až § 79 zákona. Tím je zajištěn dohled Úřadu nad poskytovanými utajovanými informacemi u mezinárodních jednání. Podmínky pro poskytnutí těchto informací konkretizuje ust. § 73 zákona, kde je v písm. a) i b) uvedeno o jaký stupeň utajení se u poskytované informace jedná a na základě jaké žádosti a s jakým povolením nebo souhlasem může být poskytnuta. Odlišnost mezi písmeny a) a b) uvedeného ustanovení spočívá především ve stupních utajení Důvěrné, Tajné a Přísně tajné u písm. a) a stupně utajení Vyhrazené u písm. b), přičemž v prvním případě vydává Úřad písemné povolení[28], ve druhém písemný souhlas[29], a to pouze v případě, že tento úkon nenáleží do správy žádnému jinému ústřednímu správnímu úřadu, nebo takový úřad nelze určit. Poskytnutí utajované informace je zároveň vázáno na ust. § 74 zákona, které vymezuje, kdy není splnění podmínek dle ust. § 73 vyžadováno. Z toho například vyplývá, že u jednání mezi orgánem státu a cizí mocí lze poskytnout informaci u stupně utajení Vyhrazené i bez patřičného souhlasu[30]. Náležitosti u předmětné žádosti jsou pak uvedeny v ust. § 75 zákona, popřípadě v dalších ustanovení týkajících se poskytování utajovaných informací v mezinárodním styku, např. ust. § 21 odst. 2 nebo 3 zákona (vyznačování údajů a evidence utajované informace).

3.5 Ústřední registr a registry subjektů

Jednou z dalších činností Úřadu, kterou zabezpečuje odbor administrativní a fyzické bezpečnosti Úřadu, je zřízení a následné vedení ústředního registru utajovaných informací (dále jen „ústřední registr“). Tato činnost v zásadě navazuje na předchozí kapitolu o poskytování utajovaných informací v mezinárodním styku, jelikož právě v této souvislosti je ústřední registr zřizován. Zřízení registru je vymezeno v ust. § 79 odst. 2 zákona a jeho činnost upravuje vyhláška č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací, ve znění pozdějších předpisů (dále jen „vyhláška o administrativní bezpečnosti“). V ní je v ust. § 26 kupříkladu uvedeno, že se

[28] Ustanovení § 76 odst. 3 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů
[29] Tamtéž, ustanovení § 76 odst. 4
[30] Tamtéž, ustanovení § 74 odst. 2

ústřední registr člení na centrální spisovny, které jsou hlavním přijímacím a odbavovacím místem pro poskytování utajovaných dokumentů v mezinárodním styku pro stupně utajení Důvěrné, Tajné a Přísně tajné, dále vymezuje subjekty oprávněné k takovému styku a další podrobnosti k evidenci.

Registry zřizují za účelem získání přístupu k utajované informaci cizí moci mimo jiné i orgány státu, právnické osoby nebo podnikající fyzické osoby (ust. § 79 odst. 3 zákona a ust. § 27 vyhlášky o administrativní bezpečnosti). Toto zřízení registru však podléhá schválení Úřadu, který je na základě písemné žádosti od dotčeného subjektu oprávněn před vydáním souhlasu provést kontroly skutečností uvedených v podané žádosti, případně i dalších skutečností, které se zřízením registru souvisí. Úřad následně vede přehled zřízených registrů a zároveň provádí i kontrolu jejich činnosti[31]. V případě potřeby se ještě nabízí možnost zřízení pomocných registrů[32] nebo kontrolních bodů[33] (ust. § 79 odst. 4 zákona), k čemuž jsou oprávněny všechny subjekty. Úřadu musí být rovněž hlášeny veškeré změny, které subjekty ve svých registrech provedou. Následná komunikace při doručování utajovaných dokumentů Úřadu nebo od Úřadu k jednotlivým subjektům může probíhat jak písemně, tak elektronicky. V případě elektronické formy je nutno doručování zajistit skrze certifikované informační systémy. Seznam podnikatelů s takovými systémy je uveřejněn na internetových stránkách Úřadu v sekci Seznamy. Samotný seznam vymezuje název držitele certifikátu s jeho identifikačním číslem, pro jaký stupeň utajení mu byl certifikát vydán a rovněž datum platnosti takového certifikátu.

Evidence, kterou ústřední registr vede, by měla zahrnovat veškeré dokumenty obsahující utajované informace stupně utajení *Důvěrné, Tajné* a *Přísně tajné*, se kterými je manipulováno v mezinárodním styku, a zároveň by měly být i Úřadem doručovány, jak vyplývá z ust. § 77 odst. 1 zákona, pokud není stanoveno jinak[34].

Utajované informace stupně utajení Vyhrazené se v registrech neevidují. V případě přímého doručení dokumentu ze zahraničí místnímu subjektu, který má

[31] Ustanovení § 79 odst. 8 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů
[32] Ustanovení § 27a vyhlášky č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací, ve znění pozdějšívh předpisů
[33] Tamtéž, ustanovení § 27b
[34] Ustanovení § 77 odst. 2 až 5 nebo ust. § 78 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů

legálně zřízený registr, bez zaevidování dokumentu v ústředním registru, je nutné takový dokument do evidence doplnit. U stupně utajení Přísně tajné může registr poskytnout jinému registru utajovaný dokument pouze prostřednictvím ústředního registru (§ 27 odst. 8 vyhlášky o administrativní bezpečnosti). V ústředním registru je rovněž veden seznam zaměstnanců Úřadu, kterým je umožněn přístup k utajovaným informacím v mezinárodním styku. Obsah seznamu následně upravuje příslušné ustanovení[35].

3.6 Vydávání kurýrních listů a jejich přeprava

Samotná kurýrní přeprava není, až na výjimky, činností Úřadu, který takovou přepravu vykonává jen v odůvodněných případech. Činností Úřadu je však vydávání kurýrních listů[36] - protokolů určených pro mezinárodní přepravu utajovaných dokumentů. Výjimka je u utajovaných informací, pro které vede registr Ministerstvo zahraničí, jak je uvedeno v ust. § 78 odst. 1 zákona, jejichž přeprava se provádí na základě Vídeňské úmluvy o diplomatických stycích diplomatickou kurýrní poštou. V tomto případě se kurýrní listy nevydávají. Proces vydání kurýrního listu začíná přijetím písemné žádosti, kterou Úřadu zasílá odpovědná osoba nebo bezpečnostní ředitel daného subjektu. Vydaný kurýrní list pak slouží kurýrovi k prokázání oprávněnosti činit další úkony od vypravení dokumentu až po jeho doručení. Ten kromě kurýrního listu musí mít pro přepravu dokumentu i platné osvědčení[37] požadovaného stupně utajení (viz kapitola 3.1). Další podrobnosti upravuje ust. § 26 odst. 9 vyhlášky o administrativní bezpečnosti, které rovněž stanoví, že se při této přepravě postupuje obdobně jako u přepravy zásilky v ust. § 22 tamtéž.

[35] Ustanovení § 26 odst. 7 vyhlášky č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací, ve znění pozdějších předpisů
[36] Tamtéž, příloha č. 11
[37] Ustanovení § 54 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů

3.7 **Certifikace**

Certifikace je důležitým nástrojem k ochraně utajovaných informací. U druhů zajištění ochrany utajovaných informací vymezených v ust. § 5 zákona se vztahuje především k fyzické bezpečnosti (§ 24 až § 33), bezpečnosti informačních a komunikačních systémů (§ 34 až § 35a) nebo ke kryptografické ochraně (§ 37 až § 45). Zákon samotnou certifikaci vymezuje v ust. § 46 jako postup, jímž Úřad nebo Národní úřad pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) ověřují způsobilost technického prostředku k ochraně utajovaných informací, způsobilost informačního systému k nakládání s utajovanými informacemi, způsobilost kryptografického prostředku k ochraně utajovaných informací, způsobilost kryptografického pracoviště pro vykonávání činností podle ust. § 37 odst. 4 zákona nebo způsobilost stínicí komory k ochraně utajovaných informací. Z tohoto ustanovení rovněž vyplývá, kdy se způsobilostí zabývá Úřad a kdy NÚKIB, byť v ustanovení § 45a zákona je řečeno, že výkon státní správy v oblasti ochrany utajovaných informací podle hlavy deváté vykonává právě NÚKIB, nestanoví-li zákon jinak. Jedná se tedy o jednu z oblastí, pro kterou je NÚKIB ústředním správním úřadem, avšak nelze z tohoto ustanovení vyvozovat, že jediným úřadem, který tuto činnost vykonává. O tuto činnost se totiž dělí oba úřady. Více k certifikaci spadající do působnosti NÚKIB v kapitole č. 5.3.

Do procesu, který je prováděn v této oblasti Úřadem, se řadí ověřování způsobilosti technického prostředku[38]. V rámci Úřadu se jedná o činnost, kterou provádí buď sám a jejímž výsledkem je vydání vlastního posudku, nebo si nechá zpracovat posudek, o kterém uzavřel smlouvu o zajištění činnosti s orgánem státu nebo podnikatelem. Podmínky takové smlouvy jsou vymezeny v ust. § 52 zákona. Výsledný posudek je pak souhrnem vlastností technického prostředku, který slouží Úřadu jako podklad pro udělení či neudělení certifikátu. Charakteristika technických prostředků je uvedena v ust. § 30 zákona a jsou jimy například mechanické zábranné prostředky, speciální televizní systémy, tísňové systémy nebo zařízení elektrické požární signalizace. Vydaný certifikát technického prostředku je veřejnou listinou. Žádost o certifikaci technického prostředku a platnost certifikátu technického prostředku

[38] Ustanovení § 46 odst. 1 písm. a) zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů, vyplývající též z ustanovení § 46 odst. 14 tamtéž

konkretizuje ust. § 47 zákona, kde je například v odst. 1 vymezen žadatel[39] o certifikaci a povinná příloha, která se přikládá k žádosti. Přílohu jako takovou však dále nerozvádí. Obsahové náležitosti certifikátu pak uvádí ust. § 46 odst. 4 zákona. Úřad je rovněž zmocněn k vydání prováděcího právního předpisu (vyhlášky), který upravuje proces certifikace technického prostředku. V tomto případě se jedná o vyhlášku č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů (dále jen „vyhláška o fyzické bezpečnosti“), která například v ust. § 11 odst. 1 uvádí obsahové náležitosti u žádosti o certifikaci technického prostředku a v odst. 2 popisuje dokumentaci přikládanou k žádosti nebo v ust. § 15 obsahové náležitosti žádosti o uzavření smlouvy o zajištění činnosti.

3.8 Vydávání bezpečnostních standardů

Úřad je rovněž oprávněn vydávat bezpečnostní standardy, které charakterizuje zákon v ust. § 2 písm. j) jako *utajovaný soubor pravidel, ve kterém se stanoví postupy, technická řešení, bezpečnostní parametry a organizační opatření pro zajištění nejmenší možné míry ochrany utajovaných informací*. Tyto standardy musí splňovat celou definici podle zákona, jinak by nebyl zamýšlený účel zákonodárce naplněn. Jejich prostřednictvím jsou pak stanoveny například podmínky pro manipulaci s taktickou utajovanou informací, které zároveň souvisí s bezpečností informačních a komunikačních systémů a také s kryptografickou ochranou. Taktickou utajovanou informací je podle definice ust. § 35a odst. 1 zákona informace s krátkou dobou trvání důvodu utajení, jež se zpracovává v informačním nebo komunikačním systému a při přenosu se chrání kryptografickou ochranou, která je při takovém nakládání s utajovanou informací nezbytná (více kapitola č. 5.1 a 5.2). Stupeň utajení zde není nijak definován, a proto se může jednat o kterýkoliv zákonem vymezený stupeň. Výjimku tvoří ust. § 35a odst. 2, která se týká ochrany taktické informace do stupně utajení Tajné související s procesem vyhodnocení rizik, kdy požadované předpoklady pro manipulaci s taktickou informací opět upravuje bezpečnostní standard.

[39] Účastník řízení podle ust. § 46 odst. 19 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů

3.9 Ukládání správních trestů

Úřadu náleží pravomoc postihovat jednotlivé osoby nebo subjekty za nedodržení nebo porušení povinností, které pro ně ze zákona vyplývají. Tato kompetence je zanesena v ust. § 137 písm. i) zákona jako ukládání správních trestů. Ty jsou vymezeny v ust. § 148 až § 156 zákona, kde jsou uvedeny přestupky charakterizující jednotlivé správní delikty a také výši pokut, které je možné za ně udělit. Úřad tak má stejně jako jiné orgány státní správy možnost určité vymahatelnosti požadovaného jednání ze strany dotčených subjektů pod hrozbou sankcí, jelikož tyto subjekty nesou za své jednání v této oblasti plnou odpovědnost. Jednotlivé přestupky se pak člení podle toho, zda je spáchala fyzická osoba (§ 148), podnikající fyzická osoba či právnická osoba (§ 153) nebo podnikatel (§ 154 až § 155a), či zda došlo ke spáchání přestupku fyzickou osobou, která má přístup k utajované informaci (§ 149) nebo která je držitelem oznámení (§ 151), osvědčení (§ 150) nebo dokladu (§ 152).
Přestupky projednává ve většině případů Úřad, pouze v některých případech vymezených v ust. § 156 zákona NÚKIB. Pro výkon rozhodnutí se používá správní řád[40], jehož použití je vymezeno v ust. § 159 zákona.

Kromě sankcí za přestupky má Úřad ještě možnost ukládat pořádkové pokuty (ust. § 116 zákona). Ty se vztahují jednak na toho, kdo ztěžuje postup v řízení, a dále na orgán státu, právnickou osobu nebo podnikající fyzickou osobu za neposkytnutí informací, které Úřad od takového subjektu bezúplatně žádal pro potřeby řízení. Také v tomto případě se užije pro potřeby řízení o pořádkové pokutě správního řádu.

3.10 Vydávání věstníku

Úřad stejně jako některé jiné ústřední orgány státní správy vydává Věstník Úřadu[41]. Jedná se o materiál uveřejněný na internetových stránkách Úřadu[42], který slouží k tomu, aby byla dostatečně zajištěna informovanost široké veřejnosti, a tím i

[40] Zákon č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů
[41] Ustanovení § 137 písm. k) zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů
[42] *Věstník* [online]. Praha: Národní bezpečnostní úřad [cit. 2019-03-01]. Dostupné z: https://www.nbu.cz/cs/o-nas/985-vestnik/

všech subjektů majících k Úřadu relevantní vztah. Úřad tímto způsobem publikuje různá opatření, která přijal, aktuální seznamy subjektů[43], metodické pokyny či komentáře a stanoviska k novým právním předpisům v oblastech, kterými se při výkonu své působnosti zabývá. Vychází nejméně dvakrát ročně, a to na základě potřeb Úřadu.

3.11 **Ředitel Úřadu**

V čele Úřadu stojí ředitel[44], který jako jediný má rozhodovací pravomoci. Obdobně jsou například vedena ministerstva, kde je hlavní osobou s rozhodovacími pravomocemi ministr. Tento způsob fungování státní správy lze nazvat jako monokratický. Ředitele Úřadu jmenuje a odvolává vláda, která dle čl. 76 odst. 1 Ústavy rozhoduje ve sboru, a to na základě předchozího projednání této věci ve výboru Poslanecké sněmovny, který je příslušný zabývat se vnitřní a vnější bezpečností státu[45].

Odpovědný za výkon své funkce je ředitel Úřadu pouze předsedovi vlády, nebo jím pověřenému členovi vlády[46], který v odůvodněném případě může vládě navrhnout jeho odvolání. Samotné kompetence ředitele Úřadu jsou uvedeny v jednotlivých ustanoveních zákona. Ten může ze své funkce rozhodovat například o zproštění mlčenlivosti u zaniklého orgánu státu bez právního nástupce (§ 63 odst. 2 zákona), o přiměřeném prodloužení lhůty (§ 118 odst. 3 zákona), o zproštění mlčenlivosti zaměstnanců Úřadu provádějících řízení na základě žádosti orgánů činných v trestním řízení, dále rozhodovat o rozkladu podaném proti rozhodnutí Úřadu vydaném v řízení (§ 130 odst. 1 zákona), jmenovat a odvolávat členy rozkladové komise (§ 130 odst. 2 zákona) nebo rozhodovat o dalších úkonech v řízení o rozkladu charakterizovaných v ust. § 131 zákona. Ředitel má také určité povinnosti, které musí plnit, například při kontrole činnosti Úřadu (viz kapitola č. 4).

[43] Například seznam orgánů státu a podnikatelů s nimiž Úřad uzavřel smlouvu podle ust. § 52 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů

[44] Ustanovení § 136 odst. 2 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů

[45] *Výbor pro bezpečnost* [online]. Praha: Parlament České republiky, Poslanecká sněmovna [cit. 2019-03-01]. Dostupné z: https://www.psp.cz/sqw/hp.sqw?k=4900

[46] Ustanovení § 136 odst. 3 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů

3.12 Další oprávnění a povinnosti Úřadu

Zákon stanovuje v ust. § 138 další oprávnění a povinnosti Úřadu a NÚKIB, kterými se zákonodárce snaží vymezit celkovou působnost Úřadu. Pro Úřad tedy platí, že je oprávněn k některým dalším činnostem, jako je zpracování osobních údajů v rozsahu plnění úkolů podle zákona, vedení evidence porušení ochrany utajovaných informací a další evidence, požadovat bezplatné poskytnutí informace od určených subjektů, požadovat od policie a zpravodajských služeb informace, vyžadovat opis z evidence Rejstříku trestů, nahlížet do trestních spisů, uchovávat údaje získané v rámci plnění úkolů podle zákona, vedení evidence fyzických osob s platným osvědčením o zvláštní odborné způsobilosti, uzavírání smluv s orgánem státu nebo podnikatelem k provádění některých úkonů při certifikaci či spolupracovat s úřadem cizí moci.

4. Kontrola činnosti Národního bezpečnostního úřadu

Kontrolu činnosti Úřadu vymezuje ust. § 145 zákona a vykonává ho Poslanecká sněmovna, která pro tuto agendu zřizuje zvláštní kontrolní orgán (dále jen „kontrolní orgán“). Ten se skládá nejméně ze sedmi členů, přičemž podmínkou při stanovení počtu členů je, aby byl zastoupen každý poslanecký klub ustavený podle příslušnosti k politické straně nebo politickému hnutí, za něž poslanci kandidovali ve volbách. Počet členů je vždy lichý a členy mohou být pouze již zmínění poslanci. Na jednání kontrolního orgánu i na práva a povinnosti jeho členů se vztahuje zákon č. 90/1995 Sb., o jednacím řádu Poslanecké sněmovny, ve znění pozdějších předpisů, který zde plní subsidiární funkci obdobnou správnímu řádu u některých ustanovení zákona[47]. Vstup členů kontrolního orgánu do prostor Úřadu je možný pouze v doprovodu ředitele Úřadu nebo jím pověřeného pracovníka. Ten jim následně předkládá zprávy o činnosti Úřadu nebo o jednotlivých řízeních o žádosti[48], které Úřad vedl. Případně je také předkládán návrh rozpočtu Úřadu, podklady ke kontrole rozpočtu nebo vnitřní předpisy Úřadu. Kontrolní orgán však není způsobilý zasahovat do personálních pravomocí Úřadu nebo přebírat řízení Úřadu za příslušné vedoucí pracovníky. Má-li kontrolní orgán podezření, že činnost Úřadu není v souladu se zákonem, resp. i jinými zákony, může požadovat od ředitele Úřadu patřičné vysvětlení[49]. To se může týkat omezování práv a svobod občanů nebo vad v rámci vedených řízení. Každé zjištěné porušení zákona zaměstnancem Úřadu, které souvisí s výkonem jeho pracovní činnosti pro Úřad, je z povinnosti oznámeno řediteli Úřadu a předsedovi vlády[50].

[47] Použití správního řádu, ust. § 159 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů
[48] Tamtéž, ustanovení § 137 písm. a)
[49] Tamtéž, ustanovení § 146 odst. 1
[50] Tamtéž, ustanovení § 146 odst. 2

5. Národní úřad pro kybernetickou a informační bezpečnost

Národní úřad pro kybernetickou a informační bezpečnost (zkráceně NÚKIB) je dalším ústředním správním orgánem zřízeným podle ust. § 2 kompetenčního zákona. Vztahují se na něj tedy obdobné zásady činnosti správních orgánů jako na Úřad. NÚKIB se ovšem neřídí pouze zákonem[51] a k němu příslušnými prováděcími právními předpisy, ale také zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů (dál jen „zákon o kybernetické bezpečnosti“), a prováděcími právními předpisy, které k tomuto zákonu náleží. NÚKIB je instituce, která se vyčlenila z Úřadu a stala se ústředním správním úřadem, v jehož čele stojí stejně jako u Úřadu ředitel. Byl zřízen zákonem č. 205/2017 Sb., kterým byl novelizován zákon o kybernetické bezpečnosti. Jeho působnost je především v oblasti kybernetické ochrany České republiky, vydávání metodických pokynů a bezpečnostních standardů v této oblasti a zajišťování ochrany utajovaných informací proudících skrze informační a komunikační systémy. Výkon státní správy této instituce je uveden v ust. § 21a až § 22b zákona o kybernetické bezpečnosti, kde je v ust. § 22 vymezen souhrn jeho činností, obdobně jako je tomu v ust. § 137a zákona, případně v ust. § 138 tamtéž. K výkonu státní správy, kterou má v oblasti ochrany utajovaných informací NÚKIB, je však nutné se opět vrátit k zákonu. Ten uvádí především tři zásadní oblasti, kde tuto činnost NÚKIB provádí. Jedná se o bezpečnost informačních a komunikačních systémů (ust. § 33a až § 35a zákona), kryptografickou ochranu (ust. § 36a až § 45 zákona) a certifikaci (ust. § 45a až § 53 zákona). Zákon o kybernetické bezpečnosti se na tyto oblasti spojené s ochranou utajovaných informací nevztahuje, což je vymezeno v ust. § 1 odst. 3 tohoto zákona.

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

5.1 Bezpečnost informačních a komunikačních systémů

Bezpečnost informačních a komunikačních systémů je upravena v ust. § 33a až § 35a zákona a je dalším druhem zajištění ochrany utajovaných informací[52]. Jednotlivá ustanovení pak vymezují výkon státní správy v této oblasti a také charakteristiku a jiné náležitosti informačního systému (§ 34), komunikačního systému (§ 35) a manipulace s taktickou informací (§ 35a), která byla již zmíněna v souvislosti s bezpečnostními standardy v kapitole č. 3.8. Ustanovení § 5 písm. e) dále uvádí, co tvoří bezpečnost informačních a komunikačních systémů. Jedná se *o systém opatření, jejichž cílem je zajistit důvěrnost, integritu a dostupnost utajovaných informací, s nimiž tyto systémy nakládají, a odpovědnost správy a uživatele za jejich činnost v informačním nebo komunikačním systému*. Uvedená důvěrnost, integrita a dostupnost charakterizují tři koncepty bezpečnostní triády CIA[53] (anglicky Confidentiality, Integrity, and Availability), která má předejít například nechtěnému odhalení utajovaných informací nebo jejich zničení, což by v konečném důsledku mohlo znamenat ztrátu finančních prostředků subjektu nebo jeho nedůvěryhodnost a znemožnění dalších úkonů, které v této oblasti provádí. Kromě zákona se řídí bezpečnost informačních a komunikačních systémů také prováděcím právním předpisem, a to vyhláškou č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor, ve znění vyhlášky č. 453/2011 Sb. (dále jen „vyhláška o bezpečnosti informačních a komunikačních systémů“).

Bezpečnost informačních a komunikačních systémů zajišťuje odbor bezpečnosti informačních a komunikačních technologií. Ten dohlíží v případě bezpečnosti informačních systémů[54] například na platnou certifikaci informačního systému a na doložení písemného schválení uvedení takového systému do provozu (ust. § 34 odst. 2 zákona). V případě komunikačních systémů zase na posouzení zpracovaných projektů, které se týkají zabezpečení komunikačního systému[55], jež přichází do styku

[52] Podle ust. § 5 písm. e) zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů
[53] ROUSE, M. Confidentiality, integrity, and availability (CIA triad) [online]. Newton, Massachusetts: TechTarget, 2014 [cit. 2019-03-03]. Dostupné z: https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA
[54] Definice informačního systému v ust. § 34 odst. 1 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů
[55] Definice komunikačního systému v ust. § 35 odst. 1 tamtéž

s utajovanými informacemi. U komunikačních systémů však povinnost ohlašovat písemné schválení již není, jako je tomu u systémů informačních. Společné pro obě ustanovení, jak ust. § 34, tak ust. § 35 zákona, je zmínění o informačním nebo komunikačním systému podnikatele, který má přístup k utajované informaci stupně utajení Vyhrazené. Takový systém totiž může být schválen do provozu jen v době platnosti prohlášení podnikatele. Po skončení platnosti zaniká i schválení systému k jeho uvedení do provozu.

Manipulace s taktickou utajovanou informací je rozvedena v kapitole 3.8, avšak s ohledem k této podkapitole je vhodné zmínit vyhlášku o bezpečnosti informačních a komunikačních systémů, která v ust. § 16 odst. 3 mimo jiné zmiňuje, že u správce informačního systému, který vykonává funkci administrátora s právy úplného řízení sytému, a u bezpečnostního správce celého informačního systému malého rozsahu nebo s nízkým podílem zpracování utajovaných informací nejvyššího stupně utajení, v nichž se zpracovává pouze *taktická utajovaná informace*, může NÚKIB se zvážením identifikovaných rizik uznat jako dostačující splnění podmínek pro přístup fyzické osoby k utajované informaci na úrovni shodné s nejvyšším stupněm utajení utajovaných informací, se kterým může informační systém nakládat.

5.2 Kryptografická ochrana

Kryptografická ochrana je rozvedena v ustanovení § 36a až § 45 zákona. Řadí se mezi ostatní druhy zajištění ochrany utajovaných informací a je opět tím druhem ochrany, u kterého vykonává působnost v oblasti státní správy NÚKIB. Zákon ji v ust. § 5 písm. f) definuje jako *systém opatření na ochranu utajovaných informací použitím kryptografických metod a kryptografických materiálů při zpracování, přenosu nebo ukládání utajovaných informací*. Samotnou kryptografii lze zjednodušeně definovat jako nauku o šifrovacích metodách. Činnosti v této oblasti provádí odbor bezpečnosti informačních a komunikačních technologií, který se při plnění svých povinností řídí kromě zákona také prováděcími právními předpisy. V této oblasti se jedná především o dvě vyhlášky, a to vyhlášku č. 432/2011 Sb., o zajištění kryptografické ochrany utajovaných informací, ve znění vyhlášky č. 417/2013 Sb. (dále jen „vyhláška o zajištění kryptografické ochrany“), a vyhlášku č. 525/2005 Sb., o provádění certifikace

při zabezpečování kryptografické ochrany utajovaných informací, ve znění vyhlášky č. 434/2011 Sb. (dále jen „vyhláška o provádění certifikace“). Obdobně jako u certifikace uvedené v kapitole č. 3.7 nebo 5.3 je i zde možnost uzavření smlouvy o činnosti[56] s orgánem státu nebo podnikatelem. Náležitosti takové žádosti upravuje ust. § 6 vyhlášky o zajištění kryptografické ochrany a ust. § 11 vyhlášky o provádění certifikace (včetně obsahových náležitostí přikládané dokumentace). Tyto smlouvy se mohou uzavřít v rámci kryptografické ochrany z důvodů uvedených v ust. § 39 odst. 3 nebo ust. § 45 odst. 4 zákona. V těchto případech se jedná především o zajištění odborné zkoušky nebo její části a vydání osvědčení nebo o provedení měření možného úniku utajovaných informací u elektrických a elektronických zařízení, zabezpečené oblasti či objektu sloužícímu k ochraně takových informací.

S kryptografickou ochranou je neodlučitelně spjat také její výkon. Ten zajišťuje pracovník kryptografické ochrany, který je k výkonu takové ochrany pověřen odpovědnou nebo jí pověřenou osobou, je držitelem platného osvědčení fyzické osoby[57] a držitelem osvědčení o zvláštní odborné způsobilosti[58] v této oblasti (ust. § 38 odst. 2), přičemž všechny tyto podmínky musí být splněny současně. Samotným výkonem kryptografické ochrany se pak rozumí její bezpečnostní správa, speciální obsluha kryptografického prostředku nebo výroba či servis kryptografického prostředku nebo materiálu k zajištění jeho funkce (ust. § 38 odst. 1).

Kryptografická ochrana se ve svém zákonném výčtu dále zabývá manipulací (§ 41), přepravou (§42), kompromitací (§ 43), distribucí a evidencí (§ 43a) kryptografického materiálu. Tím je podle zákonné definice (viz ust. § 37 zákona) kryptografický prostředek, materiál k zajištění jeho funkce nebo kryptografický dokument. Tento prostředek, má-li sloužit k ochraně utajovaných informací, pak musí mít platný certifikát[59].

[56] Ustanovení § 52 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů, viz kapitola 3.7
[57] Tamtéž, ustanovení § 12 a § 54 odst. 2
[58] Tamtéž, ustanovení § 39
[59] Tamtéž, ustanovení § 46 odst. 1 písm. c)

V neposlední řadě jsou s kryptografickou ochranou spjata také kryptografická pracoviště a stínicí komory. Tyto pojmy jsou opět vymezeny zákonem. *Kryptografické pracoviště* (§ 37 odst. 3) jako pracoviště určené k výrobě nebo testování materiálu k zajištění funkce kryptografického prostředku, ukládání kryptografického materiálu nebo k distribuci a evidenci kryptografického materiálu nebo k výrobě a testování kryptografických prostředků. Rovněž musí splňovat bezpečnostní standardy a být do provozu schváleno. *Stínicí komorou* pak podle ust. § 32 odst. 1 vyhlášky o bezpečnosti informačních a komunikačních systémů je uzavřený stísněný prostor zabraňující šíření elektromagnetického, optického a akustického vyzařování mimo tento prostor. Také zde je využitelnost u obojího podmíněna platným certifikátem, jak vyplývá z ust. § 46 odst. 1 písm. d) a e) zákona.

Stínicí komory jsou spojeny především s kompromitujícím vyzařováním, na základě kterého by mohlo dojít k úniku utajovaných informací, jsou-li takové informace stínicí komorou chráněné (ust. § 45 zákona). Kompromitující vyzařování upravuje vyhláška o bezpečnosti informačních a komunikačních systémů, která definuje kompromitující vyzařování jako vyzařování elektrických a elektronických zařízení, které by mohlo způsobit únik utajované informace stupně utajení Důvěrné, Tajné nebo Přísně tajné[60]. Měření provádí Národní středisko pro měření kompromitujícího vyzařování, jehož činnost NÚKIB zajišťuje[61]. Kompromitací kryptografického materiálu je nutné rozumět takové nakládání s předmětným materiálem, které by způsobilo nebo mohlo způsobit porušení ochrany utajované informace[62].

NÚKIB je rovněž oprávněn pro kryptografická pracoviště nebo kryptografický materiál vydávat bezpečnostní standardy.

[60] Ustanovení § 29a vyhlášky č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor, ve znění vyhlášky č. 453/2011 Sb.
[61] Ustanovení § 137a písm. d) zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů
[62] Tamtéž, ustanovení § 43 odst. 1

5.3 Certifikace

Jak již bylo řečeno v kapitole 3.7, o tuto činnost se dělí oba úřady. Provádění certifikace u NÚKIB je svěřeno odboru bezpečnosti informačních a komunikačních technologií. V jeho gesci jsou pak činnosti uvedené v ust. § 46 odst. 1 písm. b) až e) zákona, což vyplývá z odst. 15 téhož ustanovení. V tomto případě jde o podstatně větší výčet, než jaký byl stanoven v této oblasti Úřadu. Zahrnuje ověření způsobilosti informačního systému k nakládání s utajovanými informacemi, způsobilosti kryptografického prostředku k ochraně utajovaných informací, způsobilosti kryptografického pracoviště pro vykonávání činností podle § 37 odst. 4 zákona, a způsobilosti stínicí komory k ochraně utajovaných informací. Společné obsahové náležitosti certifikátů zmiňuje ust. § 46 odst. 5 zákona, a zvláštní obsahové náležitosti odst. 6 až 9 citovaného ustanovení. Také zde platí, že jsou vydané certifikáty veřejnými listinami. V ust. § 46 odst. 13 zákona je ještě doplněna povinná příloha certifikátu, tj. certifikační zpráva, která obsahuje podmínky a zásady užívání takových certifikovaných systémů. Samotné žádosti o certifikaci pak konkretizují jednotlivá ustanovení, tj. u žádosti o certifikaci a platnost certifikátu informačního systému ust. § 48 zákona, u žádosti o certifikaci a platnost certifikátu kryptografického prostředku ust. § 49 zákona, u žádosti o certifikaci a platnost certifikátu kryptografického pracoviště ust. § 50 zákona a u žádosti o certifikaci a platnost certifikátu stínicí komory ust. § 51 zákona. Obsahové náležitosti takových žádostí opět upravují prováděcí právní předpisy. V tomto případě u certifikace informačních systémů a u stínicích komor vyhláška o bezpečnosti informačních a komunikačních systémů, konkrétněji ust. § 24 a ust. § 33 citované vyhlášky. U certifikace kryptografického prostředku a kryptografického pracoviště vyhláška o provádění certifikace, konkrétněji ust. § 1 a ust. § 2 citované vyhlášky. Obě vyhlášky rovněž stanovují i obsahové náležitosti žádosti orgánu státu nebo podnikatele o uzavření smlouvy o zajištění činnosti[63], a to vyhláška o bezpečnosti informačních a komunikačních systémů v ust. § 37 a vyhláška o provádění certifikace v ust. § 11. Tato smlouva je obvyklá u procesu certifikace, ale může být uzavřena i v rámci jiné činnosti, jak je uvedeno například v kapitole 5.2.

[63] Ustanovení § 52 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů, viz kapitola 3.7

5.4 Další oprávnění a povinnosti úřadu

Stejně jako u Úřadu i zde zákon v ust. § 138 vymezuje další oprávnění a povinnosti Úřadu a NÚKIB, kdy se zákonodárce snaží o další, v zásadě doplňující výklad kompetencí těchto správních úřadů. Pro NÚKIB pak platí, že je oprávněn k některým dalším činnostem, jako je zpracování osobních údajů v rozsahu plnění úkolů podle zákona, požadovat bezplatné poskytnutí informace od určených subjektů, uchovávání údajů získaných v rámci plnění úkolů podle zákona, vedení evidence fyzických osob s platným osvědčením o zvláštní odborné způsobilosti, uzavírání smluv s orgánem státu nebo podnikatelem k provádění některých úkonů při certifikaci systémů a kryptografických pracovišť, k provádění školení související s vykonáním zvláštní odborné způsobilosti nebo vést certifikační spis.

6. Zpravodajské služby

Činnost zpravodajských služeb je v rámci výkonu státní správy v oblasti ochrany utajovaných informací upravena v ust. § 140 zákona. Toto vymezení vlastní působnosti je nezbytné vzhledem k oblastem, v jakých zpravodajské služby působí, a také k činnostem, které provádějí. Mezi tyto činnosti se pak řadí nejen získávání informací, ale i jejich zabezpečení, které je upraveno zákonem. Mezi zpravodajské služby, které jsou charakterizovány v ustanovení § 3 zákona č. 153/1994 Sb., o zpravodajských službách České republiky (dále jen „zákon o zpravodajských službách"), se řadí Bezpečnostní informační služba, Úřad pro zahraniční styky a informace a Vojenské zpravodajství (dále jen „zpravodajské služby"). Tyto instituce se řídí také jinými právními předpisy, které se na ně přímo vztahují, jako je například zákon č. 154/1994 Sb., o Bezpečnostní informační službě, nebo zákon č. 289/2005 Sb., o Vojenském zpravodajství. Úřad pro zahraniční styky a informace se vlastním zákonem neřídí. Výkon jeho činnosti je však upraven v ust. § 17 a násl. zákona o zpravodajských službách. V jejich čele pak obdobně jako u Úřadu stojí ředitelé, jejichž jmenování a odvolání provádějí ty orgány, pod které daná zpravodajská služba spadá. Vždy je však nutný souhlas vlády, pokud ředitele přímo sama nejmenuje, jak vyplývá z ust. § 4 zákona o zpravodajských službách.

Vymezení všech oprávnění a povinností zpravodajských služeb v této oblasti charakterizuje zákon a jeho jednotlivá ustanovení. Hlavní z nich pak vymezuje již zmíněné ust. § 140 zákona. Zpravodajské služby tak například rozhodují o žádosti fyzické osoby o osvědčení u svých příslušníků, zaměstnanců a uchazečů o přijetí do služebního nebo pracovního poměru, s výjimkou těch, kteří jsou již držiteli platného osvědčení fyzické osoby pro požadovaný stupeň utajení a rozhodují o vydání takového osvědčení nebo o zrušení jeho platnosti. Rovněž provádějí na základě písemné žádosti Úřadu některé úkony řízení[64]. Z toho vyplývá, že zpravodajské služby nejen vedou řízení, ale vykonávají i úkony v řízení vedené Úřadem.

Při rozhodování o uvedených záležitostech mají zpravodajské služby postavení Úřadu a odpovědná osoba zpravodajské služby pak postavení ředitele Úřadu.

[64] Úkony řízení upravuje ust. § 107 až § 111 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů

Příslušnost k jednotlivým úkonům pak vyplývá z působnosti zpravodajských služeb, kterou upravuje ust. § 5 zákona o zpravodajských službách (ust. § 140 odst. 2 zákona). Mezi jejich další povinnosti se řadí především povinnost oznámit Úřadu zjištění okolností vedoucích k tomu, že držitel platného osvědčení nebo dokladu již nesplňuje veškeré podmínky pro jeho vydání[65]. Nesmí to však ohrozit zájem sledovaný zpravodajskou službou (ust. § 140 odst. 3 zákona).

Při zaměření se na další oprávnění zpravodajských služeb při plnění jejich úkolů v této oblasti (§ 140 odst. 4 zákona) se jedná především o právo používat prostředky k získávání informací podle zákona o zpravodajských službách, využívat údaje ze svých evidencí a evidencí Úřadu, které jim Úřad poskytne, požadovat a využívat údaje z dalších evidencí a materiálů, zpracovávat osobní údaje, vést evidence, požadovat poskytnutí informací od orgánu státu, právnické osoby nebo podnikající fyzické osoby, vyžadovat opis a výpis z evidence Rejstříku trestů nebo opis z evidence přestupků, uchovávat údaje získané v rámci plnění úkolů podle zákona, provádět opatření k ochraně osobních údajů vedených ve své evidenci a využívat údaje z evidence osob, kterým byl umožněn přístup k utajovaným informacím bez platného osvědčení[66].

Lze uvést i některé konkrétní výjimky vztahující se na zpravodajské služby. Jednou z nich je například ust. § 58 odst. 3 zákona, které pojednává o umožnění přístupu k utajovaným informacím fyzické osobě bez platného osvědčení, pakliže jedná ve prospěch zpravodajské služby[67]. Další výjimkou je, že zřízení registru pro evidenci utajovaných informací (viz kap. 2.5) nepodléhá u zpravodajských služeb schválení Úřadu (ust. § 79 odst. 3 zákona). Obdobně se pak neprovádí pomocí registru ani poskytování utajovaných informací mezi zpravodajskou službou a zpravodajskou službou cizí moci (ust. § 77 odst. 2 zákona). U kryptografické ochrany se výjimka týká například ověřování způsobilosti elektrických a elektronických zařízení, zabezpečené oblasti nebo objektu sloužícímu k ochraně utajovaných informací před kompromitujícím vyzařováním, jež jsou provozovány nebo užívány zpravodajskými službami, které si jejich ověřování provádí samy (ust. § 45 odst. 5 zákona).

[65] Prověřování provádí zpravodajská služba dle ust. § 110 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů
[66] Tyto osoby vymezuje ust. § 58 tamtéž
[67] Vymezení osoby jednající ve prospěch zpr. služby viz např. ust. § 15 odst. 2 zákona č. 154/1994 Sb., o bezpečnostní informační službě, ve znění pozdějších předpisů

S ohledem na výkon činnosti zpravodajských služeb je uvedeno v § 11 odst. 4 písm. c) zákona č. 106/1999Sb., o svobodném přístupu k informacím, že *povinné subjekty dále neposkytnou informace o plnění úkolů zpravodajských služeb, nebo o činnosti zpravodajských služeb, pokud by poskytnutí této informace ohrozilo plnění jejich úkolů či ochranu utajovaných informací*. Požadované informace se tak sdělí pouze v rozsahu, v jakém to stanoví zákon[68]. Tím se zamezí poskytnutí neoprávněnému subjektu, který by s nimi mohl dále nakládat ve svém vlastním zájmu, čímž by mohl poškodit zájmy České republiky.

[68] Ust. § 12 zákona č. 106/1999Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů

7. Ministerstvo vnitra a policie

Postup Ministerstva vnitra České republiky (dále jen „Ministerstvo vnitra“) nebo Policie České republiky (dále jen „policie“) při výkonu státní správy v oblasti ochrany utajovaných informací upravuje ust. § 141 zákona. To navazuje na potřebu zmíněných orgánů činit některé úkony v této oblasti ve vlastní působnosti, především u vedení řízení. Z pohledu Ministerstva vnitra se tak jedná o rozhodování o žádostech fyzických osob o osvědčení pro příslušníky policie, kteří plní závažné úkoly ministra vnitra, s výjimkou těch příslušníků, kteří již platné osvědčení fyzické osoby pro požadovaný stupeň utajení mají[69]. Dále pak rozhodování o vydání takového osvědčení a s tím související případné rozhodování o zrušení jeho platnosti. Ministerstvo vnitra má v tomto případě postavení Úřadu a ministr vnitra postavení ředitele Úřadu[70]. Policie jako taková řízení nevede, ale podílí se v rámci své působnosti na plnění úkolů Ministerstva vnitra nebo na základě písemné žádosti Úřadu provádí pro Úřad některé úkony v řízení[71]. Při plnění těchto úkolů je rovněž oprávněna využívat údaje z evidence osob, které mají přístup k utajovaným informacím bez platného osvědčení[72]. Zde je rozdíl oproti zpravodajským službám, které vykonávají obě tyto činnosti dělící se v tomto případě mezi Ministerstvo vnitra a policii.

7.1 Ministerstvo vnitra

Ministerstva vnitra má i další povinnosti a oprávnění, které mu plynou ze zákona. Jedná se o povinnosti uvedené v ust. § 141 odst. 3, tj. oznámit neprodleně Úřadu zjištěné okolnosti nasvědčující tomu, že držitel osvědčení nebo dokladu přestal splňovat podmínky pro jejich vydání[73], nebo provádět na žádost Úřadu opatření k evidenční ochraně osobních údajů držitele osvědčení a jeho rodiny. Dále má i určitá oprávnění potřebná k plnění úkolů[74], jako využívat údaje ze svých evidencí a evidencí Úřadu, které mu Úřad poskytne, zpracovávat osobní údaje, vést evidence, požadovat

[69] Ustanovení § 141 odst. 1 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů
[70] Tamtéž, ustanovení § 141 odst. 2
[71] Tamtéž, ustanovení § 141 odst. 5, jedná se o úkony uvedené v ust. § 107 až § 111 téhož zákona
[72] Tamtéž, ustanovení § 58, např. poslanci, senátoři nebo soudci
[73] Tamtéž, ustanovení § 110, které upravuje prověřování podmínek
[74] Tamtéž, ustanovení § 141 odst. 4

informace u orgánu státu, právnické osoby nebo podnikající fyzické osoby, vyžadovat stanovisko policie ke spolehlivosti jejího příslušníka nebo vyžadovat opis a výpis z evidence Rejstříku trestů, případně opis z evidence přestupků. Ministerstvo vnitra má však ještě oprávnění vydávat interní akty řízení, kterými je například Nařízení Ministerstva vnitra č. 42/2012 sb., o provádění ochrany utajovaných informací a o bezpečnostní způsobilosti, ve znění nařízení č. 39/2016 Sb. (dále jen „nařízení"), které bylo vydáno k zajištění jednotného postupu při ochraně utajovaných informací a bezpečnostní způsobilosti v útvarech Ministerstva vnitra, v Policejním prezidiu České republiky nebo v útvarech policie s celostátní působností, jak vyplývá z jeho úvodní části. Dále například komentuje různé podmínky u jednotlivých druhů zajištění ochrany utajovaných informací, odpovědnost nejvyšších činitelů zmiňovaných orgánů za zajištění ochrany utajovaných informací nebo i kontrolní činnost a preventivní opatření.

7.2 Policie České republiky

Policie při výkonu svých povinností přichází do styku s různými informacemi, se kterými následně nakládá. Řídí se kromě zákona také zákonem č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů (dále jen „zákon o Policii"). V této podkapitole jsou vymezena ta ustanovení ze zákona o Policii, která s utajováním informací podle tohoto zákona souvisí.

Práci s informacemi všeobecně upravuje hlava desátá zákona o Policii. Zde je důležité zmínit především dvě ustanovení. Jednak je to ust. § 83, které je v oddílu pojednávajícím o informování o osobních údajích a jejich případné opravě. Zde se uvádí odst. 4 písm. b), kdy nebude vyhověno (nebo pouze částečně vyhověno) písemným žádostem žadatelů vymezených v odst. 1 a 2 téhož ustanovení, a to pokud by tím mohlo dojít k ohrožení utajovaných informací, nebo dle písm. a) k ohrožení plnění úkolů podle ust. § 85, které je druhým ze zmiňovaných ustanovení. Tento oddíl pojednává o zpracování osobních údajů v souvislosti s trestnou činností a se zajištěním vnitřní a vnější bezpečnosti České republiky. Zmíněné ust. § 85 v písm. c) hovoří mimo jiné o tom, že policie může při plnění svých úkolů shromažďovat osobní údaje i utajeným způsobem.

S ohledem na mezinárodní spolupráci uváděnou v hlavě jedenácté zákona o Policii, která hraje také důležitou roli při ochraně utajovaných informací související se stykem České republiky s cizí mocí, je vymezeno ust. § 94, které uvádí, že policie může subjektům uvedeným v ust. § 89 poskytovat utajované informace i bez souhlasu Úřadu. Poskytování utajovaných informací se zde neuskutečňuje prostřednictvím ústředního registru[75], ale podle jiného právního předpisu. Jiným právním předpisem se má v tomto případě na mysli zákon.

Ve společných a přechodných ustanovení pak ještě zákon o Policii uvádí v oddílu dokumentace v ust. § 115 odst. 1, že policista nebo zaměstnanec policie jsou povinni zachovávat mlčenlivost o skutečnostech, se kterými se seznámili při plnění úkolů policie nebo v souvislosti s nimi, a které v zájmu zabezpečení úkolů policie nebo v zájmu jiných osob vyžadují, aby zůstaly utajeny před nepovolanými osobami.

[75] Ústřední registr viz kapitola 3.5

8. Informační bezpečnost

S ochranou utajovaných informací je v moderní době spjata také informační bepečnost, která tvoří podstatnou část celého zabezpečovacího procesu, a to jak z pohledu elektronického, tak i fyzického přenosu, zpracování či skladování informací a dat. Může na ni být nahlíženo jako na postup, při kterém se vytváří podmínky zajišťující ochranu před vstupem nepovolaných osob do prostor či elektronických systémů obsahujících utajované informace. Toho lze dosáhnout různými způsoby. V rámci utajovaných informací se řídí tato informační bezpečnost a její zajištění zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. Konkrétní vymezení požadavků a další podrobnosti na zabezpečení pak vymezují prováděcí právní předpisy vztahující se ke zmíněnému zákonu a uvedené například v seznamu použitých zdrojů této práce. Samotný pojem informační bezpečnosti je však mnohem širší a zahrnuje i jiné právní předpisy, které se k této problematice vztahují.

V souvislosti s informační bezpečností vztahující se k organizaci nebo instituci nakládající s předmětnými informacemi vymezenými v nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací, se mimo legislativně povinná a vymezená opatření uplatňují, nebo by se měla adekvátně uplatňovat opatření zmíněná v kapitole 5.1, jež zahrnují důvěrnost, integritu a dostupnost (v anglickém znění také jako CIA triad[76]). Tyto tři prvky daného modelu jsou považovány za nejdůležitější složky pro zajištění uvedeného druhu bezpečnosti[77]. *Důvěrnost* je v tomto případě vyjádřena jako určité nastavení norem nebo pravidel, která omezují přístup k informacím, a tím zachovávají jejich utajení. *Integrita* (též celistvost) by měla být jistota toho, že informace je důvěryhodná a korektní, a že s ní nebylo v průběhu přenosu manipulováno. *Dostupnost* je zase zárukou spolehlivosti u oprávněných osob (autorizovaných subjektů), které mají k informacím přístup (může se týkat příjemce, zpracovatele a jiných osob nakládajících nebo přicházejících s utajovanými ifnformacemi do kontaktu). Tyto tři prvky[78] rámcově vymezují prováděcí právní předpisy, které aplikují nezbytně nutná opatření pro provádění operací s utajovanými informacemi a při styku s nimi.

[76] Nezaměňovat s Central Intelligence Agency
[77] ROUSE, Margaret. Confidentiality, integrity, and availability (CIA triad) [online]. Newton, Massachusetts: TechTarget, 2014 [cit. 2020-02-28]. Dostupné z: https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA
[78] Důvěrnost, integritu a dostupnost uvádí také například Čandík (2004, s. 8, 35)

Ideální model zajišťující informační bezpečnost by měl zahrnovat i další způsoby prevence rizik s tím spojených. Mezi tyto faktory patří v rámci vnitřního zabezpečení instituce například zvyšování kvality a zabezpečení informačních[79] a komunikačních[80] systémů, v rámci vnější ochrany pak například zvyšování kvality fyzické bezpečnosti[81]. Uvedený model jako vztah nadřízenosti a podřízenosti zmiňuje také Požár (2005, s. 38-39). Ten kromě jiného definuje některé další pojmy v rámci informační bezpečnosti jako *aktiva* (assets), *bezpečnostní hrozby* (threats) či *bezpečnostní mechanismy, které realizují protiopatření* (countermeasure). Z pohledu výkonu činnosti v oblasti ochrany utajovaných informací ve spojitosti s informační bezpečností se jeví jako nejdůležitější pojem aktiva, která jsou v tomto případě reprezentována právě utajovanými informacemi. Tyto informace pak představují nejcennější předmět, s nímž je při styku mezi Úřadem a jinou organizací či subjektem nakládáno. S tím souvisí vše kolem jejich zabezpečení. Platná a pružná legislativa reagující na nové nastálé situace je jedním ze dvou hlavních bodů. Tím druhým, neméně důležitým, je právě informační bezpečnost. Ta v celém svém souhrnu představuje *zásady bezpečné práce s informacemi všeho druhu a všech typů*[82]. Dále zahrnuje i způsob zpracování, uložení a správy takových informací, a to nejen v elektronické (či digitální) podobě, ale i fyzické (například listinné), zásady skartace materiálů, nakládání s informacemi během jejich přenosu či přesunu nebo zásady pro jejich poskytování[83].

[79] *Bezpečnost informačních systémů* [online]. Praha: Národní bezpečnostní úřad [cit. 2020-03-15]. Dostupné z: https://www.nbu.cz/cs/ochrana-utajovanych-informaci/bezpecnost-informacnich-systemu/
[80] *Bezpečnost komunikačních systémů* [online]. Praha: Národní bezpečnostní úřad [cit. 2020-03-15]. Dostupné z: https://www.nbu.cz/cs/ochrana-utajovanych-informaci/bezpecnost-komunikacnich-systemu/
[81] *Fyzická bezpečnost (technické prostředky a další prvky fyzické bezpečnosti a jejich certifikace)* [online]. Praha: Národní bezpečnostní úřad [cit. 2020-03-15]. Dostupné z: https://www.nbu.cz/cs/ochrana-utajovanych-informaci/fyzicka-bezpecnost-technicke-prostredky-a-dalsi-prvky-fyzicke-bezpecnosti-a-jejich-certifikace/
[82] Požár, J. *Informační bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005, s. 39
[83] Tamtéž, s. 39

V návaznosti na legislativu je v rámci ochrany utajovaných informací nejdůležitější již zmíněný zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti (dále jen zákon) a jeho prováděcí právní předpisy (vyhlášky). V oblasti informační bezpečnosti lze však zmínit i další důležitý právní předpis, a to zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů. Tento právní předpis, jak je uvedeno v ust. § 1 odst. 1 upravuje práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti. Dále dle ust. § 1 odst. 2 zapracovává příslušné předpisy Evropské unie a upravuje zajišťování bezpečnosti sítí elektronických komunikací a informačních systémů. Důležité je však poznamenat, že tento zákon se dle ust. §1 odst. 3 nevztahuje na informační nebo komunikační systémy, které nakládají s utajovanými informacemi. Tím je reflektováno, že tato kompetence náleží NÚKIB a řídí se jinými právními předpisy (viz kap. 5). Dalším předpisem, který se v rámci veřejné správy dotýká informační bezpečnosti je zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů. Tento zákon dle ust. § 1 odst. 1 stanoví práva a povinnosti, které souvisejí s vytvářením, správou, provozem, užíváním a rozvojem informačních systémů veřejné správy spravovaných státními orgány nebo orgány územních samosprávných celků. Ovšem i zde zákonodárce vymezuje k jakým úkonům se předmětný zákon nevztahuje. To uvádí konkrétněji v ust. § 1 odst. 2, kde je vymezeno, že se nevztahuje na informační systémy veřejné správy spravované pro potřeby nakládání s utajovanými informacemi (písm. a)), zpravodajskými službami (písm. b)), Národním bezpečnostním úřadem (písm. c)) a Národním úřadem pro kybernetickou a informační bezpečnost (písm. d)). Tedy i zde je primárním právním předpisem zákon a příslušné vyhlášky. Z pohledu utajovaných informací je proto důležité odlišit informační bezpečnost instituce nenakládající s utajovanými informacemi a informační bezpečnost u instituce nebo subjektu, kteří s nimi pracují, nakládají nebo je uchovávají. Taková instituce nebo subjekt musí pak splňovat kromě základních technických požadavků na informační bezpečnost i jiné bezpečnostní prvky, vymezené k tomu určenou legislativou. Pro tyto účely pak zákonodárce jasně definuje a vymezuje konkrétní bezpečnostní požadavky a procedury prováděné pro fyzickou, administrativní, personální, průmyslovou a kryptografickou bezpečnost, jejichž definici upřesňuje zákon v ust. § 5 písm. a) až f).

Zásadní pro výkon předmětné činnosti zajišťující bezpečnost informací je pracovat nejen s aktuálními právními předpisy, ale také je pravidelně aktualizovat v rámci vnitřní bezpečnostní politiky ústředních správních úřadů a dalších organizací. S tím souvisí rovněž pravidelná aktualizace technických norem a příslušné dokumentace směřující k ochraně již zmíněných aktiv (assets) a také dalších osob, například zaměstnanců. Příslušná opatření se rámcově zavádějí v návaznosti na provedenou analýzu rizik. Tato analýza je procesem, který spočívá v odhalení a definici možných hrozeb (threats) a určení pravděpodobnosti, že určitá hrozba bude prostřednictvím nějakých slabin uskutečněna (Požár, 2006, s. 42). Výsledkem takové analýzy je pak souhrn doporučených protiopatření (countermeasure) ke snížení rizika na minimum (Požár, 2006, s. 42).

8.1 Standardizace

Pro potřeby technické dokumentace se užívají různé normy ISO[84]. Ty vydává mezinárodní organizace pro normalizaci, která sídlí ve Švýcarské Ženevě. Tato organizace byla založena roku 1945 a jejím cílem je sjednocení průmyslových standardů[85]. V rámci informační bezpečnosti jsou nejzásadnější standardy ISO s označením 27000 a 27001. Standardy této řady se uplatňují v systému řízení bezpečnosti informací, zkráceně ISMS[86]. Jedná se o *mezinárodní zkratku pro systém stanovující základní požadavky na bezpečnost všech forem reprezentace informací podle normy ISO27001*[87]. Pro lepší představu lze uvést, že ISO 27000 je *rodina mezinárodních standardů zaměřená na řízení informační bezpečnosti v organizacích*[88]. ISO 27001 je pak *hlavní norma pro systém řízení bezpečnosti informací*[89]. V rámci veřejné správy je k nim přistupováno dle zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, a také dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů.

[84] International Organization for Standardization
[85] *O organizaci ISO* [online]. Třinec: Hamri Plus [cit. 2020-03-21]. Dostupné z: http://www.info-iso.cz/iso
[86] Information Security Management System
[87] *ISMS (Information Security Management System)* [online]. Plzeň: Vědeckotechnický park, 2016 [cit. 2020-03-21]. Dostupné z: https://managementmania.com/cs/isms-information-security-management-system
[88] *ISO 27000* [online]. Plzeň: Vědeckotechnický park, 2017 [cit. 2020-03-21]. Dostupné z: https://managementmania.com/cs/iso-27000
[89] Tamtéž [cit. 2020-03-21]

8.2 eGovernment

Jedním z důvodů, který vede k nutnosti se věnovat informační bezpečnosti, je i snaha státních orgánů o co nejdostupnější kontakt s veřejností při vyřizování různých záležitostí, což činí prostřednictvím informačních a komunikačních technologií. Tento proces je označován zkratkou eGovernment (electronic government) a je chápán jako *využití informačních a komunikačních technologií veřejnou a státní správou k poskytování informací a veřejných služeb nejširší veřejnosti, přičemž zcela zásadní vlastností těchto technologií je schopnost transformovat vztahy mezi veřejnou správou a veřejností*[90]. To by mělo postupně umožnit i snažší komunikaci občanů s úřady a tím prakticky omezit nutnost osobní účasti na kontaktních místech správních orgánů na minimum. Zajištění bezpečnosti takové agendy je proto velmi důležitým krokem k zajištění bezproblémových služeb, které by měl eGovernment poskytovat.

Základním právním předpisem, který se týká eGovernmentu, je zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů. Ani zde však není opomenuto v ust. § 1 odst. 2, že *tento zákon se nevztahuje na dokumenty, které obsahují utajované informace*. S těmi, jak již bylo zmíněno dříve, operuje zákon.

Komplexnější informace o eGovernmentu lze dohledat také na webovém portálu Ministerstva vnitra České republiky[91].

[90] Pavlíček, A., Galba A. Moderní informatika. Praha: Professional Publishing, 2012, s. 122
[91] *Ministerstvo vnitra České* republiky [online]. Praha: eGovernment - Ministerstvo vnitra České republiky, 2019 [cit. 2020-03-22]. Dostupné z: https://www.mvcr.cz/egovernment.aspx

8.3 Šifrování

Jedním z oborů, které se zabývají šifrováním a tím také realizací určité oblasti informační bezpečnosti je kryptografie[92]. Jedná se o *proces, jehož cílem je zamezit přístupu třetích stran k důvěrné informaci*[93]. Kryptografie za tímto účelem používá *transformaci informace do podoby, která je nesrozumitelná, ale ze které je možné získat původní formu použitím inverzní transformace* (Čandík, 2004, s. 97). Dešifrovací klíč je pak oprávněn vlastnit pouze ten, kdo informaci potřebuje rozumět. Kryptografickou ochranu v rámci utajovaných informací zmiňuje jak zákon o ochraně utajovaných informací a bezpečnostní způsobilosti, tak i jeho některé prováděcí právní předpisy (viz kapitola 5.2). Důvod, který vedl ke vzniku kryptografie, byla potřeba ochrany a zabezpečení informací, a to pomocí určitého kódu (nebo též šifry). Tento kód byl známý pouze těm, kdo s těmito infromacemi měli operovat a dále nakládat. Kryptografie samotná se však postupem času měnila v závislosti na potřebách dané doby souvisejících především s vývojem technologického pokroku. Kryptografie tedy nemá za úkol zabránit tomu, aby daná informace nepadla do cizích rukou, ale má zabránit tomu, aby někdo porozuměl jejímu obsahu (Piper a Murphy, 2006, s. 14). S tím také souvisí potřeba zavedení kvalitního kódu, který nebude pro protistranu snadné prolomit a tím zjistit obsah zcizené informace. Samotná kryptografie tak ve svém procesu navazuje na již zmíněnou důvěrnost a integritu, ke kterým v rámci šifrovacího procesu lze ještě přidat autentizaci (případně autenticitu) a nepopiratelnost, jako základní požadavky na bezpečnou komunikaci[94]. Konkrétní šifra pak může mít podobu fyzické, symetrické nebo asymetrické šifry[95].

Kromě kryptografie se ochranou informací zabývá také například *steganografie*, která popisuje způsoby subjektivně nevnímatelného přenosu informace pomocí jejího vložení do krycích dat, a která se používá především pro komunikaci mezi dvěma osobami nebo skupinami[96]. Steganografie tedy studuje metody utajení komunikace a jejím cílem je ukrytí skutečnosti, že tajná komunikace vůbec existuje[97]. Tím se liší právě od kryptografie, která se zabývá metodami utajení obsahu zprávy, ale nikoli samotným utajením komunikace.

[92] Věda o vytváření šifrovacích systémů (Piper, Murphy, 2006, s. 15)
[93] Pavlíček, A., Galba A. Moderní informatika. Praha: Professional Publishing, 2012, s. 119
[94] Tamtéž, s. 119
[95] Tamtéž, s. 120-121
[96] Čandík, M. Základy informační bezpečnosti. Zlín: Univerzita Tomáše Bati ve Zlíně, 2004, s. 97-98
[97] Tamtéž, s. 87, 92

Závěr

Na základě zvoleného tématu bylo v práci za použití stanovených metod zhodnoceno fungování institucí státní správy v oblasti ochrany utajovaných informací, především se zaměřením na platnou legislativu upravující postupy mezi jednotlivými orgány a subjekty, včetně dalších náležitostí, které vyplývají z celého procesu ochrany utajovaných informací, jehož se jednotlivé orgány zmíněné v této práci účastní.

S rozvojem technologií bylo potřeba věnovat pozornost také informační bezpečnosti, která bude tento pokrok reflektovat a zároveň také zajišťovat, aby byly naplněny veškeré náležitosti, které jsou spojené s ochranou utajovaných informací.

Bude-li výše uvedené dodržováno, pak je pravděpodobné, že se podaří předejít případným negativním jevům, které by souvisely se zastaralou právní úpravou nebo nedostatečnou standardizací postupů zahrnující i technologické aspekty u veškerých prováděných činností. S tím neméně souvisí také zajištění konzistentnosti v rámci informační bezpečnosti a z toho vycházející potřeby pravidelného sledování aktuálních rizik.

Výsledku pak bylo docíleno studiem použitých zdrojů ve snaze o co největší přiblížení k aktuálním potřebám vyplývajících z praxe. S tím souviselo i uvedení potřebných informací odkazující na základní právní prameny a jejich vzájemné zhodnocení, včetně poskytnutí určitého pohledu na jejich provázanost nebo odlišnost, čímž byla naplněna základní premisa této práce.

Práce tak tvoří ucelený soubor podávající náhled na předmětné činnosti související s ochranou utajovaných informací prováděné jednotlivými orgány a definované příslušnými právními akty, a to se značnou mírou jejich vzájemného propojení. Téma by bylo možné rozšířit o hlubší proniknutí do prováděcích právních předpisů, jelikož návaznost vyhlášek k samotnému zákonu je nezbytnou součástí k zajištění ochrany utajovaných informací, nebo o další konkretizaci ISO norem vztahující se k certifikaci a systémům užívaných předmětnými úřady. Rozšíření by mohlo obsáhnout také širší pohled na výkon bezpečnostních služeb a jejich působnost.

Z právního hlediska by šlo lépe pojmout jednotlivou charakteristiku u působnosti a oprávnění úřadů, která se ve vymezených ustanoveních zákona vzájemně duplikují, což se jeví z pohledu autora práce jako nadbytečné. Za zvážení by stálo v rámci legislativních úprav navrhnout samostatný zákon upravující činnost Úřadu pro zahraniční styky a informace. Možné zlepšení by přineslo kvalitnější zajištění kontroly bezpečnostních služeb při výkonu jejich působnosti a také zkrácení lhůty pro vydávání osvědčení fyzické osoby v rámci bezpečnostního řízení pro jednotlivé stupně utajení.

Seznam použitých zdrojů

Literární zdroje

1. BŘEŇ, J. *Základní charakteristika státní správy*. Praha: Institut pro veřejnou správu Praha, 2017. 132 s. ISBN 978-80-86976-44-0.
2. ČANDÍK, M. *Základy informační bezpečnosti*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2004. 107 s. ISBN 80-7318-218-1.
3. DVOŘÁK, J. *Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti: komentář*. Praha: Wolters Kluwer, 2018. 480 s. ISBN 978-80-7598-016-8.
4. MOLNÁR, Z. *Pokročilé metody vědecké práce*. Zeleneč: Profess Consulting, 2012. 170 s. ISBN 978-80-7259-064-3.
5. PAVLÍČEK, A., GALBA A. *Moderní informatika*. Praha: Professional Publishing, 2012. 184 s. ISBN 978-80-7431-109-3.
6. PIPER, F. C., MURPHY S. *Kryptografie*. Praha: Dokořán, 2006. 157 s. ISBN 80-7363-074-5.
7. POŽÁR, J. *Informační bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. 309 s. ISBN 80-86898-38-5.

Elektronické zdroje

1. ROUSE, M. *Confidentiality, integrity, and availability (CIA triad)* [online]. Newton, Massachusetts: TechTarget, 2014 [cit. 2020-02-28]. Dostupné z: https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA
2. *Věstník* [online]. Praha: Národní bezpečnostní úřad [cit. 2019-03-01]. Dostupné z: https://www.nbu.cz/cs/o-nas/985-vestnik/
3. *Výbor pro bezpečnost* [online]. Praha: Parlament České republiky, Poslanecká sněmovna [cit. 2019-03-01]. Dostupné z: https://www.psp.cz/sqw/hp.sqw?k=4900
4. *Bezpečnost informačních systémů* [online]. Praha: Národní bezpečnostní úřad [cit. 2020-03-15]. Dostupné z: https://www.nbu.cz/cs/ochrana-utajovanych-informaci/bezpecnost-informacnich-systemu/
5. *Bezpečnost komunikačních systémů* [online]. Praha: Národní bezpečnostní úřad [cit. 2020-03-15]. Dostupné z: https://www.nbu.cz/cs/ochrana-utajovanych-informaci/bezpecnost-komunikacnich-systemu/

6. *Fyzická bezpečnost (technické prostředky a další prvky fyzické bezpečnosti a jejich certifikace)* [online]. Praha: Národní bezpečnostní úřad [cit. 2020-03-15]. Dostupné z: https://www.nbu.cz/cs/ochrana-utajovanych-informaci/fyzicka-bezpecnost-technicke-prostredky-a-dalsi-prvky-fyzicke-bezpecnosti-a-jejich-certifikace/
7. Bezpečnost komunikačních systémů [online]. Praha: Národní bezpečnostní úřad [cit. 2020-03-15]. Dostupné z: https://www.nbu.cz/cs/ochrana-utajovanych-informaci/bezpecnost-komunikacnich-systemu/
8. *O organizaci ISO* [online]. Třinec: Hamri Plus [cit. 2020-03-21]. Dostupné z: http://www.info-iso.cz/iso
9. *ISMS (Information Security Management System)* [online]. Plzeň: Vědeckotechnický park, 2016 [cit. 2020-03-21]. Dostupné z: https://managementmania.com/cs/isms-information-security-management-system
10. *ISO 27000* [online]. Plzeň: Vědeckotechnický park, 2017 [cit. 2020-03-21]. Dostupné z: https://managementmania.com/cs/iso-27000
11. *Ministerstvo vnitra České republiky* [online]. Praha: eGovernment - Ministerstvo vnitra České republiky, 2019 [cit. 2020-03-22]. Dostupné z: https://www.mvcr.cz/egovernment.aspx

Legislativní dokumenty

1. ČESKO. Ústavní zákon č. 1 ze dne 16. prosince 1992 Sb., Ústava České republiky. In *Sbírka zákonů České republiky*. 1993, částka 1, s. 3-16. Dostupné z WWW: <https://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=1/1993&typeLaw=zakon&what=Cislo_zakona_smlouvy>.
2. ČESKO. Zákon č. 2 ze dne 8. ledna 1969 o zřízení ministerstev a jiných ústředních orgánů státní správy České socialistické republiky. In *Sbírka zákonů České republiky*. 1969, částka 1, s. 16-19. Dostupné z WWW: <https://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=2/1969&typeLaw=zakon&what=Cislo_zakona_smlouvy>.
3. ČESKO. Zákon č. 412 ze dne 21. září 2005 o ochraně utajovaných informací a o bezpečnostní způsobilosti. In *Sbírka zákonů České republiky*. 2005, částka 143, s. 7526-7576. Dostupné z WWW: <https://aplikace.mvcr.cz/sbirkazakonu/SearchResult.aspx?q=412/2005&typeLaw=zakon&what=Cislo_zakona_smlouvy>.

4. ČESKO. Zákon č. 181 ze dne 23. července 2014 o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In *Sbírka zákonů České republiky*. 2014, částka 75, s. 1926-1936. Dostupné z WWW: <https://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=181/2014&typeLaw=zakon&what=Cislo_zakona_smlouvy>.
5. ČESKO. Zákon č. 153 ze dne 7. července 1994 o zpravodajských službách České republiky. In *Sbírka zákonů České republiky*. 1994, částka 49, s. 1601-1604. Dostupné z WWW: <https://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=153/1994&typeLaw=zakon&what=Cislo_zakona_smlouvy>.
6. ČESKO. Zákon č. 154 ze dne 7. července 1994 o Bezpečnostní informační službě. In *Sbírka zákonů České republiky*. 1994, částka 49, s. 1605-1629. Dostupné z WWW: <https://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=154/1994&typeLaw=zakon&what=Cislo_zakona_smlouvy>.
7. ČESKO. Zákon č. 289 ze dne 16. června 2005 o Vojenském zpravodajství. In *Sbírka zákonů České republiky*. 2005, částka 104, s. 5388-5393. Dostupné z WWW: <https://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=289/2005&typeLaw=zakon&what=Cislo_zakona_smlouvy>.
8. ČESKO. Zákon č. 273 ze dne 17. července 2008 o Policii České republiky. In *Sbírka zákonů České republiky*. 2008, částka 91, s. 4086-4116. Dostupné z WWW: <https://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=273/2008&typeLaw=zakon&what=Cislo_zakona_smlouvy>.
9. ČESKO. Zákon č. 365 ze dne 14. září 2000 o informačních systémech veřejné správy a o změně některých dalších zákonů. In *Sbírka zákonů České republiky*. 2000, částka 99, s. 4666-4671. Dostupné z WWW: <https://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=365/2000&typeLaw=zakon&what=Cislo_zakona_smlouvy>.
10. ČESKO. Zákon č. 106 ze dne 11. května 1999 o svobodném přístupu k informacím. In *Sbírka zákonů České republiky*. 1999, částka 39, s. 2578-2582. Dostupné z WWW: <https://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=106/1999&typeLaw=zakon&what=Cislo_zakona_smlouvy>.
11. ČESKO. Zákon č. 300 ze dne 17. července 2008 o elektronických úkonech a autorizované konverzi dokumentů. In *Sbírka zákonů České republiky*. 2008, částka 98, s. 4491-4500. Dostupné z WWW: <https://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=300/2008&typeLaw=zakon&what=Cislo_zakona_smlouvy>.

12. ČESKO. Nařízení vlády č. 522 ze dne 7. prosince 2005, kterým se stanoví seznam utajovaných informací. In *Sbírka zákonů České republiky*. 2005, částka 179, s. 9950-9977. Dostupné z WWW: <https://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=522/2005&typeLaw=zakon&what=Cislo_zakona_smlouvy>.
13. ČESKO. Vyhláška č. 363 ze dne 23. listopadu 2011 o personální bezpečnosti a o bezpečnostní způsobilosti. In *Sbírka zákonů České republiky*. 2011, částka 127, s. 4535-4556. Dostupné z WWW: <https://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=363/2011&typeLaw=zakon&what=Cislo_zakona_smlouvy>.
14. ČESKO. Vyhláška č. 405 ze dne 7. prosince 2011, o průmyslové bezpečnosti. In *Sbírka zákonů České republiky*. 2011, částka 142, s. 5334-5365. Dostupné z WWW: <https://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=405/2011&typeLaw=zakon&what=Cislo_zakona_smlouvy>.
15. ČESKO. Vyhláška č. 432 ze dne 16. prosince 2011 o zajištění kryptografické ochrany utajovaných informací. In *Sbírka zákonů České republiky*. 2011, částka 150, s. 5712-5729. Dostupné z WWW: <https://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=432/2011&typeLaw=zakon&what=Cislo_zakona_smlouvy>.
16. ČESKO. Vyhláška č. 523 ze dne 5. prosince 2005 o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor. In *Sbírka zákonů České republiky*. 2005, částka 179, s. 9978-9993. Dostupné z WWW: <https://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=523/2005&typeLaw=zakon&what=Cislo_zakona_smlouvy>.
17. ČESKO. Vyhláška č. 525 ze dne 14. prosince 2005 o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací. In *Sbírka zákonů České republiky*. 2005, částka 179, s. 10009-10014. Dostupné z WWW: <https://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=525/2005&typeLaw=zakon&what=Cislo_zakona_smlouvy>.
18. ČESKO. Vyhláška č. 528 ze dne 14. prosince 2005 o fyzické bezpečnosti a certifikaci technických prostředků. In *Sbírka zákonů České republiky*. 2005, částka 179, s. 10079-10115. Dostupné z WWW: <https://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=528/2005&typeLaw=zakon&what=Cislo_zakona_smlouvy>.

19. ČESKO. Vyhláška č. 529 ze dne 15. prosince 2005 o administrativní bezpečnosti a o registrech utajovaných informací. In *Sbírka zákonů České republiky*. 2005, částka 179, s. 10116-10151. Dostupné z WWW: <https://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=529/2005&typeLaw=zakon&what=Cislo_zakona_smlouvy>.
20. ČESKO. Nařízení Ministerstva vnitra č. 42 ze dne 29. srpna 2012, o provádění ochrany utajovaných informací a o bezpečnostní způsobilosti. In *Vnitřní předpisy Ministerstva vnitra České republiky*.