Z P R Á V A

O ČINNOSTI

NÁRODNÍHO BEZPEČNOSTNÍHO ÚŘADU

ZA ROK 2014

Praha 2015

1. ÚVOD

Činnost Národního bezpečnostního úřadu (dále jen „Úřad“) byla, v souladu s jeho působností a úkoly stanovenými především zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů (dále jen „zákon“), v roce 2014 zaměřena zejména na tyto hlavní oblasti:

- rozhodování o žádostech fyzických osob, žádostech podnikatelů a žádostech o doklad a provádění bezpečnostního řízení,
- certifikace technických prostředků, informačních systémů, kryptografických prostředků, kryptografických pracovišť a stínicích komor,
- spolupráce s bezpečnostními úřady členských zemí Organizace Severoatlantické smlouvy (NATO) a Evropské unie (EU) a zemí kandidujících na vstup do těchto organizací (vzájemné konzultace, příprava návrhů na sjednávání mezinárodních smluv) a podíl odborných pracovníků Úřadu na práci a jednání orgánů NATO a EU,
- aplikace právní úpravy ochrany utajovaných informací a bezpečnostní způsobilosti při plnění výše uvedených úkolů, výkon státního dozoru a poskytování metodické pomoci směřující k upevňování právního vědomí dotčených subjektů a ke sjednocování aplikační praxe v dané oblasti,
- legislativní, organizační a provozně-technické činnosti v souvislosti s gescí za oblast kybernetické bezpečnosti včetně otevření Národního centra kybernetické bezpečnosti (dále jen „NCKB“) v Brně, příprava aplikace nových právních předpisů a další činnosti v oblasti zajištění kybernetické bezpečnosti (tvorba kybernetické bezpečnostní politiky ČR, vymezování kritické informační infrastruktury ČR a významných informačních systémů, cvičení s tematikou kybernetické bezpečnosti, spolupráce se zainteresovanými subjekty v ČR i v zahraničí, účast na konferencích, seminářích a přednáškách, poskytování informací veřejnosti atd.).

2. ČINNOST ÚŘADU

2.1. LEGISLATIVNÍ A PRÁVNÍ ČINNOST ÚŘADU

2.1.1. Vnější legislativní činnost

Zákon byl v roce 2014 třikrát novelizován, a to v následujících oblastech:

- zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), upravil vztah kontrolního orgánu k Úřadu tak, aby mohl uplatňovat kontrolu nad činností Úřadu i v této oblasti,

- zákon č. 250/2014 Sb., o změně zákonů souvisejících s přijetím zákona o státní službě, upřesnil postavení Úřadu jako ústředního správního úřadu v oblasti ochrany utajovaných informací a bezpečnostní způsobilosti,

- další změna zákona se dotkla znění § 17 týkajícího se rizik podnikatele v oblasti ekonomické stability, a to v souvislosti s přijetím zákona č. 267/2014 Sb., kterým se mění zákon č. 586/1992 Sb., o daních z příjmů, ve znění pozdějších předpisů, a další související zákony, který změnil platnou právní úpravu týkající se jednotného inkasního místa.

Uvedené zákony nabyly účinnosti dnem 1. ledna 2015.

Úřad, který byl na základě usnesení vlády ČR č. 781 ze dne 19. října 2011 stanoven gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast, pokračoval v roce 2014 v legislativních pracích k přijetí zákona o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Návrh zákona o kybernetické bezpečnosti byl postupně projednán vládou ČR, schválen Poslaneckou sněmovnou i Senátem Parlamentu ČR a podepsán prezidentem republiky byl dne 13. srpna 2014. Ve Sbírce zákonů byl zákon o kybernetické bezpečnosti publikován dne 29. srpna 2014 v částce 75 pod č. 181 a účinnosti nabyl dnem 1. ledna 2015. Od uvedeného dne vykonává Úřad v oblasti kybernetické bezpečnosti státní správu na základě tohoto zákona a zákonem o kybernetické bezpečnosti mu tak přibyla nová působnost.

V návaznosti na přijetí zákona o kybernetické bezpečnosti zpracovával Úřad prováděcí právní předpisy k tomuto zákonu.

- Úřad se podílel na zpracování nařízení vlády, kterým se mění nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, které je v gesci Ministerstva vnitra, a které nově upravilo problematiku kybernetické bezpečnosti v oblasti komunikačních a informačních systémů pro určení prvku kritické infrastruktury.

- Úřad zpracoval vyhlášku o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti), která upravuje obsah bezpečnostních opatření a jejich rozsah, jakož i rozsah a doporučenou strukturu bezpečnostní dokumentace, dále konkrétní kategorie a typy kybernetických bezpečnostních incidentů a náležitosti a způsob jejich hlášení, rovněž vzor a formu oznámení kontaktních údajů a stanoví základní náležitosti oznámení o provedení reaktivního opatření a jeho výsledku s cílem zajištění zpětné vazby.

- Úřad dále ve spolupráci s Ministerstvem vnitra zpracoval i vyhlášku o významných informačních systémech a jejich určujících kritériích, jejichž

správci budou podléhat povinnostem podle zákona o kybernetické bezpečnosti.

Všechny uvedené prováděcí právní předpisy byly publikovány ve Sbírce zákonů dne 19. prosince 2014 v částce 127 pod č. 315, č. 316 a č. 317 a nabyly účinnosti dnem 1. ledna 2015.

Úřad se rovněž aktivně podílel na tvorbě návrhů zákonů, majících vazby na ochranu utajovaných informací a výkon citlivých činností, které byly připravovány jednotlivými ministerstvy nebo jinými ústředními orgány státní správy v souvislosti s přijetím nových zákonů nebo se změnami stávajících zákonů. Jednalo se mj. o změnu zákona o nakládání s bezpečnostním materiálem, zákona o zahraničním obchodu s vojenským materiálem, zákona o mírovém využívání jaderné energie a ionizujícího záření (atomový zákon) nebo o nově připravovaný zákon o soukromé bezpečnostní činnosti.

Úřad v rámci mezirezortního připomínkového řízení dále zpracoval stovky připomínek k návrhům právních předpisů předkládaných ministerstvy nebo jinými ústředními orgány státní správy.

2.1.2. Vnitřní legislativní činnost

V průběhu roku 2014 bylo vydáno celkem 42 nových interních aktů řízení ředitele Úřadu. Konkrétně se jednalo o 8 směrnic a 34 pokynů, které byly vydány jako reakce na změny v právním řádu nebo z důvodu snahy o zefektivnění činnosti Úřadu. Oproti roku 2013 bylo vydáno o 2 interní akty řízení méně, přesto pokračuje trend vydávání vyššího počtu interních aktů řízení oproti předchozím letům, a to také z důvodu zavádění nové působnosti Úřadu v oblasti kybernetické bezpečnosti do aplikační praxe.

2.1.3. Vyjádření k oznámení podle § 69 odst. 1 písm. r) zákona

Úřad již třetím rokem (od 1. ledna 2012) v rámci ochrany utajovaných informací zabezpečuje agendu, která se váže k zadávání veřejných zakázek veřejnými zadavateli, a podle § 138 odst. 1 písm. l) zákona se vyjadřuje k oznámení veřejných zadavatelů podle § 69 odst. 1 písm. r) zákona. Tato činnost spočívá v posuzování oznámení z hlediska ochrany utajovaných informací, učiněných veřejnými zadavateli, v nichž Úřadu oznamují skutečnost, že v rámci zadávacího řízení budou postupovat mimo režim zákona č. 137/2006 Sb., o veřejných zakázkách, ve znění pozdějších předpisů, z důvodu ochrany utajovaných informací, nebo že pro účast v zadávacím resp. koncesním řízení hodlají stanovit profesní kvalifikační předpoklad osvědčení podnikatele.

V roce 2014 se Úřad vyjádřil k 80 podaným oznámením. Počet těchto oznámení osciluje od počátku této agendy kolem tohoto čísla, přičemž největší, takřka poloviční, podíl na oznámeních má Ministerstvo obrany. V rámci posuzování podaných oznámení Úřad s veřejnými zadavateli ověřoval nezbytnou nutnost jimi zvoleného postupu včetně vyžadování příslušných dokumentů obsahujících utajované informace a ověřování těchto skutečností se zaměstnanci oznamovatelů.

Přehledy o zaslaných oznámeních a vyjádřeních Úřadu se, podle zákona, pravidelně zasílají k využití Úřadu pro ochranu hospodářské soutěže.

2.1.4. Právní činnost

V roce 2014 bylo pro porušení povinností stanovených zákonem ukončeno celkem 37 správních řízení, z toho ve 26 případech s fyzickými osobami a v 11 případech s právnickými osobami. Ve 41 případech byla uložena sankce (převážně peněžitá pokuta, jen ve 3 případech bylo uloženo napomenutí). Ve 3 dalších případech nebylo správní řízení dosud ukončeno. Celková výše uložených pokut dosáhla částky 403.000 Kč.

V roce 2014 nedošlo k zastavení řízení. Ve 39 dalších případech byla věc odložena nebo správní řízení nebylo zahájeno (ve 31 případech u fyzických osob, v 8 případech u právnických osob). Dále v 8 případech nebyla správní řízení prozatím zahájena, neboť jsou Úřadem činěny patřičné kroky v rámci přípravného řízení. Ve 29 případech byla věc z důvodu nepříslušnosti postoupena k projednání příslušnému služebnímu funkcionáři.

Správní řízení v roce 2014

	Fyzická osoba	Právnická osoba	Celkem
Ukončená správní řízení	26	11	**37**
Počet uložených sankcí	30	11	**41**
Zastavená správní řízení	0	0	**0**
Dosud neukončená správní řízení	2	1	**3**

V souladu se směrnicí ředitele Úřadu č. 5/2013, o zadávání veřejných zakázek v Národním bezpečnostním úřadu, ve znění pozdějších předpisů, odpovídá za závazný postup Úřadu v oblasti zadávání veřejných zakázek odbor právní a legislativní. Právní oddělení odboru právního a legislativního tak mj. odpovídá za stanovení správného postupu při zadávání veřejných zakázek a dohled nad dodržováním zásad zadávání veřejných zakázek podle zákona č. 137/2006 Sb., o veřejných zakázkách, ve znění pozdějších předpisů. Převážnou většinu veřejných zakázek zadávaných Úřadem v roce 2014 tvořily z hlediska objemu finančních prostředků veřejné zakázky malého rozsahu, které jsou zadávány prostřednictvím elektronického tržiště Gemin, kde jsou také údaje o všech těchto veřejných zakázkách zveřejněny. Odbor právní a legislativní se k zadání těchto veřejných zakázek vyjadřoval prostřednictvím schvalovacího nástroje v elektronickém tržišti, u zakázek malého rozsahu s plněním nad 500.000 Kč bez DPH vydává k zadání ještě zvláštní souhlas. Z podlimitních a nadlimitních veřejných zakázek, kde odbor právní a legislativní přímo vede zadávací řízení, byla v roce 2014 nejvýznamnější realizovanou veřejnou zakázkou nadlimitní veřejná zakázka „Realizace technologického centra pro provoz Národního centra kybernetické bezpečnosti“.

V oblasti právní činnosti bylo v roce 2014 dále uzavřeno cca 70 smluv nebo dodatků k již existujícím smlouvám s externími subjekty, jejichž předmětem je

především zajištění činností a dodávek nezbytných pro plnění stanovených úkolů Úřadu.

Součást právní činnosti tvoří rovněž vyřizování nároků na náhradu škody způsobené nezákonným rozhodnutím nebo nesprávným úředním postupem, podle zákona č. 82/1998 Sb., o odpovědnosti státu za škodu způsobenou při výkonu veřejné moci rozhodnutím nebo nesprávným úředním postupem, ve znění pozdějších předpisů. V současnosti probíhá řízení ve věci uplatnění nároku na náhradu této škody se třemi žadateli. Průběžně je vedena evidence plnění legislativních závazků vyplývajících z členství v EU v působnosti Úřadu prostřednictvím Informačního systému aproximace práva (ISAP). Pro potřeby organizačních celků Úřadu byla vypracována řada právních stanovisek k aplikaci právních předpisů z oblasti působnosti Úřadu i ostatních právních předpisů.

2.2. MEZINÁRODNÍ SPOLUPRÁCE ÚŘADU

2.2.1. Mezinárodní smlouvy

Úřad má jako ústřední správní úřad pro oblast ochrany utajovaných informací ve své kompetenci přípravu návrhů na sjednávání smluv o ochraně utajovaných informací. Při stanovování priorit v této oblasti Úřad vychází z praktické potřeby výměny utajovaných informací s konkrétními státy a z potřeby zajistit těmto informacím odpovídající ochranu. Sjednávání smluv o ochraně utajovaných informací je zcela v souladu se zahraničně politickými zájmy ČR, stejně jako se závazky, které pro ČR vyplývají z členství v EU a NATO.

Smlouvy o ochraně utajovaných informací upravují režim poskytování utajovaných informací mezi ČR a druhou smluvní stranou, ochranu předaných utajovaných informací a spolupráci správních orgánů odpovědných za jejich ochranu. Vzhledem k tomu, že tyto smlouvy upravují věci, jejichž úprava je vyhrazena zákonu, a dále práva a povinnosti osob, jedná se o smlouvy, k jejichž ratifikaci je, v souladu s čl. 49 Ústavy ČR, potřebný souhlas obou komor Parlamentu ČR. Ve smyslu Směrnice vlády pro sjednávání, vnitrostátní projednávání, provádění a ukončování platnosti mezinárodních smluv, schválené usnesením vlády ČR č. 131 ze dne 11. února 2004, se jedná o mezinárodní smlouvy prezidentské kategorie.

Smlouvy o ochraně utajovaných informací jsou sjednávány v souladu s Ústavou ČR a ostatními právními předpisy a v souladu s mezinárodně-právními závazky ČR (včetně práva EU a bezpečnostních standardů NATO). Smlouvy dále reflektují obecně uznávané principy a uzance mezinárodního práva. Jejich provádění nemá dopad na státní rozpočet.

2.2.1.1. Hodnocení sjednávání smluv o ochraně utajovaných informací za rok 2014

V roce 2014 byly vyvíjeny následující aktivity v rámci sjednávání mezinárodních smluv:

- **Smlouva mezi Českou republikou a Belgickým královstvím o výměně a vzájemné ochraně utajovaných informací**

  V roce 2014 pokračovalo expertní jednání o smlouvě.

- **Smlouva mezi Českou republikou a Nizozemským královstvím o výměně a vzájemné ochraně utajovaných informací**

  Vzhledem k tomu, že v Nizozemském království došlo ke změně zákona upravujícího ochranu utajovaných informací, bylo dohodnuto znovu provést expertní jednání. Nizozemská strana však nebyla připravena v roce 2014 toto zahájit.

- **Bezpečnostní prováděcí dohoda pro projekty v oblasti průmyslu mezi vládou České republiky a vládou Spojených států amerických**

  Text smlouvy je dohodnut, nicméně se čeká na vyjádření *Department of State* k některým ustanovením.

- **Smlouva mezi Českou republikou a Srbskou republikou o výměně a vzájemné ochraně utajovaných informací**

  V roce 2013 byla smlouva podepsána a následně byla postoupena Parlamentu ČR k vyslovení souhlasu s ratifikací. Senát Parlamentu ČR dal souhlas s ratifikací svým usnesením č. 30 ze dne 3. prosince 2014. Poslanecká sněmovna Parlamentu ČR stačila projednat uvedenou smlouvu pouze v prvním čtení a v zahraničním výboru, který doporučil dát souhlas s ratifikací svým usnesením č. 61 ze dne 13. listopadu 2014.

- **Smlouva mezi Českou republikou a Tureckou republikou o výměně a vzájemné ochraně utajovaných informací**

  V roce 2014 se zástupci Úřadu setkali se svými tureckými partnery při expertních jednání o smlouvě o vojenské spolupráci. Byla řešena i otázka sjednání obecné smlouvy o výměně a vzájemné ochraně utajovaných informací a bylo dosaženo dohody, že si strany znovu vymění vzorové návrhy.

- **Dohoda mezi členskými státy Evropské unie zasedajícími v Radě o ochraně utajovaných informací vyměňovaných v zájmu Evropské unie**

  Parlament ČR vyslovil souhlas s ratifikací již v roce 2012. Čeká se na ratifikaci v ostatních státech.

- **Smlouva mezi Českou republikou a Spojenými arabskými emiráty o výměně a vzájemné ochraně utajovaných informací**

  Expertní jednání probíhají.

- **Smlouva mezi Českou republikou a Maltskou republikou o výměně a vzájemné ochraně utajovaných informací**

  Obě strany si vyměnily návrhy na sjednání smlouvy, expertní jednání se plánuje až na rok 2015.

- **Smlouva mezi Českou republikou a Iráckou republikou o výměně a vzájemné ochraně utajovaných informací**

  Návrh smlouvy byl předán irácké straně, čeká se na její vyjádření.

- **Smlouva mezi Českou republikou a Spojeným královstvím o výměně a vzájemné ochraně utajovaných informací**

  S ohledem na změnu právní úpravy ochrany utajovaných informací ve Spojeném království je nutné tuto změnu zohlednit ve stávajícím smluvním rámci. Úřad se snaží přesvědčit druhou stranu o nezbytnosti sjednání nové obecné smlouvy o ochraně utajovaných informací, která by nahradila 10 let starou Bezpečnostní dohodu mezi vládou České republiky a vládou Spojeného království Velké Británie a Severního Irska o ochraně utajovaných skutečností z oblasti obrany, předávaných mezi oběma státy (18/2004 Sb.m.s.).

- **Smlouva mezi Českou republikou a Moldavskou republikou o výměně a vzájemné ochraně utajovaných informací**

  Připravuje se expertní jednání.

2.2.1.2. Výhled na rok 2015

V roce 2015 Úřad předpokládá dokončení expertních jednání s Belgií, Nizozemskem, Tureckem, USA a Spojenými arabskými emiráty. Dále se očekává zahájení jednání s Maltou, Moldavskem, Irákem a Spojeným královstvím.

2.2.2. Aktivity v rámci NATO a EU a spolupráce s bezpečnostními úřady partnerských států

Zaměstnanci Úřadu se podíleli na činnosti významných výborů a pracovních skupin NATO a obdobných orgánů v rámci institucí EU a ESA.

Úřad od svého založení průběžně spolupracuje s národními bezpečnostními úřady členských zemí NATO a EU v oblasti ochrany utajovaných informací (výměny zkušeností, provádění úkonů v bezpečnostním řízení, uznávání bezpečnostních oprávnění, povolování návštěv, které předpokládají přístup k utajovaným informacím, atd.) a poskytuje konzultační a asistenční činnost státům, které aspirují na členství v obou uvedených organizacích. Asistenční a konzultační činnost ve vztahu k nečlenským státům EU nebo NATO se zaměřuje zejména na oblast Balkánu (Albánie, Bosna a Hercegovina, Černá Hora, Chorvatsko, Kosovo, Makedonie a Srbsko), jižního Kavkazu (Ázerbájdžán, Gruzie) a Dálného východu (Korejská republika).

V roce 2014 uspořádal Úřad workshopy v oblasti bezpečnostního řízení, opravných prostředků, bezpečnosti informačních systémů, TEMPEST a kybernetické bezpečnosti pro zástupce národních bezpečnostních úřadů Bosny a Hercegoviny, Kosova a Koreje.

2.2.3. Mezinárodní aktivity v oblasti kybernetické bezpečnosti

V roce 2014 Úřad rozvíjel bilaterální a multilaterální mezinárodní spolupráci v oblasti kybernetické bezpečnosti.

Hlavním tématem pro Úřad na evropské úrovni byla i v roce 2014 bezpečnost sítí a informací. Směrnice o bezpečnosti sítí a informací (NIS) byla Evropskou komisí představena dne 7. února 2013 v souvislosti se společným sdělením Evropské komise a vysoké představitelky EU pro zahraniční věci a bezpečnostní politiku o evropské strategii pro kybernetickou bezpečnost.

Úřad od počátku aktivně vysílá své experty na jednání na půdě Rady EU, která probíhají v rámci Pracovní skupiny pro telekomunikace a informační společnost. Směrnice byla intenzivně projednávána během řeckého i italského předsednictví, přičemž cílem italského předsednictví bylo dokončení jejího projednávání. Za tímto účelem byla od poloviny října 2014 zahájena neformální jednání s Evropským parlamentem, jejichž cílem je sjednotit stanovisko Evropského parlamentu a Rady EU. Cílem Úřadu je prosazení pozice ČR, která se soustředí zejména na ochranu kritické informační infrastruktury státu a zabránění významnému rozšiřování oblasti působnosti směrnice na soukromoprávní subjekty.

ČR má své zastoupení formou účasti na pořádaných formálních a neformálních jednáních v Evropské agentuře pro bezpečnost sítí a informací (ENISA). Dva zástupci Úřadu jsou členy představenstva ENISA (jedná se o pozice Management Board Member a Alternate Management Board Member), kde jsou zodpovědní za schvalování programu a plánu prací a rozpočtu agentury. Na podzim roku 2014 byl zástupce NCKB osloven, aby se stal členem užší pracovní skupiny ENISA vytvořené na podporu tvorby a implementace národních strategií kybernetické bezpečnosti. Přizvaný zástupce se tak bude od příštího roku ve spolupráci s dalšími odborníky podílet na konzultacích a přípravě metodických a podpůrných materiálů pro tvorbu strategických dokumentů tak, aby co nejvíce reflektovaly aktuální hrozby a rizika v oblasti kybernetické bezpečnosti.

Otázky kybernetické bezpečnosti byly diskutovány také na půdě Organizace pro bezpečnost a spolupráci v Evropě (OBSE). V listopadu 2014 švýcarské předsednictví OBSE uspořádalo konferenci ICT CBMs: Promoting implementation, supporting negotiations, kde zástupce Úřadu spolu se zástupkyní slovenského CSIRT.SK prezentovali v panelu týkajícím se regionální spolupráce společnou platformu států Visegrádské čtyřky a Rakouska v oblasti kybernetické bezpečnosti, tzv. CECSP.

ČR dosáhla významného úspěchu v oblasti zvyšování zabezpečenía odolnosti kritické informační infrastruktury státu skrze regionální spolupráci mezi pracovišti CERT, když byla z její a rakouské iniciativy založena v květnu 2013 Středoevropská

platforma kybernetické bezpečnosti (Central European Cyber Security Platform – CECSP). Během rakouského předsednictví se v dubnu 2014 uskutečnilo již třetí zasedání na politické úrovni, kde se hodnotil pokrok v dosavadní spolupráci na poli kybernetické bezpečnosti. Prioritou tohoto jednání bylo mj. přijetí pracovního programu CECSP pro období nadcházejících 3 let a dohody o pravidlech a principech spolupráce v rámci platformy. Další zasedání platformy, na technické úrovni se uskutečnilo v prosinci 2014. V rámci platformy se dále uskutečnilo kybernetické cvičení a pokračovalo se v budování rámce na sdílení informací.

V červnu Úřad navázal spolupráci s příslušným italským úřadem Dipartimento delle Informazioni per la Sicurezza, v říjnu s EC3 Unit Europolu a dále v listopadu s rumunským národním dohledovým pracovištěm CERT-RO. V roce 2014 byla rovněž prohlubována spolupráce se stávajícími partnerskými úřady, zejména ze Slovenska, Rakouska, Maďarska, Polska, Německa, Francie, Koreje, USA a Izraele.

Se slovenským CSIRT.SK došlo k vzájemné výměně bezpečnostních nástrojů vyvíjených jednotlivými týmy.

V případě USA se posílila spolupráce s Department of Homeland Security, který Úřadu nabídl přístup do svého neveřejného portálu a dále možnost účastnit se školení v oblasti průmyslových řídicích systémů. Posílila se i spolupráce s Federálním úřadem pro vyšetřování (Federal Bureau of Investigation), který připravil pro pracovníky Úřadu školení.

Kybernetická bezpečnost se stala jedním z bodů mezivládních konzultací vlády České republiky a Státu Izrael, které se uskutečnily v listopadu v Jeruzalémě. Během těchto konzultací byla podepsána společná deklarace o spolupráci v oblasti kybernetické bezpečnosti. Za vládu České republiky deklaraci podepsal náměstek ředitele Úřadu Jaroslav Šmíd. Spolupráce se bude týkat:

- sdílení informací, osvědčených postupů a zkušeností týkajících se kybernetických bezpečnostních hrozeb a událostí, jakož i jiných relevantních otázek týkajících se kybernetické bezpečnosti,

- zvýšení celkové kybernetické odolnosti a připravenosti proti internetovým hrozbám prostřednictvím sdílení informací, výměny zkušeností a spolupráce v odborné přípravě včetně společných kybernetických cvičení,

- sdílení relevantních informací o projektech výzkumu a vývoje v oblasti kybernetické bezpečnosti,

- vytvoření zabezpečeného komunikačního kanálu za účelem sdílení informací týkajících se kybernetických bezpečnostních hrozeb a událostí.

Spolupráce v oblasti kybernetické bezpečnosti byla také předmětem jednání ředitele Úřadu Dušana Navrátila s komisařkou EU pro digitální agendu Neelií Kroesovou, ministrem britské vlády Francisem Maudem a koordinátorem amerického ministerstva zahraničních věcí (Department of State) Christopherem Painterem.

V rámci spolupráce mezi ČR a právní a politickou divizí NATO (Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), jejímž posláním je přispívat ke zvyšování kybernetické obrany a zlepšovat spolupráci a sdílení informací mezi účastnickými státy a NATO, vyslal Úřad v lednu 2014 jednoho zástupce do NATO CCD COE jako tzv. „voluntary national contribution“, nicméně k vlastní činnosti se Úřad připojil podepsáním tzv. Notices of Joining až v květnu a červnu.

Celkem 6 pracovníků GovCERT.CZ se v roce 2014 zúčastnilo bezplatného školení expertů, zaměřeného na analýzu malware, bezpečnostní monitoring, forenzní činnost a analýzu pokročilých síťových hrozeb. Vedle toho se 2 pracovníci NCKB účastnili týdenního kurzu zabývajícího se aplikací mezinárodního práva v oblasti kybernetické bezpečnosti.

V srpnu 2014 se GovCERT.CZ stal akreditovaným členem evropského sdružení Trusted Introducer. Toto sdružení působí v rámci evropské organizace TERENA a sdružuje evropské bezpečnostní týmy vládní, národní, komerční sféry (např. bank, provozovatelů internetového připojení, výrobců hardware atd.) nebo univerzit. Vstup mezi akreditované týmy Trusted Introducer znamená další krok k užší spolupráci se světovou infrastrukturou bezpečnostních týmů CERT nebo CSIRT.

Úřad se během roku 2014 zúčastnil celkem 6 cvičení – Cyber Europe, Locked Shields, CECSP 2014 Exercise, Cyber Czech, EU-Multi Layer a Cyber Coalition.

V rámci otevírání NCKB v Brně v květnu uspořádal Úřad kybernetickou konferenci Cyber Security – Achievements and Challenges, kde jako keynote spekaers vystoupili mimo jiné Sorin Ducaru (náměstek generálního tajemníka NATO pro nové bezpečnostní hrozby), Freddy Dezeure (ředitel CERT-EU), Udo Helmbrecht (generální ředitel ENISA), Melissa Hathaway (bývalá poradkyně amerického prezidenta George W. Bushe pro otázky kybernetické bezpečnosti) či Paul Schneider (bývalý náměstek ředitele amerického Department of Homeland Security).

2.3. PERSONÁLNÍ BEZPEČNOST

V roce 2014 v oblasti personální bezpečnosti Úřad prováděl zejména bezpečnostní řízení o žádostech fyzických osob, vydával osvědčení fyzické osoby a osvědčení fyzické osoby pro cizí moc, potvrzující cizí moci vydání osvědčení fyzické osoby a vydával rozhodnutí o nevydání osvědčení fyzické osoby.

Ve vztahu k osobám, které jsou držiteli osvědčení fyzické osoby, se činnost Úřadu zaměřovala především na provádění úkonů k prověřování, zda tyto osoby i nadále splňují podmínky stanovené zákonem pro vydání osvědčení. V této souvislosti Úřad vedl řízení o zrušení platnosti osvědčení fyzické osoby a v případech, kdy fyzická osoba přestala splňovat podmínky pro vydání osvědčení, vydával rozhodnutí o zrušení platnosti osvědčení fyzické osoby.

Úřad dále realizoval řadu dalších úkonů spojených s výše uvedenými činnostmi, např. zakládání, vedení, doplňování, evidenci a vyřazování bezpečnostních svazků, vedení evidence fyzických osob, které jsou držiteli osvědčení fyzické osoby atd.

K nejvýznamnější legislativním změnám, které v uplynulém roce měly dopad do oblasti personální bezpečnosti, patřilo nabytí účinnosti zákona č. 89/2012 Sb., občanský zákoník, a v souvislosti s tím i nabytí účinnosti novely vyhlášky č. 363/2011 Sb., o personální bezpečnosti a o bezpečnostní způsobilosti.

Úřad v oblasti personální bezpečnosti spolupracoval s orgány státu, především s Policií ČR a se zpravodajskými službami, právnickými osobami a dalšími subjekty, které disponovaly informacemi důležitými pro bezpečnostní řízení.

Součinnost, kterou v rámci bezpečnostního řízení poskytují Úřadu zpravodajské služby, Policie ČR a další spolupracující orgány státu a právnické osoby, byla i v roce 2014 na velmi dobré úrovni. V souladu s usnesením vlády ČR č. 1381 ze dne 12. prosince 2007 byla vzájemná spolupráce dále upravována. V průběhu roku byl podepsán Prováděcí protokol č. 7 uzavřený na základě čl. 15 odst. 11 Realizační dohody mezi Národním bezpečnostním úřadem, Ministerstvem vnitra, Inspekcí policie a Policií ČR.

Další oblastí činnosti Úřadu byla spolupráce s úřady cizí moci, které mají v působnosti ochranu utajovaných informací, při provádění vlastních bezpečnostních řízení (vyžadování informací). Úřad u partnerských úřadů vyžádal informace ke 212 osobám a na základě jejich žádostí prováděl šetření k 65 osobám, které byly v daném státě prověřovány pro přístup k utajovaným informacím.

2.3.1. Bezpečnostní řízení o žádostech fyzických osob

Ze statistických údajů ohledně bezpečnostního řízení o žádostech fyzických osob, které jsou přehledně shrnuty v kapitole 2.3.5., vyplývá, že v průběhu roku 2014 bylo Úřadem přijato 5 067 žádostí o vydání osvědčení fyzické osoby, což je přibližně stejný počet jako v roce předchozím. Největší podíl tvořily žádosti o vydání osvědčení fyzické osoby pro stupeň utajení Tajné (56 %), oproti loňskému roku došlo k nárůstu počtu žádostí pro stupeň utajení Důvěrné o 35 %. Obdobně jako v předchozích letech byl největší počet žádostí přijat v posledním čtvrtletí hodnoceného roku, a to v počtu 1 927, což činí více než jednu třetinu z celkového počtu přijatých žádostí za rok 2014. O většině těchto žádostí tak bude rozhodnuto až v roce 2015.

Celkem bylo v loňském roce rozhodnuto ve 4 840 případech o vydání osvědčení fyzické osoby a ve 24 případech o nevydání osvědčení. Ve 134 případech pak bylo bezpečnostní řízení zastaveno. Nejčastějším důvodem zastavení bezpečnostního řízení bylo zpětvzetí žádosti účastníkem řízení (55 případů). Významný podíl na zastavení bezpečnostního řízení měla také povinnost odpovědné osoby neprodleně oznámit Úřadu pominutí skutečností odůvodňujících nutnost přístupu fyzické osoby k utajovaným informacím (46 případů). Úřad tak mohl probíhající bezpečnostní řízení zastavit, neboť důvod řízení zanikl. Tím došlo ke snížení nákladů Úřadu a s ním spolupracujících orgánů a organizací, neboť nebylo nutné v těchto případech bezpečnostní řízení dokončovat. Současně tím byl

posílen princip „need to know“, jehož hlavním smyslem je, aby k utajovaným informacím mohly mít přístup pouze osoby, které tyto informace k výkonu své pracovní nebo jiné obdobné činnosti nezbytně potřebují znát.

2.3.2. Prověřování splňování podmínek po vydání osvědčení

Významný objem činnosti Úřadu v oblasti personální bezpečnosti souvisel s prověřováním, zda fyzická osoba, která je držitelem osvědčení fyzické osoby, i nadále splňuje podmínky pro jeho vydání. Prověřeno takto bylo celkem 3 400 držitelů osvědčení. Tato činnost byla standardně prováděna před vydáním osvědčení pro cizí moc a v případech, kdy Úřad obdržel od zpravodajských služeb, Ministerstva vnitra nebo Policie ČR informace, jejichž obsah nasvědčoval tomu, že držitel osvědčení fyzické osoby by mohl přestat splňovat podmínky pro jeho vydání, nebo tyto informace vyplynuly z nahlášených změn samotným držitelem osvědčení fyzické osoby, případně je Úřad získal přímo svou vlastní činností (např. z průběžného monitoringu tzv. otevřených zdrojů). Nezanedbatelnou část takto prověřených případů tvořilo rovněž periodické ověřování realizované po dobu platnosti příslušného osvědčení. Ve 182 případech toto prověřování vyústilo v zahájení řízení o zrušení platnosti osvědčení fyzické osoby, které bylo ve 48 případech ukončeno vydáním rozhodnutí o zrušení platnosti osvědčení fyzické osoby (viz kap. 2.3.5. Statistické přehledy).

2.3.3. Analýza důvodů nevydání nebo zrušení platnosti osvědčení fyzické osoby

Jak již bylo uvedeno v kapitolách 2.3.1. a 2.3.2., v minulém roce ve 24 případech nebylo žadateli osvědčení vydáno a ve 48 případech bylo rozhodnuto o zrušení platnosti osvědčení.

Převládajícím důvodem pro nevydání nebo zrušení platnosti osvědčení fyzické osoby bylo, jako v roce 2013, nesplnění podmínky bezpečnostní spolehlivosti podle § 12 odst. 1 písm. d) zákona, a to především z důvodu výskytu bezpečnostního rizika podle § 14 odst. 3 písm. d) zákona, tedy chování, které má vliv na důvěryhodnost nebo ovlivnitelnost osoby a může ovlivnit její schopnost utajovat informace.

Toto bezpečnostní riziko samo o sobě zahrnuje velký rozsah faktických důvodů. V roce 2014 měly tyto důvody opětovně příčinnou souvislost se skutečnostmi vyplývajícími z trestního či přestupkového řízení s tím, že nemalým dílem byly dokladovány i zjištěními příslušných zpravodajských služeb. Převážnou motivací k chování, které mělo vliv na důvěryhodnost nebo ovlivnitelnost žadatele či držitele osvědčení, bylo nejen získání majetkového či jiného prospěchu, ale narostl i počet případů, kdy takovou motivací bylo toliko posílení a utužení negativních interpersonálních vazeb (klientelismus), tedy bez zaznamenání okamžitého prospěchu v majetkové sféře dotčených osob.

Byť nejčetnějším shledáním uvedeného bezpečnostního rizika byly opětovně případy neodpovědného až laxního přístupu žadatelů či držitelů osvědčení k jejich závazkovým vztahům, díky němuž se ocitli v neudržitelné finanční, potažmo majetkové situaci, čímž se stali osobami významně ovlivnitelnými, oproti roku 2013

se počet takových případů snížil. Úřad v tomto ohledu zaznamenal zvýšený zájem takových žadatelů či držitelů osvědčení o využití institutu oddlužení.

Na druhou stranu nárůst oproti roku 2013 souvisel s případy, ve kterých shledání tohoto bezpečnostního rizika bylo konstatováno pro chování, na kterém se podílelo nadměrné zneužívání návykových látek, především konzumace alkoholických nápojů.

Ostatní rizika uvedená v § 14 odst. 2 a 3 zákona byla konstatována v roce 2014 ojediněle. Na tomto místě je nutno uvést, že v roce 2014 Úřad již nezaznamenal případy tzv. historických rizik, tedy činnosti spočívající v potlačování základních lidských práv a svobod před rokem 1989. To však neznamená, že v tomto ohledu takovou činnost neidentifikoval u žadatelů či držitelů osvědčení v nedávné minulosti, např. extrémismus. Také v roce 2014 byly zjištěny případy výskytu dalšího obligatorního bezpečnostního rizika – závažná nebo opakovaná činnost proti zájmům ČR, v souvislosti s takovou činností v procesu zadávání veřejných zakázek. V tomto ohledu lze říci, že uvedené obligatorní bezpečnostní riziko, které bylo dříve výlučně konstatováno na základě podkladů od příslušných zpravodajských služeb, bylo v roce 2014 Úřadem konstatováno též na základě podkladů od orgánů činných v trestním řízení.

V roce 2014 poklesl i počet případů nevydání či zrušení platnosti osvědčení pro nesplnění podmínky bezúhonnosti podle § 6 odst. 2 písm. c) zákona, kdy stále převažuje řízení motorových vozidel nebo vykonávání jiné činnosti pod vlivem návykových látek.

2.3.4. Přehled ostatních důvodů zániku platnosti osvědčení fyzické osoby

V uplynulém období zanikla platnost celkem 4 321 osvědčení, přičemž největší část případů představoval zánik platnosti osvědčení doručením nového osvědčení fyzické osoby, a to v celkovém počtu 2 939. Významným se v uplynulém hodnoceném období také jevil zánik platnosti osvědčení fyzické osoby projevem vůle držitele osvědčení, tzn., že držitel osvědčení vrátil, neboť už nadále nepotřeboval mít přístup k utajované informaci (995 případů).

Z výše uvedeného je zřejmé, že se stále pozitivně projevují dva z principů novelizace zákona, které stanoví, že fyzické osobě je umožněn přístup k utajované informaci na základě pouze jednoho osvědčení a že platnost osvědčení zaniká také projevem vůle jeho držitele. Uplatněním těchto ustanovení v praxi se snižuje počet vydaných osvědčení, a tím i administrativní zátěž Úřadu.

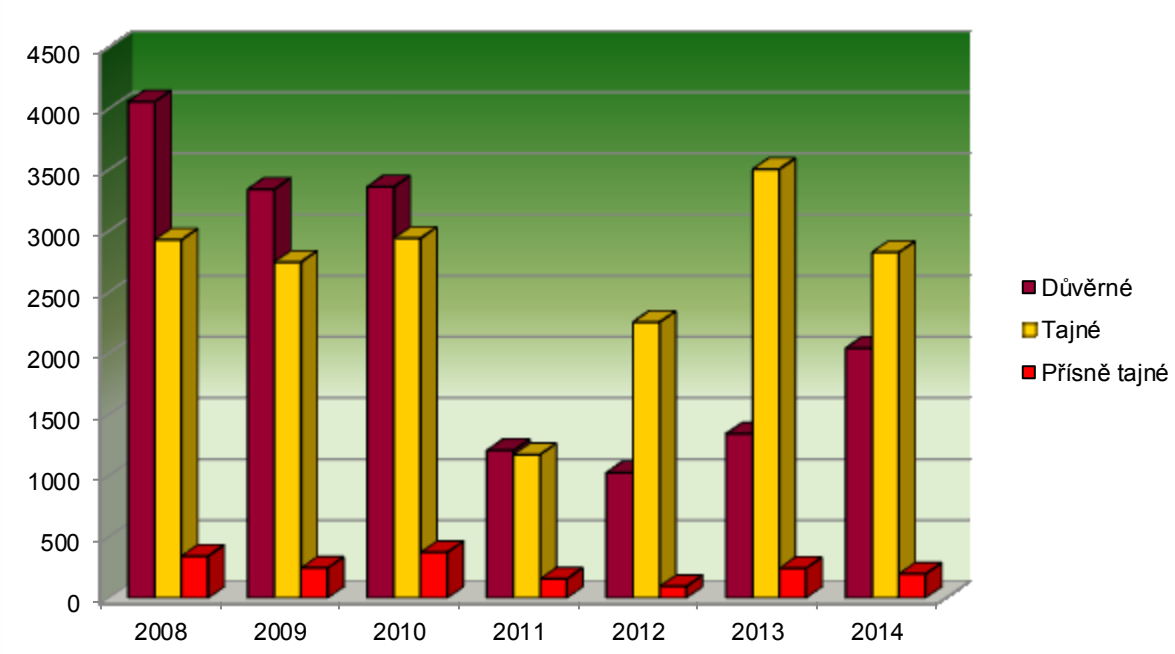
Počet případů zániku platnosti osvědčení fyzické osoby v roce 2014 podle jednotlivých důvodů je přehledně uveden v následující kapitole 2.3.5.

2.3.5. Statistické přehledy

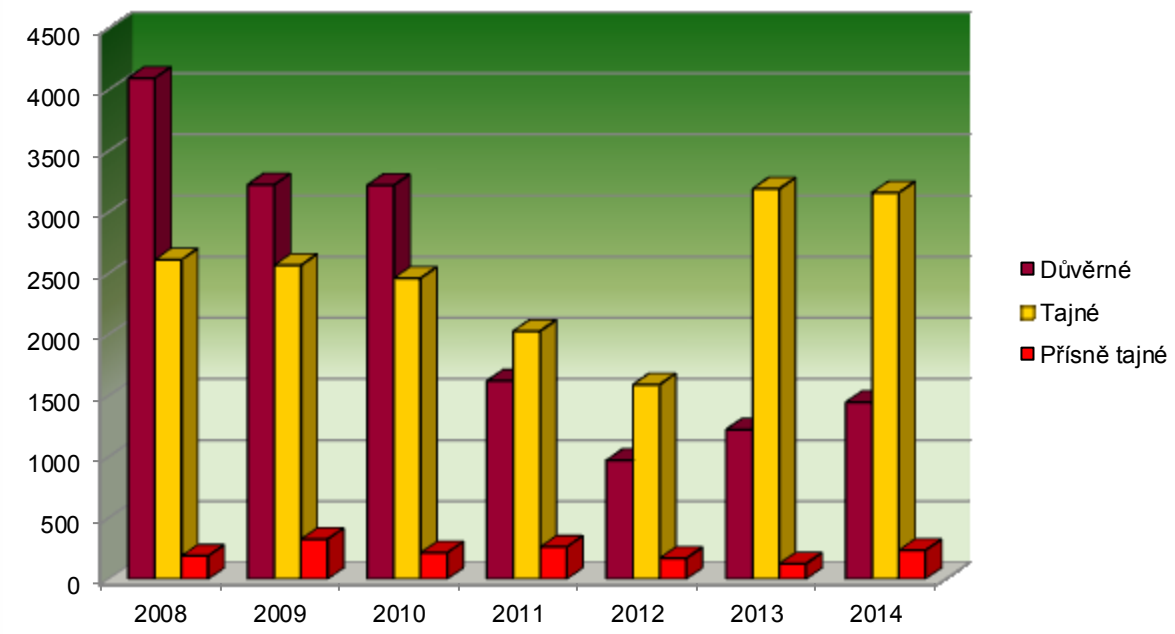
Přijaté žádosti a ukončená bezpečnostní řízení v roce 2014

	Důvěrné	Tajné	Přísně tajné	Celkem
Přijaté žádosti	2 043	2 827	197	**5 067**
Osvědčení vydáno	1 445	3 160	235	**4 840**
Osvědčení nevydáno	9	14	1	**24**
Řízení zastaveno	60	67	7	**134**

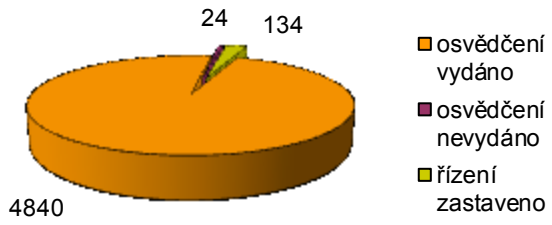
Přijaté žádosti o vydání osvědčení fyzické osoby v letech 2008 až 2014



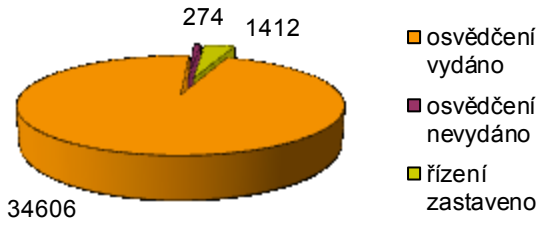
Vydaná osvědčení fyzické osoby v letech 2008 až 2014



Ukončená bezpečnostní řízení v roce 2014



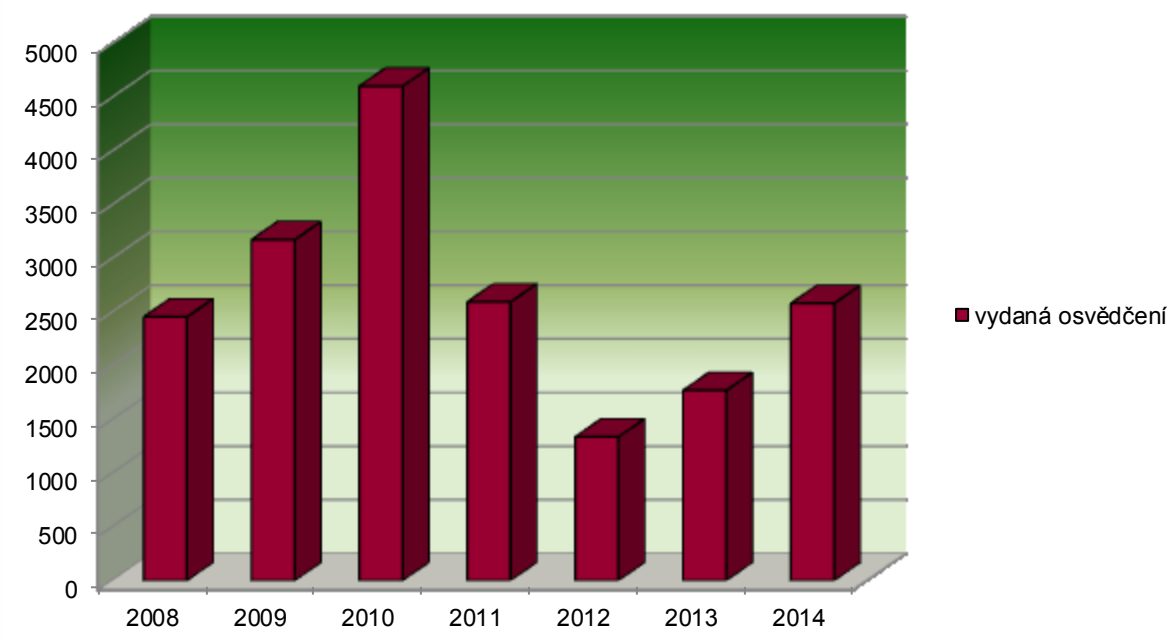
Ukončená bezpečnostní řízení v letech 2008 až 2014



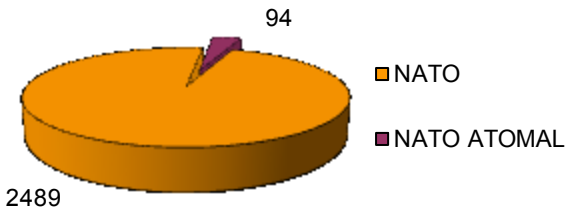
Vydaná osvědčení fyzické osoby pro cizí moc v roce 2014

COSMIC TOP SECRET	258
COSMIC TOP SECRET ATOMAL	67
NATO SECRET	2 105
NATO SECRET ATOMAL	27
NATO CONFIDENTIAL	126
Celkem	**2 583**

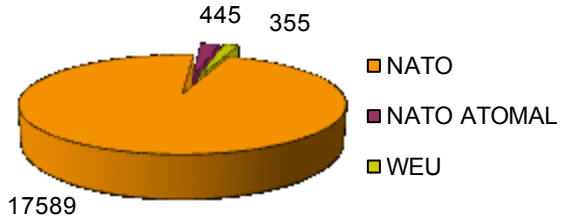
Vydaná osvědčení fyzické osoby pro cizí moc v letech 2008 až 2014



Osvědčení pro cizí moc v roce 2014



Osvědčení pro cizí moc v letech 2008 až 2014[1)]



Zánik platnosti osvědčení fyzické osoby podle důvodu v roce 2014

Zrušení platnosti osvědčení	48
Úmrtí držitele osvědčení	27
Ohlášení odcizení nebo ztráty osvědčení	61
Poškození osvědčení	10
Změna některého z údajů uvedených v osvědčení	209
Vrácení osvědčení	995
Doručení nového osvědčení	2 939
Vznik služebního nebo pracovního poměru u ZS	32
Celkem	**4 321**

Zastavení bezpečnostního řízení v roce 2014

Nedání souhlasu podle § 107 zákona	0
Ve stanovené lhůtě nebyly odstraněny nedostatky v žádosti	19
Uvedení nepravdivé nebo neúplné výpovědi	10
Nesplnění podmínek – dosažení 18 let věku, svéprávnosti, bezúhonnosti	2
Úmrtí	1
Oznámení odpovědné osoby, že pominuly skutečnosti, kterými byla žádost odůvodněna	46
Zpětvzetí žádosti	55
Ostatní	1
Celkem	**134**

2.3.6. Personální projekt

V souladu s § 72 zákona předložila ministerstva a další ústřední správní úřady své personální projekty. Usnesením vlády ČR ze dne 19. června 2012 č. 439 byl schválen Postup při zpracovávání personálních projektů a jejich ověřování Národním

[1)] Osvědčení fyzické osoby pro cizí moc pro přístup k utajovaným informacím Západoevropské unie (Western European Union) byla vydávána pouze do roku 2011, neboť tato organizace ukončila svou činnost ke dni 30. června 2011.

bezpečnostním úřadem. V něm bylo uloženo členům vlády a vedoucím ostatních ústředních správních úřadů postupovat podle materiálu schváleného v tomto usnesení a poskytovat řediteli Úřadu součinnost při zpracovávání vyjádření k personálním projektům a jejich ověřování. Předmětný materiál stanovuje jednotný obsah, formu a strukturu personálních projektů a upravuje i způsob jejich hodnocení Úřadem.

Účelem zpracování personálních projektů je získat celkový přehled o situaci v oblasti personální bezpečnosti a zhodnocení stavu z hlediska počtu fyzických osob, které žádají o vydání osvědčení fyzické osoby, ve vztahu ke skutečným potřebám a četnosti výskytu utajovaných informací u jednotlivých ministerstev a ústředních správních úřadů. Touto cestou je dosahováno snižování počtu nadbytečných nových žádostí o vydání osvědčení fyzické osoby pro přístup k utajovaným informacím oproti původním předpokladům uváděným v předchozích letech. Úřad zároveň i nadále metodicky působí na ústřední správní úřady, aby byly zohledněny veškeré podmínky pro držení osvědčení, zejména zásada „need to know“, tedy potřeba přístupu k utajované informaci, jež je nezbytná pro výkon pracovní činnosti, neboť jiný důvod přístupu k utajované informaci nelze akceptovat.

V roce 2014 bylo vyjádření Úřadu k personálním projektům předloženo do připomínkového řízení dotčeným ministerstvům a orgánům státní správy. Největší počet žádostí na rok 2015 je plánován rezortem Ministerstva obrany (3 200 žádostí) a Ministerstva vnitra (1 076 žádostí). 70 % z tohoto počtu by však měly tvořit tzv. opakované žádosti, kdy fyzická osoba potřebuje mít přístup k utajované informaci i bezprostředně po uplynutí doby platnosti dosavadního osvědčení fyzické osoby.

Na základě předložených personálních projektů a vypořádání vznesených připomínek zpracoval Úřad materiál pro jednání vlády, který vláda ČR projednala dne 3. listopadu 2014 a vydala usnesení č. 893, kterým schválila předložené personální projekty. Tímto usnesením zároveň uložila ministrům a vedoucím ostatních ústředních správních úřadů postupovat při zpracování a vedení přehledu míst a funkcí, na kterých je nezbytné mít přístup k utajovaným informacím, a při potvrzování zdůvodnění nutnosti přístupu fyzické osoby k utajované informaci tak, aby žádosti o vydání osvědčení fyzické osoby byly podávány jen v případech odůvodněné a nezbytné potřeby přístupu fyzické osoby k utajované informaci. Dále uložila trvale přehodnocovat seznamy míst a funkcí, na kterých je nezbytné mít přístup k utajovaným informacím. Řediteli Úřadu vláda uložila zajistit na žádost příslušného ministra nebo vedoucího ústředního správního úřadu metodickou podporu při plnění uvedených úkolů.

2.4. BEZPEČNOSTNÍ ZPŮSOBILOST

V roce 2014 Úřad vedl, ve smyslu části čtvrté zákona, bezpečnostní řízení k žádostem o vydání dokladu o bezpečnostní způsobilosti fyzických osob (dále jen „doklad“), vydával doklad, vydával rozhodnutí o nevydání dokladu, dále prověřoval, zda fyzické osoby, které již jsou držiteli dokladu, i nadále splňují podmínky pro jeho vydání, vydával rozhodnutí o zrušení platnosti dokladu a realizoval řadu dalších

úkonů s tím spojených, např. zakládání, vedení, doplňování, evidenci a vyřazování bezpečnostních svazků, vedení evidence fyzických osob, které jsou držiteli dokladu atd.

Většinu podaných žádostí o vydání dokladu tvořily žádosti související s výkonem nové citlivé činnosti v oblasti nakládání s bezpečnostním materiálem, a to v celkovém počtu 202 žádostí. Dne 1. ledna 2014 totiž nabyl účinnosti zákon č. 229/2013 Sb., o nakládání s některými věcmi využitelnými k obranným a bezpečnostním účelům na území České republiky (zákon o nakládání s bezpečnostním materiálem). Tento právní předpis nahradil doposud platný zákon č. 310/2006 Sb. Zákon o nakládání s bezpečnostním materiálem stanovil v § 6 odst. 2 nové citlivé činnosti. Vzhledem k problémům při aplikaci tohoto zákona v praxi, kdy vznikaly potíže jak ve výkladu pojmu „citlivá činnost v oblasti zákona o nakládání s bezpečnostním materiálem“ (tj. které osoby citlivou činnost skutečně vykonávají), tak při jednoznačném určení, který materiál je bezpečnostním materiálem skupin 5 a 6, případně který orgán státní správy je kompetentní toto potvrdit, byl uvedený zákon ještě v průběhu roku 2014 novelizován. Dne 19. listopadu 2014 tak nabyl účinnosti zákon č. 266/2014 Sb., kterým se mění zákon č. 229/2013 Sb., o nakládání s některými věcmi využitelnými k obranným a bezpečnostním účelům na území České republiky (zákon o nakládání s bezpečnostním materiálem), ve znění zákona č. 64/2014 Sb. Touto novelou byly veškeré citlivé činnosti stanovené zákonem o nakládání s bezpečnostním materiálem zrušeny.

Součinnost, kterou Úřadu v rámci bezpečnostního řízení poskytuje Policie ČR, zpravodajské služby a další spolupracující orgány státu, lze označit jako velmi dobrou a efektivní.

V roce 2014 pokračovala diskuse o dalším využívání institutu bezpečnostní způsobilosti. Úřad je připraven dále pokračovat v jednání o smysluplném a efektivním rozšíření portfolia přesně vymezených citlivých činností, jejichž výkon by byl podmíněn držením platného dokladu. Úřad také participoval na připravované rozsáhlé novele atomového zákona, která mimo jiné klade i větší nároky na bezpečnostní způsobilost osob, které vstupují do vyhrazených prostor jaderných zařízení.

2.4.1. Statistické přehledy

Přehled přijatých žádostí a ukončených bezpečnostních řízení v roce 2014

Citlivá činnost podle	Přijaté žádosti	Doklad vydán	Doklad nevydán	Řízení zastaveno	Zrušení platnosti dokladu
§ 8 zákona č. 38/1994 Sb.[2)]	92	45	0	6	1
§ 2a zákona č. 18/1997 Sb.[3)]	55	58	0	3	0
§ 6 zákona č. 229/2013 Sb.[4)]	202	101	0	41	0
§ 25c odst. 10 zákona č. 61/1988 Sb.[5)]	1	1	0	0	0
§ 157a zákona č. 137/2006 Sb.[6)]	11	8	0	0	0
§ 2a zákona č. 312/2006 Sb.[7)]	29	30	0	3	0
Ostatní	7	6	0	0	0
Celkem	**397**	**249**	**0**	**53**	**1**

2.5. PRŮMYSLOVÁ BEZPEČNOST

Mezi hlavní činnosti, které Úřad realizoval v oblasti průmyslové bezpečnosti v roce 2014, patří zejména provádění bezpečnostních řízení o žádostech podnikatelů o vydání osvědčení podnikatele, v jejichž závěru Úřad vydával osvědčení podnikatele nebo rozhodnutí o nevydání osvědčení podnikatele. Úřad dále přijímal žádosti podnikatelů o vydání osvědčení podnikatele pro cizí moc a při splnění zákonem stanovených podmínek vydával osvědčení podnikatele pro cizí moc, potvrzující cizí moci provedení bezpečnostního řízení u podnikatele a vydání osvědčení podnikatele.

Ve vztahu k podnikatelům, kteří jsou držiteli osvědčení podnikatele, se činnost Úřadu zaměřovala především na provádění úkonů k prověřování, zda držitelé i nadále splňují podmínky stanovené zákonem pro vydání osvědčení podnikatele, a to jak v návaznosti na hlášení změn údajů uvedených v žádosti podnikatele oznamovaných jednotlivými držiteli osvědčení podnikatele, tak i na základě skutečností získaných Úřadem z vlastní činnosti nebo informací poskytnutých Úřadu

---

[2)] Zákon č. 38/1994 Sb., o zahraničním obchodu s vojenským materiálem a o doplnění zákona č. 455/1991 Sb., o živnostenském podnikání (živnostenský zákon), ve znění pozdějších předpisů, a zákona č. 140/1961 Sb., trestní zákon, ve znění pozdějších předpisů, ve znění pozdějších předpisů.

[3)] Zákon č. 18/1997 Sb., o mírovém využívání jaderné energie a ionizujícího záření (atomový zákon) a o změně a doplnění některých zákonů, ve znění pozdějších předpisů.

[4)] Zákon č. 229/2013 Sb., o nakládání s některými věcmi využitelnými k obranným a bezpečnostním účelům na území České republiky (zákon o nakládání s bezpečnostním materiálem), ve znění zákona č. 64/2014 Sb.

[5)] Zákon č. 61/1988 Sb., o hornické činnosti, výbušninách a o státní báňské správě, ve znění pozdějších předpisů.

[6)] Zákon č. 137/2006 Sb., o veřejných zakázkách, ve znění pozdějších předpisů.

[7)] Zákon č. 312/2006 Sb., o insolvenčních správcích, ve znění pozdějších předpisů.

orgány státu, jinými orgány či osobami. V této souvislosti Úřad dále vedl řízení o zrušení platnosti osvědčení podnikatele a v případech, kdy podnikatel přestal splňovat podmínky pro vydání osvědčení podnikatele, vydával rozhodnutí o zrušení platnosti takových osvědčení.

V rámci průmyslové bezpečnosti se dále v roce 2014 pokračovalo v ověřování a prověřování realizace administrativní bezpečnosti podnikateli poté, co byla v roce 2013 tato agenda převedena do působnosti sekce bezpečnostního řízení.

V oblasti průmyslové bezpečnosti Úřad realizoval řadu dalších úkonů spojených s činnostmi uvedenými shora, jako např. zakládání, vedení, doplňování, evidence a vyřazování bezpečnostních svazků, vedení evidence podnikatelů, kteří jsou držiteli osvědčení podnikatele atd.

Z legislativních změn, majících vazbu a dopad do oblasti průmyslové bezpečnosti, patřila v roce 2014 mezi nejvýznamnější nabytí účinnosti zákona č. 89/2012 Sb., občanský zákoník, a zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích), a v souvislosti s nimi nabytí účinnosti zákona č. 303/2013 Sb., kterým se mění některé zákony v souvislosti s přijetím rekodifikace soukromého práva, kterým byl novelizován zákon, a dále nabytí účinnosti novely vyhlášky č. 405/2011 Sb., o průmyslové bezpečnosti. V důsledku těchto změn došlo k úpravě a rozšíření dílčích úkonů Úřadu prováděných v rámci bezpečnostního řízení a v rámci prověřování, zda držitelé osvědčení podnikatele nadále splňují podmínky stanovené zákonem pro jeho vydání.

V roce 2014 i nadále probíhala velmi dobrá a efektivní součinnost Policie ČR, zpravodajských služeb a dalších orgánů státu a právnických osob spolupracujících s Úřadem v rámci prováděných bezpečnostních řízení i v rámci prověřování splňování podmínek pro vydání osvědčení podnikatele držiteli osvědčení.

2.5.1. Bezpečnostní řízení o žádostech podnikatelů

V průběhu roku 2014 bylo Úřadem přijato 78 žádostí podnikatelů o vydání osvědčení podnikatele. Z tohoto počtu bylo k 31. prosinci 2014 rozhodnuto o 32 žádostech, u zbylých 46 žádostí k tomuto datu bezpečnostní řízení o žádosti podnikatele probíhala.

Ve srovnání s rokem 2013 došlo k drobnému nárůstu počtu přijatých žádostí, a to celkem o 13 žádostí. Při srovnávání počtů podaných žádostí s lety předcházejícími je nezbytné přihlédnout ke dvěma významným faktorům. Prvním, všeobecně pozitivně přijímaným faktorem, který se odráží v počtech podaných žádostí podnikatelů, je absence bezpečnostního řízení pro přístup podnikatele k utajované informaci stupně utajení Vyhrazené. Druhým faktorem je skutečnost, že počty podaných žádostí podnikatelů jsou nadále ovlivňovány přetrvávajícími dopady celosvětové ekonomické recese, které se v podmínkách ČR promítly mj. snížením počtu veřejných zakázek nebo zadávacích řízení, u kterých je nezbytný přístup k utajovaným informacím. Neopomenutelným aspektem, který úzce souvisí s ekonomickou situací a výrazně se promítá do počtu podaných žádostí, jsou změny ve vývoji podnikatelského prostředí, kde spočívají v transformacích obchodních

společností formou různých typů přeměn nebo se projevují ve formě úpadků nebo zániků obchodních společností.

2.5.2. Prověřování splňování podmínek po vydání osvědčení podnikatele

V roce 2014 probíhalo standardním způsobem prověřování, zda držitelé osvědčení podnikatele nadále splňují zákonem stanovené podmínky pro jejich vydání. V souvislosti s rekodifikací soukromoprávních norem (viz kap. 2.5.) došlo k úpravě a rozšíření některých úkonů prováděného prověřování.

Ve vztahu k prověřování změn údajů uvedených v žádostech o vydání osvědčení podnikatele, které podnikatelé oznamují Úřadu v souladu s § 68 písm. d) zákona, lze i nadále konstatovat, že díky změně data, ke kterému jsou podnikatelé povinni změny údajů uvedených v žádostech hlásit, která je účinná od roku 2012, a kterou byl nahrazen předchozí jednotný termín 1. listopadu, nedopadá veškerá zátěž spojená s prověřováním oznámených změn do jednoho úzkého období roku, ale úkony jsou rozloženy rovnoměrně v průběhu celého roku, čímž je zajištěna požadovaná kvalita jejich provedení a nedochází k jednorázovému přetížení Úřadu ani dalších s Úřadem spolupracujících orgánů a organizací.

2.5.3. Analýza důvodů nevydání nebo zrušení platnosti osvědčení podnikatele

V roce 2014 rozhodl Úřad ve 2 bezpečnostních řízeních vedených o žádosti podnikatele o nevydání osvědčení podnikatele. Z hlediska struktury spočíval důvod nevydání v nesplnění podmínky podle § 16 odst. 1 písm. b) zákona.

Za totéž období Úřad rozhodl v 5 případech o zrušení platnosti osvědčení podnikatele. Důvodem pro zrušení platnosti osvědčení podnikatele bylo ve všech případech nesplnění podmínky bezpečnostní spolehlivosti podle § 16 odst. 1 písm. b) zákona.

2.5.4. Přehled ostatních důvodů zániku platnosti osvědčení podnikatele

Sledovanými kategoriemi jsou nové, respektive v posledních letech výrazně novelizované instituty zániku platnosti osvědčení podnikatele.

V roce 2014 mezi důvody zániku platnosti osvědčení podnikatele převažoval zánik platnosti osvědčení podnikatele z důvodu doručení nového osvědčení podnikatele pro stejnou formu přístupu podnikatele k utajované informaci, celkem 27 případů. Druhým nejčastějším důvodem zániku platnosti osvědčení podnikatele pak byl zánik platnosti osvědčení podnikatele jeho vrácením držitelem, celkem 18 případů. V případě druhého uvedeného důvodu došlo oproti roku 2013 k významnému snížení počtu zániků platnosti osvědčení podnikatele (v roce 2013 se jednalo o celkem 48 případů).

Počet případů zániku platnosti osvědčení podnikatele v roce 2014 podle jednotlivých důvodů je uveden v kapitole 2.5.5.

2.5.5. Statistické přehledy

Přijaté žádosti o vydání osvědčení podnikatele v roce 2014

Důvěrné	Tajné	Přísně tajné	Celkem
51	27	0	**78**

Stav zpracování žádostí o vydání osvědčení podnikatele přijatých v roce 2014

Osvědčení vydáno	Osvědčení nevydáno	Řízení zastaveno	Probíhalo k 31.12.2014	Celkem
25	0	7	46	**78**

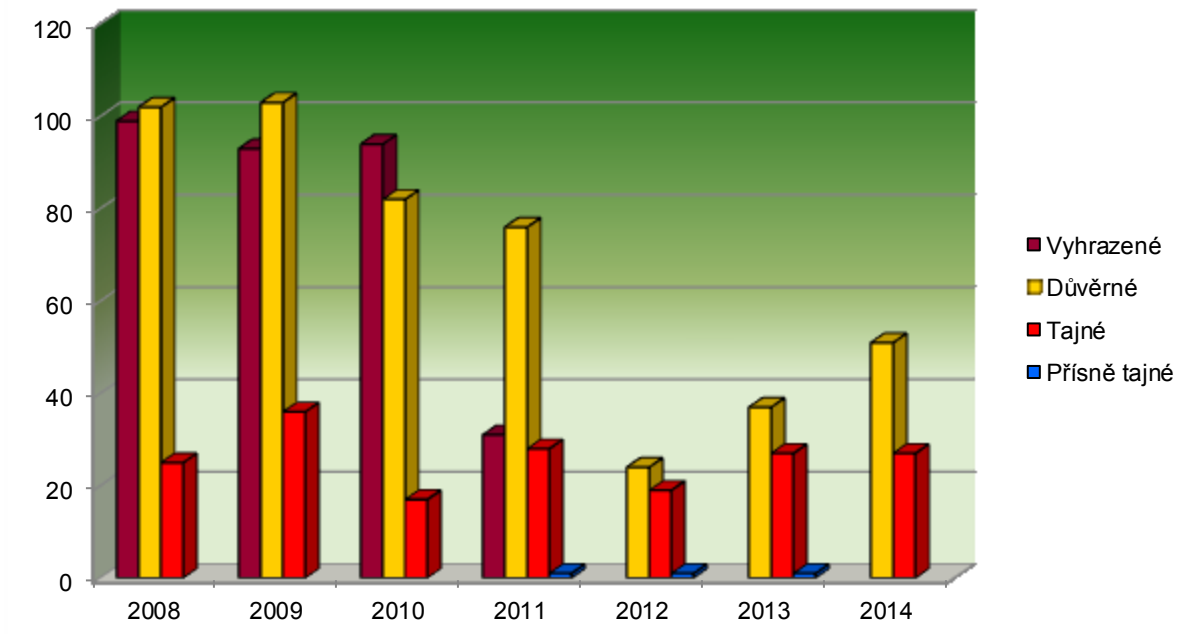
Vydaná osvědčení podnikatele v roce 2014

Důvěrné	Tajné	Přísně tajné	Celkem
65	34	1	**100**[8)]

Řízení o zrušení platnosti osvědčení podnikatele v roce 2014

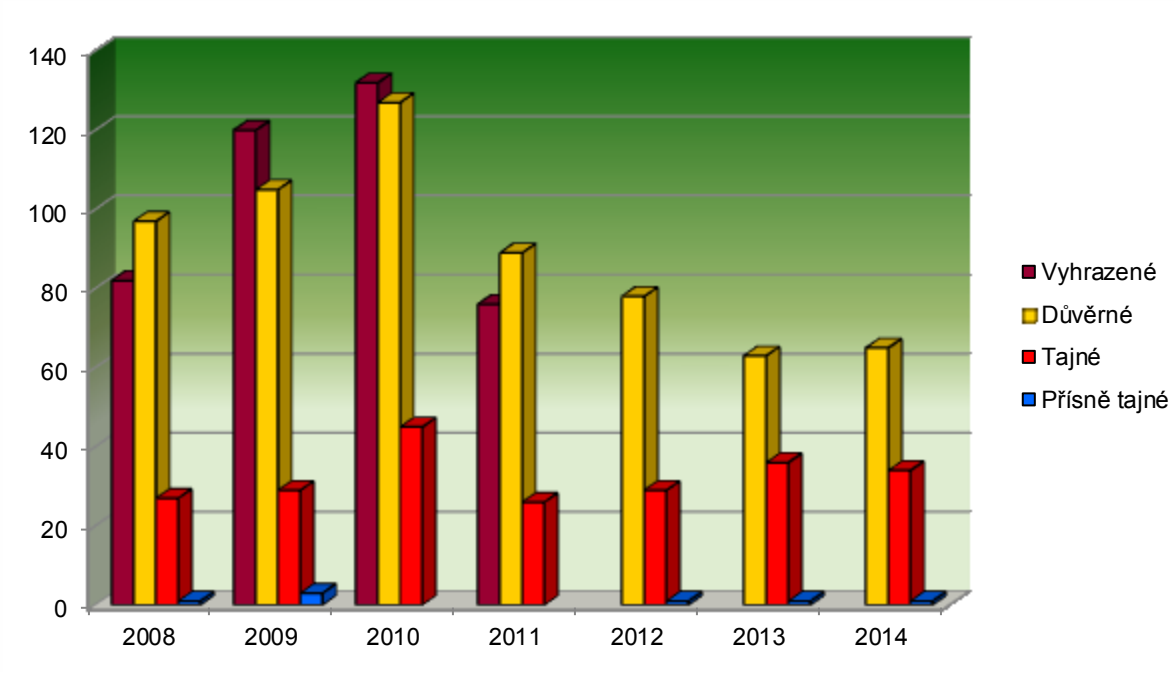
Zahájená řízení	Platnost zrušena	Řízení zastaveno	Probíhalo k 31.12.2014
13	5	15	17

Přijaté žádosti o vydání osvědčení podnikatele v letech 2008 až 2014



[8)] Uvedený počet zahrnuje osvědčení podnikatele vydaná na základě provedeného bezpečnostního řízení i osvědčení podnikatele vydaná postupem podle § 56 odst. 4 zákona (výměna osvědčení).

Vydaná osvědčení podnikatele v letech 2008 až 2014



Zánik platnosti osvědčení podnikatele podle důvodu v roce 2014

Uplynutí doby platnosti osvědčení	5
Zrušení platnosti osvědčení	5
Zrušení podnikatele	3
Ohlášení odcizení nebo ztráty osvědčení	1[9)]
Poškození osvědčení	0[9)]
Změna některého z údajů uvedených v osvědčení	2[9)]
Vrácení osvědčení	18
Doručení nového osvědčení pro stejnou formu přístupu k UI	27
Doručení rozhodnutí o nevydání osvědčení pro stejnou formu přístupu k UI	0
Celkem	**61**

2.6. BEZPEČNOST INFORMAČNÍCH A KOMUNIKAČNÍCH SYSTÉMŮ A KRYPTOGRAFICKÁ OCHRANA

Úřad odpovídá za provádění certifikace informačních systémů a za schvalování projektů bezpečnosti komunikačních systémů nakládajících

[9)] Počet případů zániku platnosti osvědčení podnikatele, při kterých nebyl uplatněn postup výměny osvědčení podle § 56 odst. 4 zákona, a došlo tak i k zániku možnosti přístupu podnikatele k utajované informaci; nezahrnuje tedy případy, kdy došlo k vydání nového osvědčení podnikatele na základě žádosti podané v zákonné 15denní lhůtě.

s utajovanými informacemi a v roli národní bezpečnostní akreditační autority dále za akreditaci lokalit informačních systémů NATO a EU rozmístěných na území ČR.

V oblasti kryptografické ochrany utajovaných informací Úřad provádí nebo zajišťuje výzkum, vývoj a výrobu národních kryptografických prostředků, vývoj a schvalování národních kryptografických algoritmů, výzkum, vývoj, výrobu a distribuci kryptografických materiálů, certifikaci kryptografických prostředků, certifikaci kryptografických pracovišť a zkoušky zvláštní odborné způsobilosti pracovníků kryptografické ochrany.

Úřad dále provádí měření kompromitujícího vyzařování elektrických a elektronických zařízení nakládajících s utajovanými informacemi a hodnotí je z hlediska způsobilosti k ochraně utajovaných informací a podobně speciálním měřením zjišťuje způsobilost zabezpečených oblastí a objektů k ochraně před únikem utajovaných informací kompromitujícím vyzařováním. Do této oblasti činnosti patří také certifikace stínicích komor a zajišťování obranně technických prohlídek.

V roce 2014 Úřad zpracoval a vydal v rámci dalšího rozvoje bezpečnostních standardů bezpečnostní standard NBÚ - 1/2013, Podmínky provozu kryptografických prostředků typu TCE 621 a center řízení TCE 671, verze 1.1, ze dne 22. září 2014 a bezpečnostní standard NBÚ - 1/2014, Podmínky, způsob a postupy vyřazování a ničení kryptografického prostředku a materiálu k zajištění jeho funkce, verze 1.0, ze dne 22. září 2014. Bezpečnostní standardy NBÚ jsou poskytovány v souladu s jejich stupněm utajení a s uplatněním zásady „need to know“.

Průběžně byly zpracovávány nebo aktualizovány další metodické materiály a vyjádření, zabývající se dílčími problémy zabezpečení informačních systémů, zejména nastavením bezpečnostních charakteristik nejčastěji používaných operačních systémů, aplikací kryptografické ochrany a aplikací ochrany proti úniku utajované informace kompromitujícím vyzařováním. Metodické materiály jsou zveřejňovány nebo poskytovány žadatelům o certifikaci a provozovatelům informačních systémů nakládajících s utajovanými informacemi podle skutečné potřeby. Pro potřeby orgánů státu bylo prováděno hodnocení vybraných produktů poskytujících bezpečnostní funkce pro informační systémy.

2.6.1. Certifikační a akreditační činnost

Nezbytnou zákonnou podmínkou pro používání informačních systémů, kryptografických prostředků, stínicích komor a zákonem stanovených kryptografických pracovišť při ochraně utajovaných informací je jejich certifikace.

2.6.1.1. Certifikace a akreditace informačních systémů

K žádostem o certifikaci informačních systémů rozpracovaným v předchozím roce přibylo v roce 2014 dalších 104 žádostí, včetně žádostí o opakovanou certifikaci, a to 39 ze státní a 65 ze soukromé sféry. Ve 24 případech byla podána žádost o certifikaci nově budovaného informačního systému, pouze 7 takových žádostí pocházelo ze státní správy.

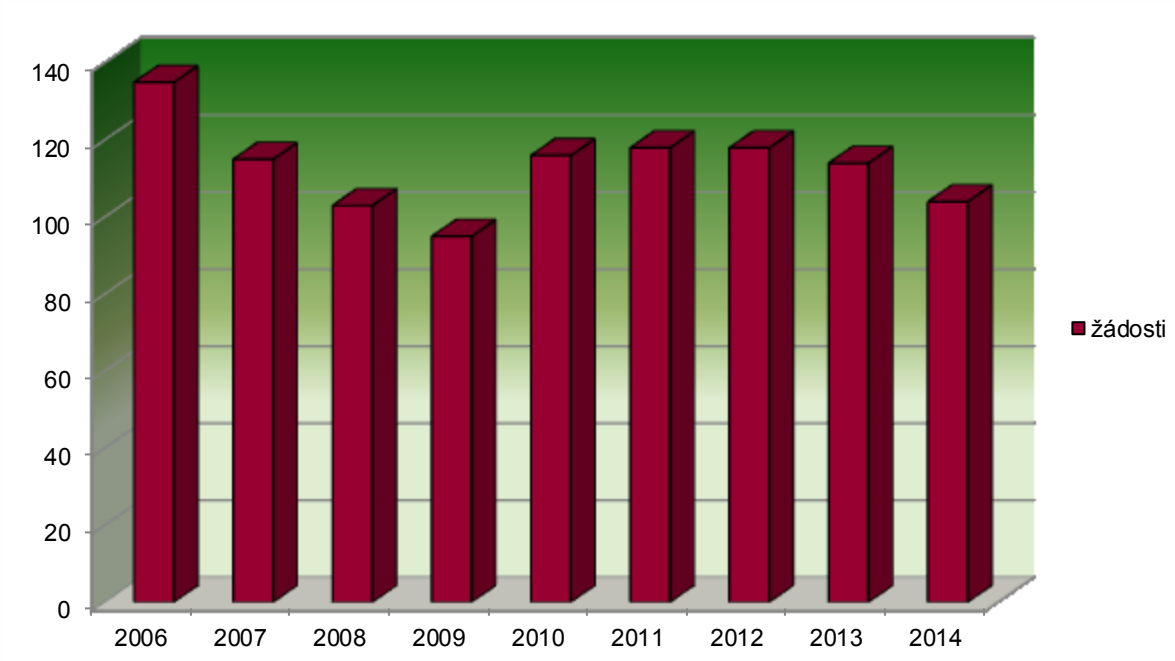
Bylo vydáno 106 certifikátů informačních systémů, z toho 44 pro žadatele ze státní správy nebo samosprávy a 62 ze soukromé sféry. Celkem 55 certifikátů bylo vydáno na žádost podanou v roce 2014. Z celkového počtu 106 certifikátů vydaných v roce 2014 se jednalo pouze v 19 případech o první certifikaci informačního systému, z toho 7 certifikátů bylo vydáno pro informační systémy státní správy.

V 15 případech provozovatel informačního systému s certifikátem platným do data spadajícího do roku 2014 nepožádal o opakovanou certifikaci a platnost certifikátu automaticky skončila.

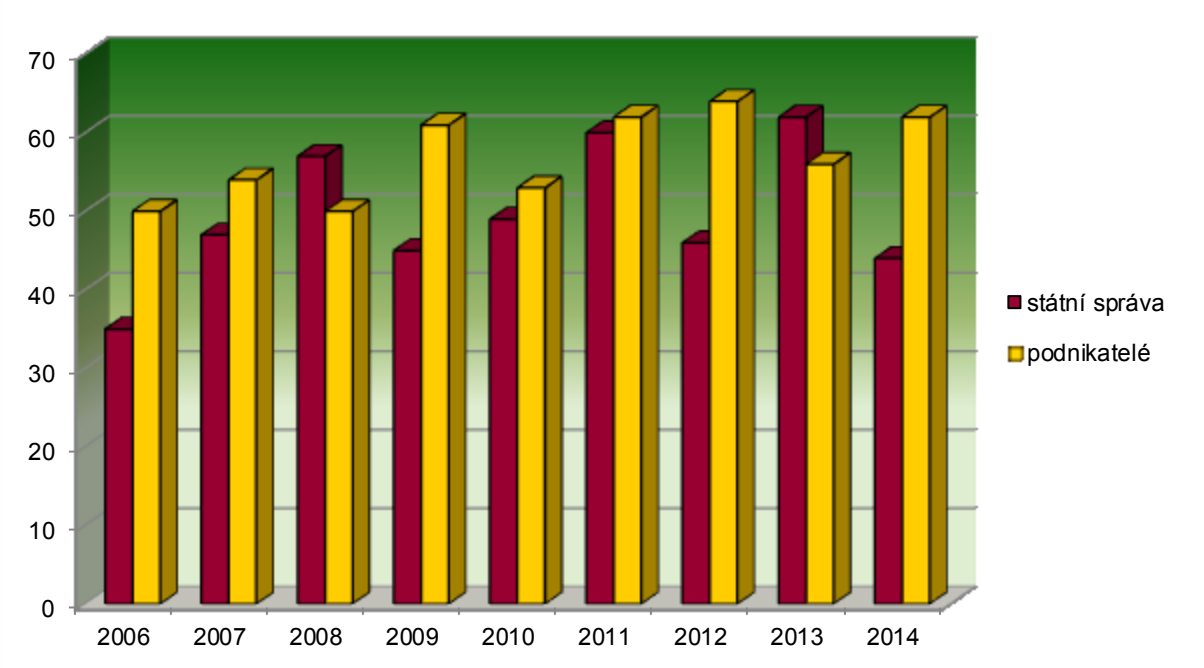
Certifikace informačních systémů v roce 2014

Přijaté žádosti	Vydané certifikáty podle stupně utajení				Vydané certifikáty	
	Vyhrazené	Důvěrné	Tajné	Přísně tajné	státní správa	podnikatelé
104	21 %	51 %	27 %	1 %	44	62

Přijaté žádosti o certifikaci informačního systému v letech 2006 až 2014



Vydané certifikáty informačních systémů v letech 2006 až 2014



Vydáním certifikátu informačního systému práce s tímto systémem nekončí, neboť zejména v rozsáhlých systémech je během doby platnosti certifikátu vyžadován určitý rozvoj a plánované změny musí být projednány, posouzeny a schváleny Úřadem. Před uplynutím doby platnosti certifikátu pak musí být certifikace pro další období opakována.

Lze konstatovat, že v roce 2014 přibyly pouze 3 žádosti o certifikaci nově budovaného informačního systému ze státní správy a 8 žádostí od podnikatelů. Trend, který je možno sledovat již od roku 2010, kdy informační systémy pro zpracování utajovaných informací jsou již většinou provozovány po více než jedno období platnosti certifikátu informačního systému, se nemění. V rámci opakovaných certifikací již provozovaných informačních systémů jsou však řešeny bezpečnostní problémy spjaté ze změnami použitých informačních technologií, rozšiřováním informačních systémů a s nasazováním prostředků kryptografické ochrany. Zejména ve státní správě technologická úroveň informačních systémů pro nakládání s utajovanými informacemi trvale roste, a to spolu s úrovní jejich zabezpečení. Výkyvy v počtu provedených certifikací souvisejí také s cykly, v nichž se provádí opakovaná certifikace (zpravidla 5 let pro nakládání s utajovanými informacemi stupně utajení Vyhrazené, 3 roky pro nakládání s utajovanými informacemi stupně utajení Důvěrné a 2 roky pro nakládání s utajovanými informacemi stupně utajení Tajné nebo Přísně tajné).

V roce 2014, kromě opakované certifikace menších informačních systémů v několika ministerstvech a úřadech (Ministerstvo průmyslu a obchodu, Ministerstvo financí, Ministerstvo spravedlnosti, Ministerstvo práce a sociálních věcí, Ministerstvo kultury, Česká národní banka, Ústavní soud, Úřad pro ochranu hospodářské soutěže, několik krajských a městských úřadů), proběhla opakovaná nebo nová certifikace významných a rozsáhlých informačních systémů v Ministerstvu vnitra a Policii ČR, Ministerstvu obrany, Ministerstvu zahraničních věcí, Bezpečnostní informační službě, Úřadu pro zahraniční styky a informace a Vojenském zpravodajství.

V rámci certifikace informačních systémů poskytovali zaměstnanci Úřadu žadatelům o certifikaci potřebné konzultace, nastavení bezpečnostních charakteristik operačních systémů a další informace potřebné pro zabezpečení určitého informačního systému. V řadě případů usměrňovali vývoj těchto systémů tak, aby byly certifikovatelné.

V roce 2014 Úřad provedl pro rezort Ministerstva obrany národní akreditaci lokalit důležitých součinnostních systémů NATO a pro Ministerstvo zahraničních věcí a Ministerstvo vnitra národní akreditaci lokalit součinnostních systémů EU. Zároveň byla příslušným orgánům NATO nebo EU pro bezpečnostní akreditaci vydána požadovaná prohlášení o shodě s bezpečnostními požadavky kladenými na tyto součinnostní systémy, na jejichž základě mohou být národní lokality jejich účastníkem. Stálou pozornost vyžaduje i hodnocení a schvalování změn prováděných v uvedených systémech a jejich rozšiřování.

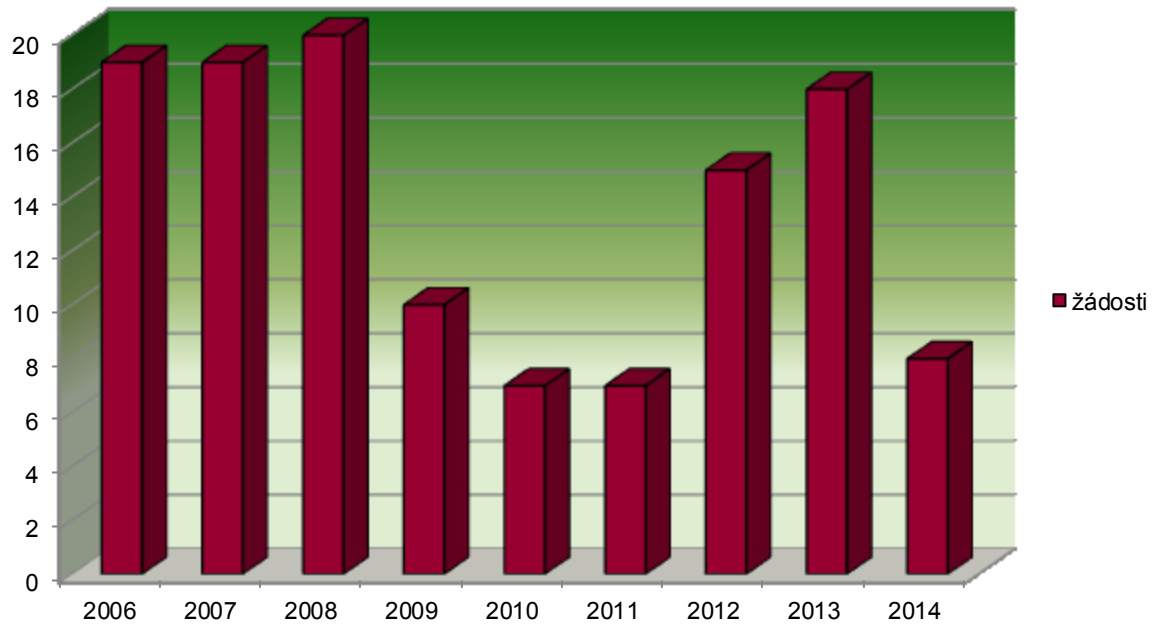
2.6.1.2. Certifikace kryptografických prostředků

V roce 2014 bylo Úřadu podáno celkem 8 žádostí o certifikaci kryptografického prostředku, z toho 6 na nový kryptografický prostředek. V řízeních k certifikaci kryptografického prostředku bylo vydáno celkem 16 certifikátů, žádné řízení nebylo ukončeno bez vydání certifikátu. Přitom významný podíl pracovní kapacity pracoviště certifikace kryptografických prostředků byl zaměřen na certifikaci kryptografických prostředků vyvíjených v ČR. Stav řízení je shrnut v následující tabulce.

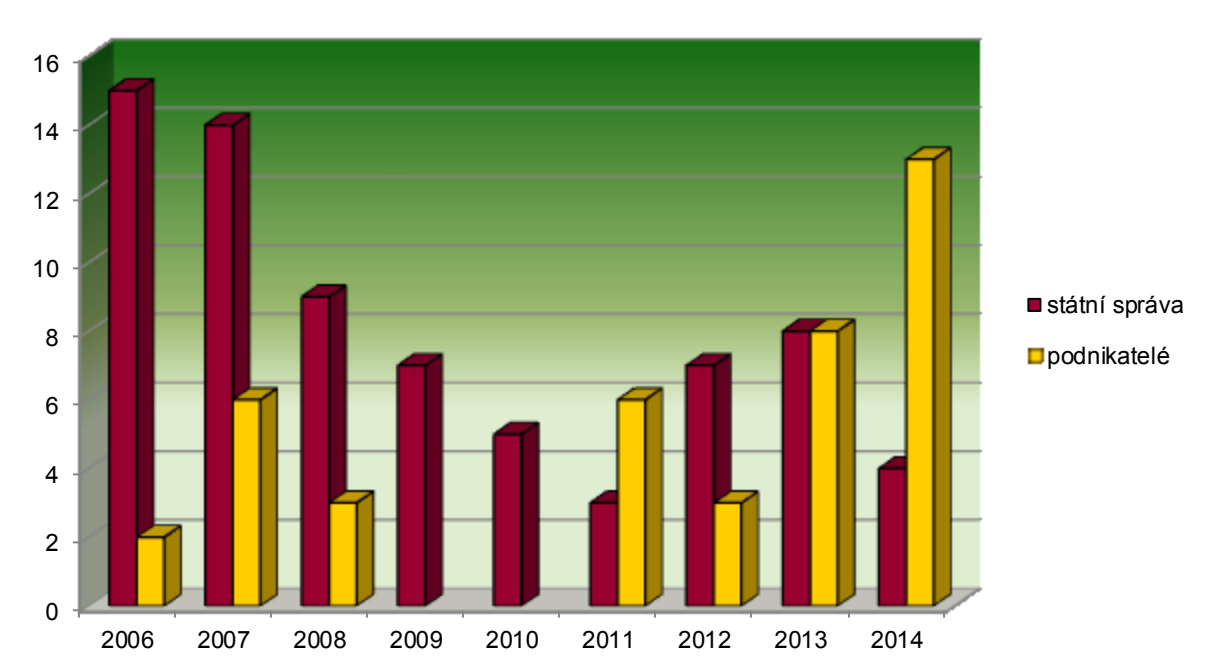
Certifikace kryptografických prostředků v roce 2014

Přijaté žádosti vč. opak.	Probíhající řízení		Ukonč. bez vydání certifikátu		Vydané certifikáty		Pro NATO a EU	
	státní správa	podnikatelé	státní správa	podnikatelé	státní správa	podnikatelé	NATO	EU
8	4	2	0	0	4	12	13	9

Přijaté žádosti o certifikaci kryptografického prostředku v letech 2006 až 2014



Vydané certifikáty kryptografických prostředků v letech 2006 až 2014



Úřad provedl opakovanou certifikaci kryptografických prostředků HCryptW, LANPCS-AES, SECTRA Panthon 3 a prostředků speciálního nebo součinnostního spojení. Nově byly certifikovány kryptografické prostředky PCS1e, Silentel v. 5.2, LANPCS-Rack a LANPCSe-AES a kryptografické prostředky třídy TCE 621 ve verzích duál (TCE 621 B/CZ Dual mode, TCE 621 C/CZ Dual mode, TCE 621/B Dual mode a TCE 621/C Dual mode) a ve verzích MINIP (TCE 621/M a TCE 621/M-AES). Nebyla prováděna opakovaná certifikace kryptografických prostředků třídy KTA a SECTEL ve všech verzích.

V návaznosti na nové poznatky k provozu byly upraveny, formou doplňku, certifikační zprávy kryptografických prostředků KRYDEC a HCryptW. Úřad vydal aktualizovaný bezpečnostní standard NBÚ-1/2013 upravující provoz a správu kryptografických prostředků třídy TCE 621 center řízení TCE 671 a standard NBÚ-1/2014 upravující podmínky, způsob a postupy vyřazování a ničení kryptografického prostředku a materiálu k zajištění jeho funkce.

Certifikované kryptografické prostředky jsou nebo budou využívány především v rezortech Ministerstva obrany, Ministerstva vnitra, Ministerstva zahraničních věcí a ve zpravodajských službách.

Spektrum kryptografických prostředků certifikovaných v ČR v zásadě pokrývá ochranu lokálního ukládání a přenosu utajovaných informací v informačních a komunikačních systémech, včetně ochrany utajované informace v hlasové formě. Početně významné zastoupení mají kryptografické prostředky pro ochranu utajovaných informací v prostředí IP sítí, naopak vyřazovány jsou linkové kryptografické prostředky. Pro potřebu řešení specifických požadavků informačních systémů jsou aktualizovány verze prostředků třídy HCrypt pro předběžné šifrování.

Pro hodnocení a certifikaci kryptografických prostředků jsou aplikovány standardy Úřadu, které vycházejí z národních zkušeností, mezinárodních standardů (CC a FIPS) i informací získaných na mezinárodních kryptografických konferencích.

Do seznamu Úřadu materiálu „kontrolovaná kryptografická položka“ byl zařazen kryptografický prostředek LANPCS-Rack, nově certifikované kryptografické prostředky tříd TCE 621 a komponenty kryptografických prostředků LANPCS a PCS1e.

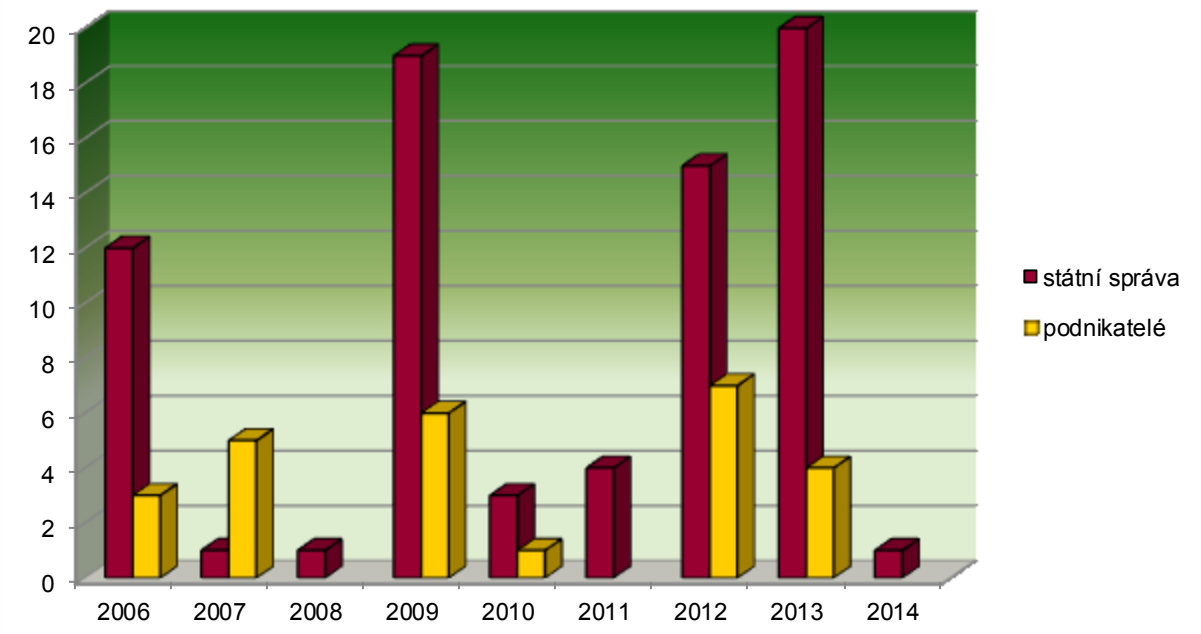
2.6.1.3. Certifikace kryptografických pracovišť

V roce 2014 byla podána jediná žádost o certifikaci kryptografického pracoviště a to z kategorie opakovaných žádostí. Z této skutečnosti vyplývá, že již dříve zřízená kryptografická pracoviště a provoz v nich je v souladu s reálnými potřebami příslušných organizací. V tomto rámci ovšem dochází k rozšiřování pracovišť o další kryptografické prostředky a ke změnám jejich umístění. Všechny změny musí být předem posouzeny a schváleny Úřadem. Stav řízení o certifikaci je shrnut v následující tabulce:

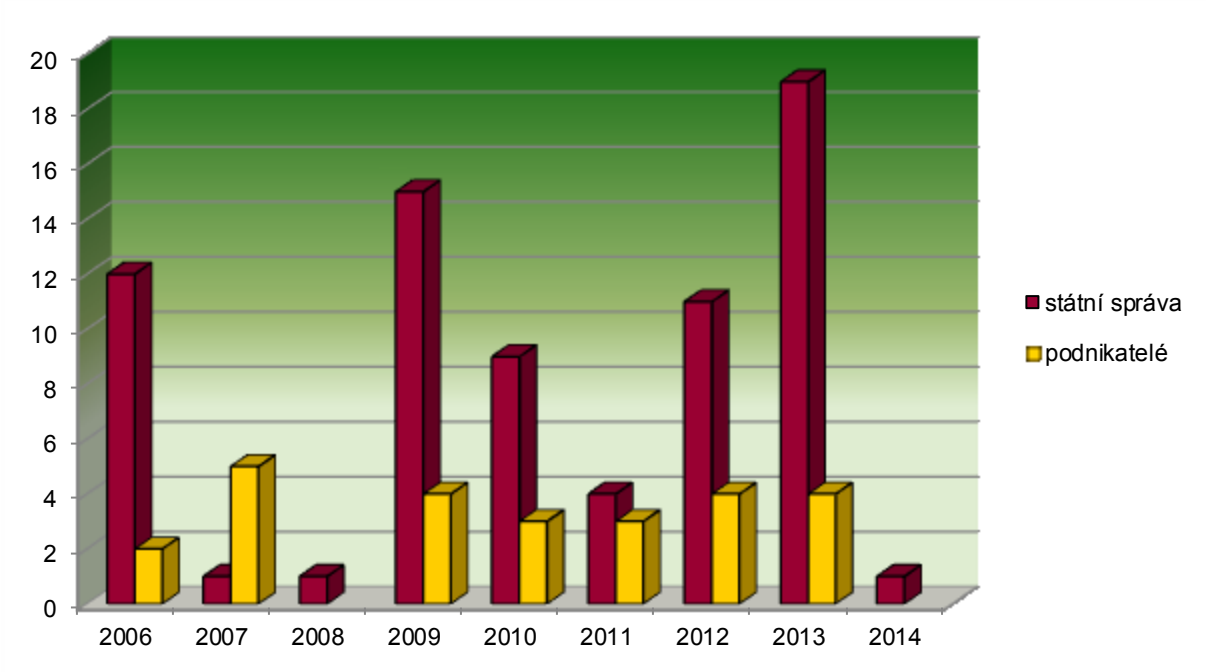
Certifikace kryptografických pracovišť v roce 2014

	Přijaté žádosti	Rozpracováno	Certifikováno	Zamítnuto
Státní správa	1	0	1	0
Podnikatelé	0	0	0	0
Celkem	**1**	**0**	**1**	**0**

Přijaté žádosti o certifikaci kryptografického pracoviště v letech 2006 až 2014



Vydané certifikáty kryptografických pracovišť v letech 2006 až 2014



2.6.1.4. Certifikace stínicích komor

Hlavní objem certifikačních měření a hodnocení útlumu stínicích komor byl prováděn pro organizační složky státu v ČR a pro Ministerstvo zahraničních věcí v zahraničí na zastupitelských úřadech. Díky tomu, že příslušné pracoviště Úřadu bylo vybaveno další technikou, bylo možné plnit požadavky Ministerstva zahraničních věcí v přiměřených lhůtách. Celkem bylo vydáno 26 certifikátů stínicích komor, přičemž bylo využíváno i podkladů z měření provedených pracovníky Ministerstva zahraničních věcí a společnosti Techniserv, s.r.o., na základě smlouvy o zajištění činnosti.

2.6.2. Další odborná činnost

2.6.2.1. Výroba kryptografického materiálu

Relevantní součástí oblasti kryptografické ochrany je výroba kryptografického materiálu (programování procesorových a paměťových modulů, generování kryptografických klíčů a hesel ke kryptografickým prostředkům) určeného pro Úřad a orgány státu k zajištění ochrany utajovaných informací v komunikačních a informačních systémech.

V této oblasti Úřad spolupracoval s odborem bezpečnosti Ministerstva obrany, který zabezpečuje generování, speciální balení a distribuci kryptografických klíčových materiálů pro kryptografické prostředky provozované v rámci rezortu Ministerstva obrany a výrobu některých kryptografických klíčových materiálů ve prospěch Úřadu.

V roce 2014 bylo v Úřadu vygenerováno celkem 84 309 kryptografických klíčů a hesel uložených na 4 910 nosičích různých typů a dalších 354 kusů jiného kryptografického materiálu (procesory, paměti, kryptografická dokumentace, instalační a šifrovací SW).

Úřad vzal do evidence a provedl distribuci celkem 2 273 ks nového kryptografického a CCI materiálu a dále zajistil servis a opravy na území ČR u 21 ks kryptografických prostředků a mimo ČR u 28 ks kryptografických prostředků.

V průběhu roku 2014 byla rozšířena výroba heslového materiálu pro kryptografické prostředky třídy HCrypt a zahájena nová výroba klíčového materiálu pro kryptografický prostředek LANPCS-AES.

Na kryptografickém pracovišti Úřadu probíhalo průběžné ničení utajovaných dokumentů vyřazených v rámci skartačního řízení.

Dále Úřad zajišťoval speciální balení a distribuci kryptografického materiálu, vedení ústřední evidence certifikovaných kryptografických prostředků dislokovaných u orgánů státu, jakož i centrální databáze všech pracovníků kryptografické ochrany v působnosti Úřadu.

2.6.2.2. Měření kompromitujícího vyzařování (TEMPEST)

2.6.2.2.1. TEMPEST měření elektronických zařízení

Úřad prováděl v roce 2014 TEMPEST měření podle standardů NATO řady SDIP, EU řady IASG 7 a podle metodiky MIL-STD 461. Objektem měření byla především zařízení orgánů státu. Jednalo se jak o měření komerčních zařízení, většinou pro účely výběrových řízení, tak speciálních informačních systémů.

Celkem bylo v roce 2014 hodnoceno více než 60 typů zařízení. Z toho bylo prováděno TEMPEST měření více než 10 ks zařízení EUROTEMPEST a Siltec, a to jako samostatného zařízení nebo v kombinaci s kryptografickým prostředkem KRYDEC. Dále bylo provedeno měření inovovaných systémů s kryptografickým prostředkem TCE 621 a KTA. Tato měření byla prováděna podle metodiky standardu SDIP-27/1. Většina zařízení splňovala požadavky tohoto standardu.

Další TEMPEST měření byla prováděna v rámci certifikace nebo akreditace informačních systémů pro zpracování utajovaných informací stupně utajení Důvěrné nebo Tajné, buď pro orgány státu (Úřad vlády, Ministerstvo zahraničních věcí, Ministerstvo obrany, Ministerstvo vnitra, Ministerstvo průmyslu a obchodu, zpravodajské služby, krajské úřady aj.), nebo pro podnikatele. Z celkového počtu hodnocených zařízení byla naprostá většina vyžádána Ministerstvem obrany.

2.6.2.2.2. Zónové měření, instalační záznamy, obranné prohlídky

Úřad dále prováděl ohodnocování prostorů metodou zónového měření. Jednalo se o prostory, ve kterých se nacházela zařízení zpracovávající utajované informace. Tento druh měření byl především použit u objektů Úřadu, Bezpečnostní informační služby, Ministerstva obrany, Ministerstva vnitra aj. Další zónová měření byla prováděna pro státní správu i pro soukromé subjekty v rámci certifikace informačních systémů.

Bylo provedeno hodnocení instalace informačních systémů zpracovávajících utajované informace stupně utajení Tajné a v rámci certifikace těchto systémů byly zpracovány instalační záznamy.

V roce 2014 byly provedeny obranné prohlídky v několika objektech na základě žádostí orgánů státní správy nebo v rámci certifikace informačních systémů.

2.6.2.2.3. Přehled provedených měření

Přehled měření v oblasti kompromitujícího vyzařování, provedených v roce 2014, je uveden v následující tabulce.

Měřená zařízení a objekty v roce 2014

Typ měření[10)]	**Počet**
Zónové měření	10 objektů
Kryptografické prostředky	1 typ
PC sestavy	8 sestav – třída 0; přes 60 typů – třída 1 a 2
Audiotechnika	2 typy zařízení
Obrané prohlídky i v rámci certifikace IS	17 objektů
Mobilní systémy	2 systémy

2.6.2.3. Schvalování projektů bezpečnosti komunikačních systémů

Komunikační systém pro výměnu utajovaných informací může být podle zákona provozován pouze na základě Úřadem schváleného projektu bezpečnosti. Platnost schválení je dána také platností certifikátu použitých kryptografických prostředků.

V roce 2014 byl dále provozován rezortní komunikační systém v Bezpečnostní informační službě a mezirezortní komunikační systém MODUS. Správu komunikačního systému MODUS využívajícího certifikovaných kryptografických prostředků SECTRA Tiger XS (přídavný kryptografický modul k mobilnímu telefonu), umožňujících mobilní telefonii pro utajované informace do stupně utajení Tajné, v roce 2014 nadále zajišťoval Úřad. Úřad provozuje středisko pro řízení komunikační sítě určené pro vrcholové představitele státu a rovněž pro řízení rezortních sítí konfigurovaných podle vlastního návrhu daného rezortu.

V roce 2014 byl v Úřadu zřízen nový komunikační systém Panthon pro mobilní komunikaci informací do stupně utajení Vyhrazené, využívající nově certifikovaného kryptografického mobilního prostředku Panthon 3. Byla zpracována příslušná bezpečnostní dokumentace a schválen projekt bezpečnosti uvedeného

[10)] U zónového měření a obranných prohlídek se jedná o objekty; v rámci jednoho objektu bylo měřeno více místností nebo budov. U kryptografických prostředků se jednalo i o ověřovací měření. U PC sestav třídy 1 a 2 se jednalo i o měření v rámci výběrových řízení např. pro Ministerstvo obrany.

komunikačního systému. Systém byl po zkušebním provozu schválen do rutinního provozu ode dne 1. června 2014 a je provozován z centra umístěného v Úřadu.

Lze uvést, že hlasovou komunikaci utajovaných informací na mezirezortní úrovni poskytují rovněž dva informační systémy tzv. vládního utajeného spojení, provozované Ministerstvem vnitra, kterými jsou informační systém Vega-T (pro nakládání s utajovanými informacemi do stupně utajení Tajné) a informační systémem Vega-D (pro nakládání s utajovanými informacemi do stupně utajení Důvěrné). Oba informační systémy jsou certifikovány Úřadem podle zákona a jejich rozvoj a rozšiřování je pod dohledem Úřadu. V roce 2014 pokračovalo připojování dalších lokalit informačního systému Vega-D. Kontrol lokalit před jejich připojením se účastní i pracovníci Úřadu.

2.6.2.4. Školení pracovníků kryptografické ochrany a zkoušky odborné způsobilosti

Úřad v roce 2014 organizačně zajistil a provedl, v souladu se zákonem, celkem 19 školení skupin pracovníků kryptografické ochrany a po následující zkoušce odborné způsobilosti vydal 126 osvědčení o zvláštní odborné způsobilosti pracovníka kryptografické ochrany. Dále provedl zaškolení celkem 7 pracovníků provozní obsluhy kryptografického prostředku a vydal 49 potvrzení o odborném zaškolení pracovníka provozní obsluhy kryptografického prostředku. Kromě toho probíhají další školení a zkoušky odborné způsobilosti na Ministerstvu vnitra, Ministerstvu obrany a Ministerstvu zahraničních věcí na základě smluv uzavřených mezi Úřadem a uvedenými ministerstvy. Úřad v roce 2014 schvaloval aktualizaci osnov a obsahu některých kurzů.

K provádění části zkoušky zvláštní odborné způsobilosti pracovníka kryptografické ochrany a vydávání potvrzení o jejím absolvování připravil Úřad aktualizaci smluv o zajištění činnosti se společnostmi S.ICZ a. s., a ATS-TELCOM PRAHA a. s., přičemž se jedná o technickou část speciální obsluhy kryptografického prostředku. Obsah přípravy, způsob provádění a organizování této části odborné zkoušky bude schvalovat Úřad.

2.6.3. Problémové oblasti bezpečnosti informačních a komunikačních systémů a kryptografické ochrany

Zabezpečování zákonem stanovených činností Úřadu v oblasti kryptografické ochrany a bezpečnosti informačních systémů nakládajících s utajovanými informacemi probíhalo v roce 2014 bez větších problémů.

- Podařilo se dosáhnout kvalitního obsazení pracovních míst pro tyto činnosti v Úřadu aktuálně přidělených, avšak vzhledem k malému počtu pracovníků, kteří řeší jednotlivé oblasti bezpečnosti, má výpadek každého pracovníka (mateřská dovolená, dlouhodobé onemocnění) poznatelný vliv na již tak vysoké pracovní vytížení odborných pracovníků. V případě odchodu odborníka z těchto oblastí je nesnadná jeho náhrada, neboť se jedná o specializované činnosti a je vyžadována bezpečnostní prověrka na stupeň utajení Tajné nebo Přísně tajné.

- Postupně jsou v Úřadu vytvářeny další potřebné bezpečnostní standardy, zejména v oblasti kryptografické ochrany, přičemž se Úřad v určitých oblastech snaží dosáhnout řešení, na kterém by se shodly rezorty, které nejvíce kryptografickou ochranu využívají.

- Z hlediska zajištění praktické ochrany utajovaných informací v informačních nebo komunikačních systémech a zajištění kryptografické ochrany všeobecně ve státní správě byl i v roce 2014 problémem nedostatek odborníků v oboru informačních technologií a kryptografické ochrany, kteří by zároveň splňovali podmínky pro přístup fyzické osoby k utajované informaci stupně utajení Důvěrné, Tajné nebo Přísně tajné. Stabilizované obsazení pracovních míst je potřebné zejména v případě pracovníků ve výkonu kryptografické ochrany. Rovněž je třeba usilovat o zajištění zastupitelnosti v klíčových rolích v bezpečnostní správě a správě informačních systémů.

2.7. ADMINISTRATIVNÍ A FYZICKÁ BEZPEČNOST, ÚSTŘEDNÍ REGISTR

V oblasti administrativní bezpečnosti, fyzické bezpečnosti a ústředního registru Úřad prováděl stanovené činnosti, které jsou vyspecifikovány níže, a dále se zapojil do čerpání evropských fondů v oblasti modernizace veřejné správy – Projekt Napojení agendového informačního programu CEFEUS na ISZR (CZ.106/1.1.00/ 14.08497).

2.7.1. Administrativní bezpečnost

V roce 2014 zpracovalo a zobecnilo pracoviště koncepce administrativní bezpečnosti poznatky získané při kontrolách administrativní bezpečnosti u orgánů státu, právnických či samostatně podnikajících fyzických osob v předchozích letech. Tyto podklady byly zapracovány do jednotlivých ustanovení připravované novely vyhlášky č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací, ve znění pozdějších předpisů. Další činnost pracoviště spočívá v dopracování vlastní novely uvedené vyhlášky a ve zpracování podkladů řešících manipulaci a archivaci utajovaných dokumentů v elektronické formě.

2.7.2. Fyzická bezpečnost

V oblasti fyzické bezpečnosti Úřad vedle své hlavní činnosti (certifikace technických prostředků, posuzování způsobu realizace zajištění ochrany utajovaných informací fyzickou bezpečností uvedeného v bezpečnostní dokumentaci podnikatele, ověřování schopnosti podnikatele zabezpečit ochranu utajovaných informací z hlediska fyzické bezpečnosti a výkon státního dozoru) dále prováděl:

- činnosti spojené s členstvím v certifikační radě společnosti TrezorTest s.r.o. (účast na výrobních auditech u 5 firem v rámci ČR, účast na certifikačních radách a účast při provádění zkoušek na mechanických zábranných systémech podle příslušných norem),

- činnosti související se stálou účastí v technické normalizační komisi TNK124 (posuzování a připomínkování překladů evropských technických norem) zřízené u Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví pro poplachové zabezpečovací systémy při zavádění nových evropských technických norem a aktualizaci stávajících technických norem pro tuto oblast,

- metodickou pomoc v souvislosti s instalací technických prostředků a s návrhy opatření fyzické bezpečnosti na vyžádání u podnikatelů nebo orgánů státu (např. Subterra a.s., Retia, a.s., AERO Vodochody AEROSPACE a.s., O2 Czech Republic a.s., Ústřední vojenský archiv, Vězeňská služba ČR, Generální finanční ředitelství, Ministerstvo financí, Masarykova univerzita aj.),

- školení v oblasti fyzické bezpečnosti složek Celní správy ČR a pracovníků ATOMAL registrů.

2.7.2.1. Certifikace technických prostředků

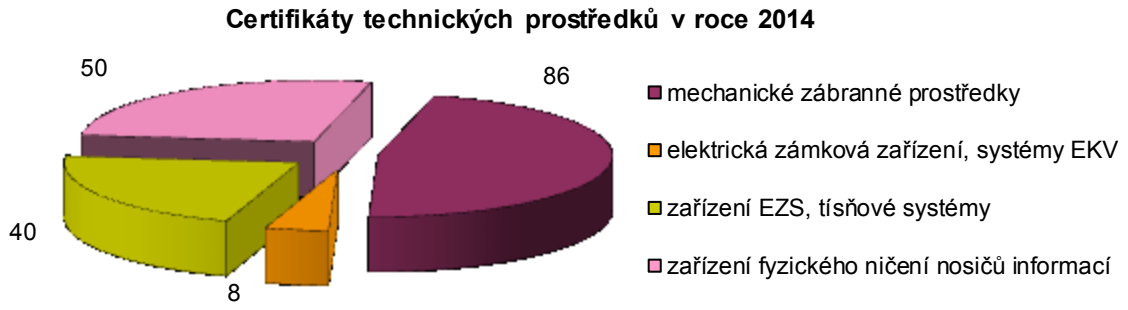
Nezbytnou zákonnou podmínkou pro používání technických prostředků k ochraně utajovaných informací je mj. i jejich certifikace. Úřad v roce 2014 přijal celkem 100 žádostí o certifikaci pro 191 technických prostředků. V rámci posuzovaní a vyhodnocování podkladů pro certifikaci bylo u 9 % žádostí vyžádáno jejich doplnění a upřesnění. Ve 2 případech byl certifikační proces ukončen bez vydání certifikátu, neboť se jednalo o technické prostředky, které se necertifikují.

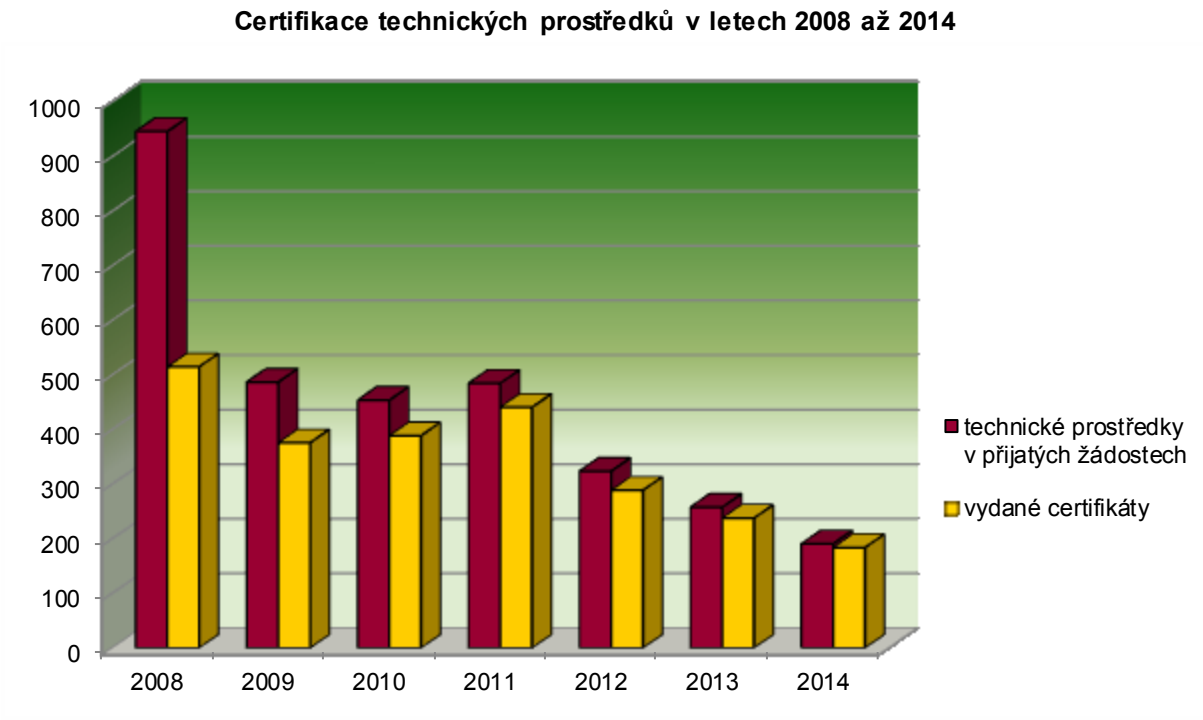
Úřad vydal celkem 184 certifikátů technických prostředků. Rozdíl mezi počtem podaných žádostí a počtem vydaných certifikátů je způsoben slučováním více technických prostředků obdobných vlastností na jeden certifikát. Počty vydaných certifikátů technických prostředků podle jednotlivých skupin definovaných zákonem jsou uvedeny v následující tabulce.

Vydané certifikáty technických prostředků v roce 2014

Mechanické zábranné prostředky[11)]	86
Elektrická zámková zařízení, systémy pro kontrolu vstupu[12)]	8
Zařízení elektrické zabezpečovací signalizace a tísňové systémy[13)]	40
Zařízení fyzického ničení nosičů informací[14)]	50
Celkem	**184**

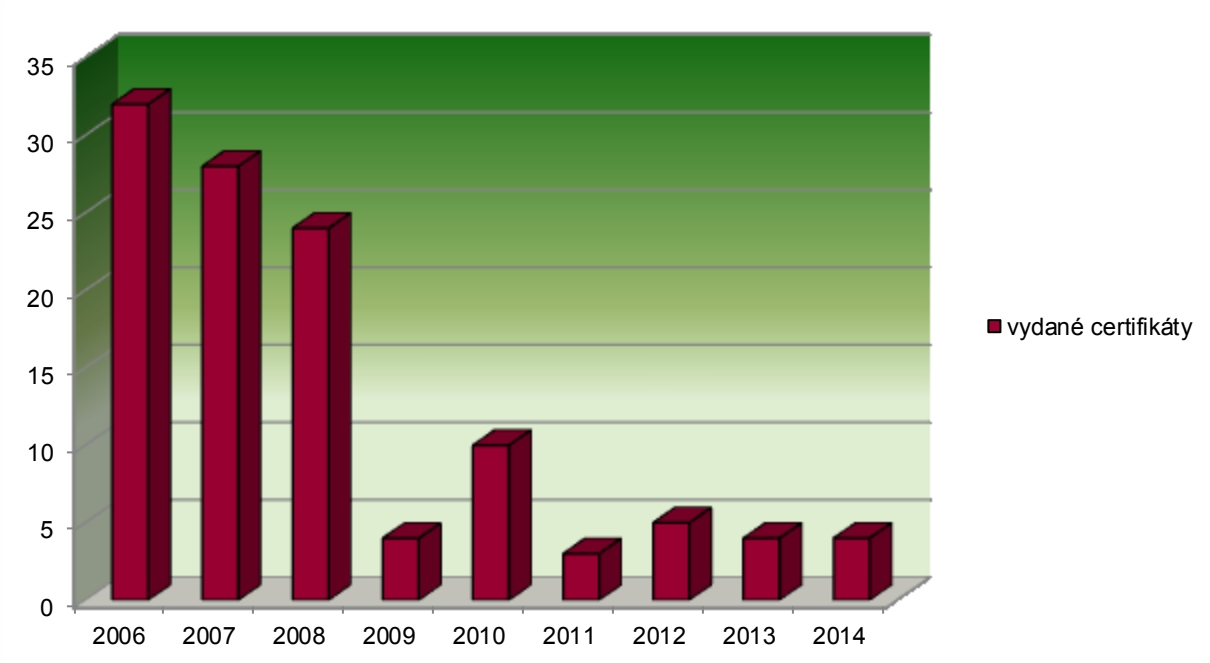
[11)] § 30 odst. 1 písm. a) zákona.
[12)] § 30 odst. 1 písm. b) zákona.
[13)] § 30 odst. 1 písm. c) a e) zákona.
[14)] § 30 odst. 1 písm. h) zákona.





Kromě certifikátů uvedených v předchozí tabulce a grafech byly v roce 2014, na základě podaných žádostí, vydány 4 certifikáty pro jednotlivé technické prostředky – uživatelské certifikáty. Tyto žádosti podávají uživatelé, kteří si zajistí vlastní posudek na konkrétní technický prostředek nasazený pro ochranu utajovaných informací. Vývoj počtu vydaných uživatelských certifikátů technických prostředků v období účinnosti zákona zobrazuje následující graf.

Uživatelské certifikáty technických prostředků v letech 2006 až 2014



V souvislosti s certifikací technických prostředků je průběžně aktualizován zveřejněný certifikační postup Úřadu, který stanovuje rozsah akreditovaných zkoušek pro jednotlivé druhy technických prostředků a slouží jako podklad pro certifikaci. Aktualizace se týká novel technických norem. Průběžně probíhá aktualizace certifikovaných technických prostředků na internetových stránkách Úřadu.

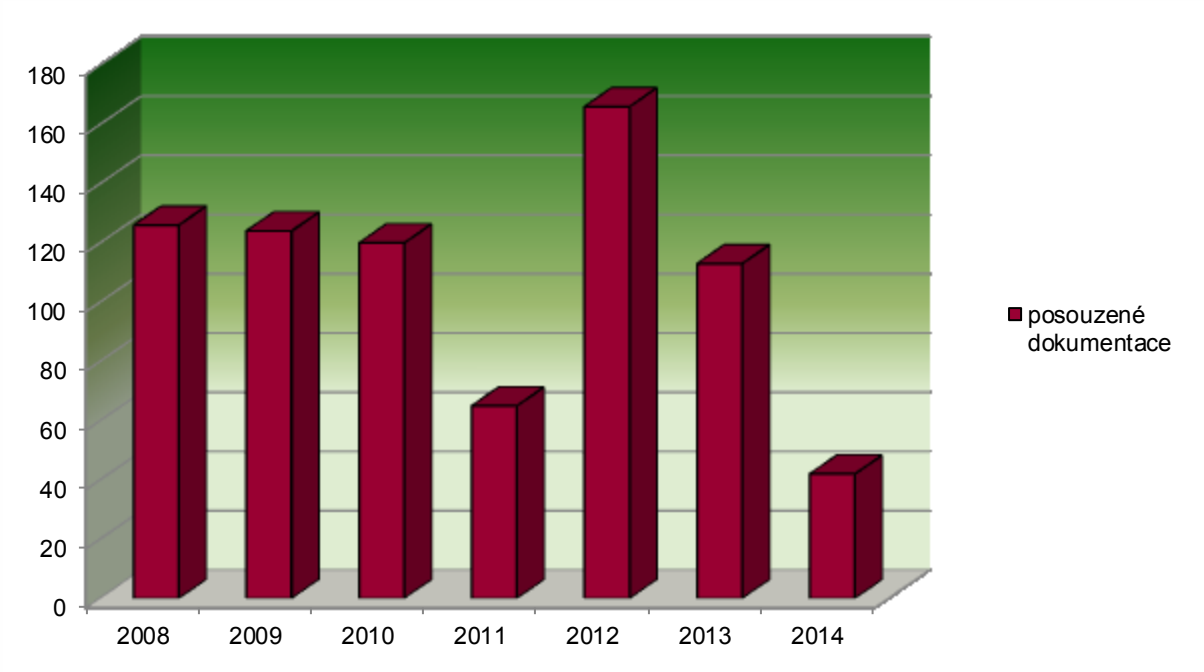
2.7.2.2. Posuzování bezpečnostní dokumentace podnikatele z hlediska fyzické bezpečnosti

V rámci vedených bezpečnostních řízení o vydání osvědčení podnikatele nebo při aktualizaci bezpečnostní dokumentace podnikatele, který je držitelem osvědčení podnikatele, bylo v roce 2014 přijato celkem 46 žádostí o stanovisko k bezpečnostní dokumentaci podnikatele z hlediska zajištění ochrany utajovaných informací fyzickou bezpečností. Při posuzování dokumentací byla v 35 % případů provedena konzultace s podnikatelem v Úřadu nebo přímo v sídle podnikatele. Bylo posouzeno 42 bezpečnostních dokumentací podnikatele a bylo provedeno 37 tzv. dohlídek, při kterých byla v sídle podnikatele ověřena jeho schopnost zabezpečit ochranu utajovaných informací z hlediska fyzické bezpečnosti. K 1. lednu 2015 zbývalo posoudit 4 bezpečnostní dokumentace podnikatele. Přehled přijatých žádostí, členěný podle kategorií zabezpečených oblastí, je uveden v následující tabulce.

Přijaté žádosti a posouzené bezpečnostní dokumentace podnikatele v roce 2014

Kontroly	Důvěrné	Tajné	Přísně tajné	Celkem
Přijaté žádosti	29	17	0	**46**
Posouzené dokumentace	26	16	0	**42**

Posouzené bezpečnostní dokumentace podnikatele v letech 2008 až 2014



2.7.2.3. Problémové oblasti fyzické bezpečnosti

Certifikace technických prostředků:

- neúplné podkladové materiály k žádosti o certifikaci technického prostředku.

Ověřování schopnosti podnikatele zabezpečit ochranu utajovaných informací z hlediska fyzické bezpečnosti:

- nedostatky ve zpracování projektů fyzické bezpečnosti (nezřetelný popis rozmístění technických prostředků),
- nekompletní popis režimových opatření fyzické bezpečnosti (označování a evidence klíčů, neaktualizované seznamy oprávněných osob),
- nedostatky při instalaci technických prostředků (nefunkčnost poplachového systému při přenosu na stanoviště ostrahy).

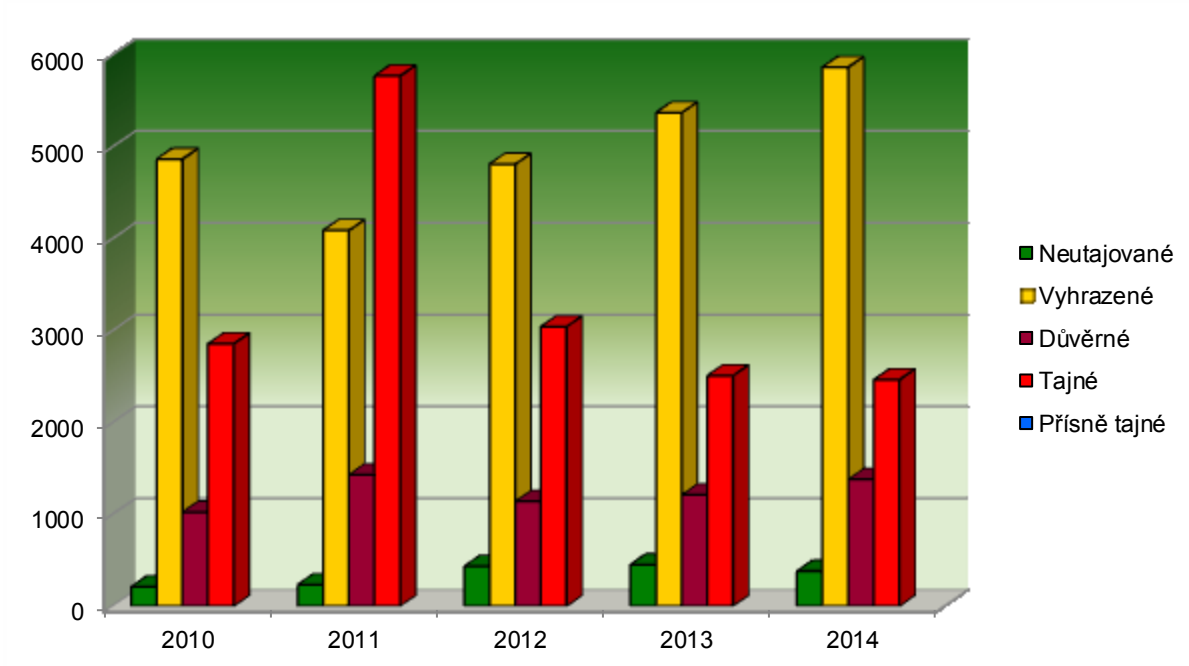
2.7.3. Ústřední registr

Prostřednictvím ústředního registru je realizováno poskytování utajovaných informací v rámci mezinárodního styku. V roce 2014 vykonával ústřední registr evidenci, distribuci a ukládání těchto utajovaných informací, a to zejména utajovaných informací NATO. U určených utajovaných dokumentů ústřední registr prováděl jejich distribuci podřízeným registrům utajovaných informací, zřízeným v rámci ústředních orgánů státní správy a právnických osob. Přehled dokumentů a utajovaných dokumentů NATO evidovaných v ústředním registru za posledních 5 let je uveden v následující tabulce a grafu.

Dokumenty NATO evidované v ústředním registru

NATO	2010	2011	2012	2013	2014	Celkem
Neutajované	212	235	434	454	384	**1 719**
Vyhrazené	4 869	4 092	4 814	5 374	5 869	**25 018**
Důvěrné	1 026	1 433	1 143	1 213	1 383	**6 198**
Tajné	2 858	5 774	3 044	2 511	2 466	**16 653**
Přísně tajné	0	0	0	0	0	**0**
Celkem	**8 965**	**11 534**	**9 435**	**9 552**	**10 102**	**49 588**

Dokumenty NATO evidované v ústředním registru



Kromě utajovaných dokumentů NATO jsou v ústředním registru evidovány utajované dokumenty EU a utajované dokumenty ostatních subjektů cizí moci. Evidovány jsou i doručené neutajované dokumenty cizí moci poskytnuté v rámci mezinárodního styku.

V ústředním registru jsou také evidovány a následně distribuovány zahraničním partnerům utajované informace poskytované orgány státu a ostatními subjekty ČR.

V rámci kontrolní činnosti ústředního registru, podle § 79 odst. 7 zákona, bylo v loňském roce provedeno 11 kontrol podřízených registrů utajovaných informací a 3 kontroly podřízených ATOMAL registrů. Zároveň se pracovníci ústředního registru účastnili 12 kontrol v rámci výkonu státního dozoru u orgánů státu a podnikatelů, které mají zřízeny registry utajovaných informací. Zjištěné nedostatky se týkaly zejména autentizace a vedení administrativních pomůcek, způsobu předávání

utajovaných dokumentů a vedení přehledu osob, které se s utajovanými dokumenty seznámily.

V rámci metodického řízení bylo v roce 2014 provedeno školení vedoucích a jejich zástupců podřízených ATOMAL registrů, které bylo zaměřeno na bezpečnost utajovaných informací ATOMAL a prezentaci zkušeností získaných při cvičení ATOMAL. Rovněž bylo provedeno školení z oblasti ochrany utajovaných informací cizí moci a administrativní bezpečnosti pro justiční organizace rezortu Ministerstva spravedlnosti.

Ústřední registr rovněž ověřoval splnění podmínek nezbytných pro zřízení registru utajovaných informací u 1 subjektu, který podal žádost o souhlas ke zřízení registru utajovaných informací cizí moci. V seznamu všech registrů zřízených na území ČR, vedeném v ústředním registru, bylo ke konci roku 2014 evidováno celkem 47 registrů utajovaných informací (bez pomocných registrů).

V rámci skartačního řízení byly zničeny utajované dokumenty cizí moci, u kterých uplynula skartační lhůta, a to jak v listinné, tak i v digitální podobě.

Jako každý rok byly provedeny inventury utajovaných dokumentů v ústředním registru i v podřízených registrech v ČR a na jejich základě byla zaslána zpráva o provedené kontrole Bezpečnostnímu úřadu NATO. V rámci inventur nebylo zjištěno, že by jakýkoliv utajovaný dokument NATO, EU nebo ostatních subjektů cizí moci nebyl zaevidován, nebyl fyzicky dohledán nebo byl shledán nekompletním.

Průběžně byly aktualizovány přístupové seznamy osob, které se mohou seznamovat s utajovanými dokumenty NATO, EU a ostatních subjektů cizí moci v rámci Úřadu a byl veden přehled aktualizovaných evidenčních listů podřízených registrů.

I nadále byly dodržovány zásady při manipulaci a ochraně utajovaných informací ATOMAL v ČR podle předpisů NATO. Každé 3 měsíce byla prováděna kontrola utajovaných dokumentů ATOMAL uložených v ústředním registru řídícím správcem (ACO) nebo jeho zástupcem (DACO). O těchto kontrolách jsou vedeny záznamy, které jsou ukládány pro inspekci NATO.

2.8. KYBERNETICKÁ BEZPEČNOST

V ČR v roce 2014 pokračovalo započaté budování kybernetické bezpečnosti. Výsledkem bylo zejména otevření NCKB a přijetí zákona o kybernetické bezpečnosti a jeho prováděcích právních předpisů.

2.8.1. Budování NCKB/GovCERT.CZ

Počátek činnosti NCKB lze datovat ke konci roku 2011, kdy byl Úřad usnesením vlády ČR č. 781 ze dne 19. října 2011 pověřen jeho vybudováním. Od té doby byla provedena celá řada úkonů směřujících k vytvoření jeho operační kapacity.

To zahrnovalo značné množství aktivit, od úkonů administrativního charakteru, přes převzetí gesce za oblast kybernetické bezpečnosti od Ministerstva vnitra včetně převzetí či navazování nových vztahů s partnerskými úřady v zahraničí, vybudování prostor a zajištění technického zázemí nutného pro fungování NCKB, až po provádění výběrových řízení a náboru nových zaměstnanců.

Organizačně je NCKB součástí sekce kybernetické bezpečnosti Úřadu a dělí se na dvě oddělení – GovCERT.CZ[15)] a oddělení teoretické podpory, vzdělávání a výzkumu. GovCERT.CZ je tým zejména IT specialistů zabývající se technickou stránkou kybernetické bezpečnosti zahrnující řešení kybernetických bezpečnostních incidentů subjektů spravujících důležité komunikační a informační systémy pro stát, analýzu malware, sběr a vyhodnocování informací o kybernetických útocích a hrozbách apod. Oddělení je odpovědné za přípravu národních strategií, kybernetických bezpečnostních politik, koordinaci s ostatními gestory bezpečnosti ČR, zajištění plnění mezinárodních závazků a spolupráce v oblasti kybernetické bezpečnosti. Zároveň je odpovědné za určování kritické informační infrastruktury státu (dále jen „KII“) a komunikaci mezi Úřadem a subjekty KII a správci významných informačních systémů (dále jen „VIS“). Oddělení také poskytuje nezbytnou právní a administrativní podporu GovCERT.CZ, zabývá se tvorbou vzdělávacích politik a vzděláváním v oblasti kybernetické bezpečnosti a do budoucna i koordinací výzkumu v oblasti kybernetické bezpečnosti na národní úrovni.

Slavnostní otevření rekonstruované budovy NCKB proběhlo dne 13. května 2014 za účasti předsedy vlády ČR Bohuslava Sobotky, ředitele Úřadu Dušana Navrátila, náměstka generálního tajemníka NATO pro nové bezpečnostní výzvy Sorina Ducaru, ředitele Evropské agentury pro bezpečnost sítí a informací (ENISA) Udo Helmbrechta, představitelů české bezpečnostní komunity a dalších významných hostů nejen z oblasti kybernetické bezpečnosti.

2.8.2. Vývoj legislativy v oblasti kybernetické bezpečnosti

V roce 2014 došlo k několika podstatným událostem na poli legislativy v oblasti kybernetické bezpečnosti. Nejzásadnější bylo přijetí zákona o kybernetické bezpečnosti (viz kap. 2.1.1.). Vytvoření tohoto zákona bylo Úřadu uloženo usnesením vlády ČR č. 781/2011. Absence podobných předpisů v právním řádu ČR nebo u zahraničních partnerů vedla k vytvoření v současné době ojedinělé koncepce zaměřující se na nastavení systému koordinace a kooperace mezi nejdůležitějšími subjekty působícími v oblasti kybernetické bezpečnosti a na zavedení bezpečnostních opatření k ochraně informačních a komunikačních systémů důležitých pro stát.

Vedle zákona o kybernetické bezpečnosti byly v roce 2014 vypracovány a schváleny také jeho prováděcí právní předpisy, tj. vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti, vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, která byla vypracována společně Úřadem

[15)] GovCERT.CZ představuje vládní koordinační místo pro okamžitou reakci na kybernetické bezpečnostní incidenty (vládní CERT – Computer Emergency Response Team), které je organizační složkou Úřadu, respektive jeho specializovaného pracoviště, NCKB.

a Ministerstvem vnitra, a novela nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.

Návrh vyhlášky o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti byl podroben dvoukolovému připomínkovému řízení s cílem dosáhnout co možná nejširší diskuse o navržené právní úpravě a její optimalizace v dopadech na veřejnoprávní a soukromoprávní subjekty v ČR. 21. února 2014 byl návrh vyhlášky zveřejněn k připomínkování odbornou veřejností. Připomínky byly následně jednotlivě vypořádány na veřejném jednání. Po zapracování vypořádaných připomínek a po proběhnutí standardního mezirezortního připomínkového řízení byl návrh vyhlášky zaslán do Legislativní rady vlády, kde byl projednán v pracovní komisi Legislativní rady vlády pro správní právo.

Návrh vyhlášky o významných informačních systémech a jejich určujících kritériích, byl vypracován v první polovině roku 2014 a v září 2014 byl rozeslán do mezirezortního připomínkového řízení. Připomínky k návrhu podalo celkem 26 připomínkových míst. Řešeny byly zejména připomínky k uvedení některých systémů do přílohy č. 1 vyhlášky, ve které jsou stanoveny VIS, popřípadě se zaměřovaly na rozsah stanovení určujících kritérií a jiné legislativně-technické aspekty vyhlášky. Po vypořádání připomínek byla vyhláška postoupena k projednání pracovní komisi Legislativní rady vlády pro správní právo.

Obě vyhlášky byly schváleny dne 15. prosince 2014 a nabyly účinnosti dnem 1. ledna 2015.

Úřad se podílel také na tvorbě novely nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, konkrétně na stanovení odvětvových kritérií pro určení prvku kritické infrastruktury v oblasti kybernetické bezpečnosti. Návrh této novely byl v gesci Ministerstva vnitra. Novela nařízení vlády nabyla účinnosti rovněž dne 1. ledna 2015.

2.8.3. Tvorba kybernetické bezpečnostní politiky ČR

Zásadními počiny při utváření politiky kybernetické bezpečnosti ČR bylo zejména vytváření nové národní strategie kybernetické bezpečnosti ČR a navazujícího akčního plánu, který dotčenou strategii dále rozpracovává a konkretizuje jednotlivé úkoly pro odpovědné subjekty. Na základě podnětu Úřadu byla aktualizována Bezpečnostní strategie ČR tak, aby reflektovala změny bezpečnostního paradigmatu v blízkém pohraničí a posilování role nestátních aktérů a hrozeb včetně těch kybernetických. V neposlední řadě Úřad plnil roli gestora kybernetické bezpečnosti poskytováním stanovisek a komentářů k dalším návrhům materiálů, které se kybernetické bezpečnosti dotýkají, a připomínkováním legislativy, která by mohla mít dopady na oblast kybernetické bezpečnosti.

2.8.3.1. Národní strategie kybernetické bezpečnosti ČR a Akční plán kybernetické bezpečnosti ČR

V roce 2011 navázal Úřad na svého předchůdce, Ministerstvo vnitra, a drobnými úpravami aktualizoval tehdejší strategii kybernetické bezpečnosti.

Výsledkem těchto úprav byla Strategie pro oblast kybernetické bezpečnosti České republiky na období 2012 – 2015. Od té doby se podařilo dosáhnout mimo jiné i dvou důležitých milníků, které byly v této strategii stanoveny, a to přijetí zákona o kybernetické bezpečnosti a otevření NCKB, jehož součástí je funkční GovCERT.CZ pro zvládání kybernetických bezpečnostních incidentů. Ostatní cíle stanovené ve strategii bylo také možné považovat za splněné či průběžně naplňované.

S blížícím se ukončením platnosti uvedené strategie a splněním v ní stanovených zásadních cílů a úkolů začal v roce 2013 Úřad v souladu se svou úlohou národní autority v oblasti kybernetické bezpečnosti vytvářet, ve spolupráci se svými partnery, zcela novou Národní strategii kybernetické bezpečnosti na období let 2015 až 2020. Nová strategie představuje pro ČR zásadní předěl ve vnímání kybernetické bezpečnosti. Oproti minulé strategii se kvalitativně přesouvá od budování základních kapacit nezbytných pro zajištění základní míry kybernetické bezpečnosti směrem k jejímu dalšímu hlubšímu a pokročilému zajišťování.

Z cílů strategie vychází i Akční plán kybernetické bezpečnosti ČR na období let 2015 až 2020, který bude definovat konkrétní úkoly, stanoví u nich zodpovědnost, termíny jejich plnění a kontrolu.

2.8.4. Informační systémy důležité pro stát a komunikace se subjekty, které provozují KII a VIS

V roce 2014 bylo dokončeno mapování informačních a komunikačních systémů důležitých pro stát, a to jak u veřejnoprávních, tak u soukromoprávních subjektů. Mapování sloužilo zejména jako podklad pro tvorbu legislativy kybernetické bezpečnosti, přičemž jeho výsledky v posledních fázích posloužily k řádnému vymezení určujících kritérií KII a VIS. V rámci celého mapování bylo osloveno více než 90 subjektů a identifikováno více než 800 informačních systémů, které byly dále hodnoceny z hlediska důležitosti pro chod státu.

V rámci mapování byly s některými subjekty započaty také bezpečnostní projekty, které měly za cíl zlepšit úroveň zabezpečení daných informačních systémů. Tyto projekty probíhaly i v průběhu roku 2014.

Na základě provedeného mapování započala komunikace se subjekty, které by se měly stát správci KII nebo VIS podle zákona o kybernetické bezpečnosti. Cílem této komunikace je zejména příprava na plnění povinností stanovených uvedeným zákonem a vymezení jednotlivých informačních systémů a činností daných subjektů k jejich případnému určení za KII, případně za VIS.

Značné úsilí bylo také věnováno poskytování informací o dopadech přijaté právní úpravy včetně důsledků, které bude standardizovaná spolupráce v oblasti kybernetické bezpečnosti přinášet. Za tím účelem se zástupci NCKB aktivně účastnili konferencí k zákonu o kybernetické bezpečnosti a jeho prováděcím právním předpisům, konferencí ke kybernetické bezpečnosti, odborných seminářů apod. V neposlední řadě byla tato osvěta realizována i vzájemnými jednáními s mnoha subjekty, které spravují informační nebo komunikační technologie důležité pro stát.

2.8.5. Spolupráce Úřadu v oblasti kybernetické bezpečnosti

Stejně jako v předchozích letech, i v roce 2014 pokračoval Úřad v navazování a rozvíjení bilaterální a multilaterální mezinárodní spolupráce. Přehled mezinárodních aktivit v této oblasti je uveden v kapitole 2.2.4.

Pro zajišťování kybernetické bezpečnosti je důležitá i široká spolupráce na národní úrovni, která zahrnuje aktivní kooperaci mezi veřejnou a soukromou sférou a občanskou společností.

V roce 2014 pokračovala spolupráce mezi bezpečnostním týmem CSIRT.CZ a GovCERT.CZ, která z původní konzultační roviny přešla do roviny praktického řešení kybernetických incidentů. CSIRT.CZ nejenže spolupracoval na řešení útoků na informační infrastrukturu, ale současně se podílel na konzultacích k zákonu o kybernetické bezpečnosti a prováděcím právním předpisům. GovCERT.CZ se rovněž v součinnosti s laboratořemi CZ.NIC zapojil do skenování českých webů na zranitelnost HeartBleed. Spolupráce se osvědčila i v rámci letošního cvičení Cyber Europe, kde oba týmy společně řešily množství technických úkolů. Nelze nezmínit také první národní kybernetické cvičení pořádané Úřadem, na jehož scénářích se významnou měrou podíleli právě pracovníci CSIRT.CZ.

Mezi další CSIRT týmy, se kterými GovCERT.CZ udržuje úzké vztahy, patří CSIRT Masarykovy univerzity (CSIRT-MU). Ten se řadí ke špičkovým pracovištím evropského formátu. Spolupráce probíhá převážně v technické oblasti. Teoretická podpora je stejně jako v loňském roce doplněna stážemi v CSIRT-MU. Neméně zajímavé je i zapojení členů GovCERT.CZ do projektu Kybernetický polygon (KYPO), jež se zabývá výzkumem, vývojem a sestavením unikátního prostředí pro provádění a analýzu hrozeb ohrožujících bezpečnost KII či projektu Czech Cyber Crime Centre of Excellence, jehož cílem je vytvořit kvalitní centrum pro školení a vzdělávání v oblasti prevence a represe kybernetické kriminality.

Relevantními partnery v oblasti řešení kybernetických bezpečnostních incidentů jsou také zpravodajské služby a Policie ČR. Meritem takovéto spolupráce je především výměna informací o aktuálních a řešených kybernetických bezpečnostních incidentech, zkušeností s jejich zvládáním a vzájemného know-how.

GovCERT.CZ nadále úzce kooperuje s Centrem CIRC neboli hlavní složkou kybernetické bezpečnosti Armády ČR. Kromě výměny informací a sdílení zkušeností a informací o kybernetických incidentech se společně účastní také kybernetických cvičení, především Cyber Coalition, kde v rámci společné reprezentace ČR v NATO představují významné partnery při řešení scénářů.

NCKB již dříve navázal a nadále udržuje vztahy s akademickou sférou v ČR formou smluv o spolupráci. Ke konci roku 2014 byly podepsány smlouvy s následujícími akademickými institucemi: Masarykova univerzita, Vysoké učení technické v Brně, Univerzita obrany, České vysoké učení technické v Praze, Univerzita Palackého v Olomouci a vysoká škola CEVRO Institut, o.p.s. Jednání probíhají s Policejní akademií České republiky v Praze, Vysokou školou báňskou – Technickou univerzitou Ostrava a Univerzitou Karlovou v Praze.

Klíčovým partnerem pro NCKB, a to zejména v oblasti analýzy botnetů a poskytování informací o IP adresách a napadených počítačích malware, je společnost Microsoft. NCKB od společnosti získává unikátní data, se kterými dále pracuje. Díky jejich analýze a vyhodnocování dochází ke zvyšování kybernetické bezpečnosti ČR.

Skrze Českou bankovní asociaci spolupracuje NCKB také s bankami, které mají zájem na zvyšování ochrany jejich počítačové infrastruktury. Právě banky se stávají častým terčem kybernetických útoků.

GovCERT.CZ také úzce kooperuje s členy tzv. Bezpečné VLAN, nyní FENIX. Tento projekt by měl v budoucnu výrazně mírnit následky masivních DDoS útoků obdobných těm, jaké ČR zaznamenala v březnu 2013.

Mimo zmíněných partnerů na národní úrovni NCKB aktivně spolupracuje s Asociací krajů České republiky, Krajem Vysočina, AFCEA a Národním centrem pro bezpečnější internet.

V říjnu 2014 uspořádalo NCKB první národní cvičení v oblasti kybernetické bezpečnosti CYBER CZECH 2014. Jednalo se o netechnické, tzv. table-top cvičení, jehož záměrem bylo formou skupinové diskuze procvičit schopnost spolupráce při zvládání kybernetických bezpečnostních incidentů a ověřit komunikační kanály, které se při řešení používají. Celodenního cvičení se zúčastnili zástupci Ministerstva dopravy, Ministerstva financí, Ministerstva obrany, Ministerstva průmyslu a obchodu, Ministerstva vnitra, Ministerstva zahraničních věcí, Ministerstva práce a sociálních věcí, Ministerstva spravedlnosti, Ministerstva životního prostředí, Ministerstva školství, mládeže a tělovýchovy, dále Úřadu na ochranu osobních údajů, Českého telekomunikačního úřadu, České národní banky, Úřadu vlády ČR a Správy základních registrů. V rámci dvou simulovaných scénářů byli všichni sezvaní cvičící, coby bezpečnostní ředitelé a manažeři bezpečnosti informačních technologií fiktivního ministerstva, vystaveni otázkám, jak by postupovali v případě rozsáhlých DDoS útoků namířených na webové stránky tohoto ministerstva a cílených phishingových zpráv zaslaných jeho zaměstnancům.

Skupinu 16 cvičících doplňovala dvanáctičlenná odborná porota složená ze zástupců bezpečnostního týmu CSIRT.CZ, CSIRT-MU, poskytovatele internetových služeb ACTIVE 24, Nejvyššího státního zastupitelství, Policie ČR, zpravodajských služeb, dále odborníků na právo IT z Masarykovy univerzity a zástupců Úřadu. Jejich úkolem bylo hodnotit a doplňovat návrhy a odpovědi cvičících.

2.8.6. Zvyšování povědomí a osvěta

NCKB v souladu se svým posláním informuje veřejnost o svém zaměření a činnostech. Mezi tyto aktivity spadá zejména přednášková a osvětová činnost, poskytování rozhovorů do médií či správa internetových stránek www.govcert.cz, na kterých lze mj. nalézt aktuální informace o kybernetických bezpečnostních incidentech a zranitelnostech, včetně doporučení k jejich řešení a preventivních opatřeních, dále informace o legislativě včetně zákona o kybernetické bezpečnosti a s ním souvisejících prováděcích právních předpisů, podpůrné materiály k procesu

určování prvků KII a VIS aj. Zástupci NCKB se rovněž aktivně účastní odborných konferencí, a to jak v ČR, tak v zahraničí.

2.8.6.1. Vzdělávací a osvětové kampaně a konference

Úlohou NCKB je kromě koordinace spolupráce na národní a mezinárodní úrovni za účelem předcházení a řešení kybernetických bezpečnostních incidentů také osvěta a podpora vzdělávání v oblasti kybernetické bezpečnosti.

Významným partnerem Úřadu pro oblast vzdělávání se v roce 2014 stal Kraj Vysočina. Ten se zapojil do projektu Kraje pro bezpečný internet, pořádaného Národním centrem pro bezpečný internet, a v rámci osvěty v oblasti kybernetické bezpečnosti pořádá přednášky, školí studenty, rodiče, pedagogy i příslušníky Policie ČR. Zástupci NCKB se zúčastnili několika ze zmíněných přednášek.

Další osvětové aktivity zaměřuje NCKB na zaměstnance státní správy. Příkladem je přednáška v Ministerstvu vnitra (Problematika kybernetické bezpečnosti z hlediska mezinárodní spolupráce), v Ministerstvu obrany a NATO Allied Command Transformation Cyber Syndicate, kde zástupci NCKB prezentovali Národní strategii kybernetické bezpečnosti na období let 2015 až 2020 a profil NCKB coby gestora kybernetické bezpečnosti v ČR. V listopadu 2014 se uskutečnil seminář na téma nové strategie kybernetické bezpečnosti ČR a ochrany KII i na půdě Poslanecké sněmovny Parlamentu ČR.

Jak již bylo zmíněno, zástupci NCKB se také často v pozici prezentujících účastní zahraničních konferencí, školení, workshopů a přednášek. Namátkou může být uvedena konference Meridian Process 2014, jež se konala v listopadu 2014 v Japonsku, kam byl pozván pracovník NCKB, aby představil proces mapování KII v ČR a seznámil mezinárodní publikum s českým konceptem zabezpečení kybernetického prostředí včetně způsobu určování KII.

V rámci tuzemských konferencí lze zmínit přednášku na mezinárodním policejním kongresu Současné trendy v kyberkriminalitě v Ostravě nebo IDG konferenci v říjnu 2014, kde proběhla prezentace zkušeností s projektem Botnet Feeds. V tomtéž měsíci se konala také třídenní mezinárodní konference Future Crisis, jedno z největších setkání národních i mezinárodních bezpečnostních složek se zástupci obranného průmyslu, kde opět vystoupili zástupci NCKB s cílem seznámit posluchače s procesem určování KII. Soustavná spolupráce pokračovala s organizací AFCEA a s Policejní akademií České republiky v Praze.

2.8.6.2. Ostatní přednášky a konference

V roce 2014 navázalo NCKB kontakty s několika dalšími institucemi zabývajícími se kybernetickou bezpečností. Jednou z aktivních neziskových organizací dlouhodobě se zabývající problematikou kybernetické bezpečnosti je Národní centrum pro bezpečnější internet (NCBI), jehož nejdůležitějším projektem je Saferinternet.cz, který usiluje o zvyšování povědomí o bezpečnějším užívání internetu. Právě s NCBI byla navázána spolupráce, v jejímž rámci se několik pracovníků Úřadu v čele s ředitelem NCKB jako hosté i jako účinkující zúčastnilo

přednášek a workshopů pořádaných právě NCBI. V říjnu 2014 na žádost NCBI převzalo NCKB záštitu nad Evropským měsícem kybernetické bezpečnosti.

Seznam některých použitých zkratek a pojmů je uveden v příloze.

2.9. OPRAVNÉ PROSTŘEDKY

2.9.1. Bezpečnostní řízení

V roce 2014 rozhodoval ředitel Úřadu o opravných prostředcích ze strany fyzických osob a podnikatelů podaných podle příslušných ustanovení zákona formou rozkladu proti následujícím rozhodnutím Úřadu:

- rozhodnutí o nevydání osvědčení či dokladu fyzické osoby nebo osvědčení podnikatele,
- rozhodnutí o zrušení platnosti osvědčení či dokladu fyzické osoby nebo osvědčení podnikatele,
- rozhodnutí o zastavení bezpečnostního řízení.

O podaných rozkladech rozhodoval ředitel Úřadu vždy na základě návrhu rozkladové komise, která byla, v souladu s § 130 zákona, ustavena ke dni 1. ledna 2011. Lhůta k rozhodnutí o rozkladu, kterou zákon v ustanovení § 130 odst. 6 stanoví v délce 3 měsíců, nebyla v žádném z případů překročena.

Rozhodnutí ředitele Úřadu o rozkladu lze napadnout správní žalobou, o níž rozhoduje Městský soud v Praze. Proti rozhodnutí Městského soudu v Praze je dále možno podat kasační stížnost, o níž rozhoduje Nejvyšší správní soud. V případě neúspěchu ve správním soudnictví se účastník řízení může obrátit se svou stížností na Ústavní soud.

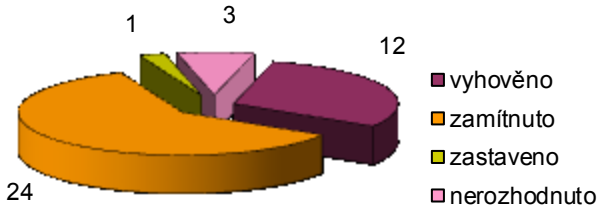
2.9.1.1. Statistické přehledy

2.9.1.1.1. Rozklady

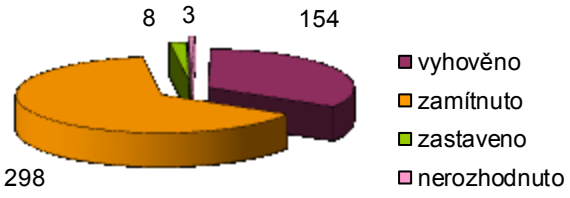
Rozklady proti rozhodnutím Úřadu v oblasti bezpečnostního řízení
(rozhoduje ředitel Úřadu)

Rok	Dosud nerozhodnuto	Vyhověno	Zamítnuto	Zastaveno	Celkem
2013	0	4	25	1	**30**
2014	3	12	24	1	**40**

Řízení o rozkladu v roce 2014



Řízení o rozkladu v letech 2006 – 2014



2.9.1.1.2. Žaloby správní

Žaloby proti rozhodnutím ředitele Úřadu o rozkladu podle zákona v letech 2006 – 2014
(rozhoduje Městský soud v Praze)

Celkem	Dosud nerozhodnuto	Řízení zastaveno	Vyhověno	Zamítnuto	Odmítnuto
90	19	14	14	41	2

2.9.1.1.3. Kasační stížnosti

Kasační stížnosti proti rozhodnutím Městského soudu v Praze o zamítnutí žaloby v letech 2006 – 2014 *(rozhoduje Nejvyšší správní soud v Brně)*

Celkem	Dosud nerozhodnuto	Řízení zastaveno	Vyhověno	Zamítnuto	Odmítnuto
22	0	0	5	15	2

Kasační stížnosti podané Úřadem proti rozhodnutím Městského soudu v Praze o vyhovění žalobě v letech 2006 – 2014 *(rozhoduje Nejvyšší správní soud v Brně)*

Celkem	Dosud nerozhodnuto	Řízení zastaveno	Vyhověno	Zamítnuto	Odmítnuto
4	1	0	3	0	0

2.9.1.1.4. Ústavní stížnosti

Ústavní stížnosti podané účastníky řízení v letech 2006 – 2014 *(rozhoduje Ústavní soud v Brně)*

Celkem	Dosud nerozhodnuto	Řízení zastaveno	Vyhověno	Zamítnuto	Odmítnuto
4	1	0	0	0	3

2.9.1.2. Hodnocení rozhodovací praxe Úřadu

Jak vyplývá z výše uvedených údajů, v současné době je rozhodnuto v 71 případech o žalobách proti rozhodnutí ředitele Úřadu o rozkladu, přičemž pouze 14 žalob bylo shledáno důvodnými. „Úspěšnost“ Úřadu tedy činí 80 %.

2.9.2. Správní řízení o pokutě

V roce 2014 ředitel Úřadu rozhodoval ve 2 případech o opravných prostředcích – rozkladech – uplatněných ze strany fyzických osob ve správním řízení pro porušení povinností v oblasti ochrany utajovaných informací, přičemž obě podání byla na základě návrhu rozkladové komise zamítnuta. Žaloba k Městskému soudu v Praze nebyla účastníky řízení ani v jednom případě podána.

2.9.3. Řízení podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím

V roce 2014 ředitel Úřadu rozhodoval rovněž o jednom opravném prostředku – rozkladu – uplatněnému v řízení podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, proti rozhodnutí Úřadu o odmítnutí žádosti o poskytnutí informace. Na základě návrhu příslušné rozkladové komise byl rozklad zamítnut, žaloba k Městskému soudu v Praze nebyla účastníkem řízení podána.

2.10. VÝZKUMNÁ A VÝVOJOVÁ ČINNOST ÚŘADU

2.10.1. Cíle a organizace výzkumu a vývoje

Hlavním cílem v oblasti výzkumu a vývoje pro rok 2014 byl rozvoj bezpečnostních technologií pro ochranu utajovaných informací v komunikačních a informačních systémech a jejich nasazení v reálném provozu ve vybraných institucích státní správy.

2.10.2. Projekty realizované v roce 2014

Koncepce výzkumu a vývoje se vytvářela na základě zjištěných poznatků Úřadu při certifikační a konzultační činnosti, při jednáních se zástupci orgánů státní správy a při výkonu státního dozoru.

Část projektů realizovaných v roce 2014 navazovala na projekty započaté v roce 2013, zároveň byly zahájeny 4 projekty nové. Všechny projekty byly realizovány ve spolupráci s externími řešiteli.

Věcně byly projekty zaměřeny do oblasti kryptografické ochrany a ochrany proti úniku utajovaných informací kompromitujícím vyzařováním.

Výsledkem realizovaných projektů jsou metodiky, analýzy, specializovaný hardware a software, technické a kryptografické prostředky a speciální měřící zařízení sloužící k uspokojení reálných potřeb bezpečnostní praxe, využitelné na národní úrovni zejména orgány státní správy a bezpečnostními složkami pracujícími s utajovanými informacemi. V obecnější rovině jsou projekty prezentovány i na mezinárodní úrovni zahraničním bezpečnostním autoritám, s nimiž Úřad spolupracuje.

V roce 2014 Úřad dále rozvíjel svou koncepci výzkumu a vývoje v oblasti kryptografické ochrany a ochrany proti úniku utajovaných informací kompromitujícím vyzařováním tak, aby mj. reflektovala požadavky rezortů státní správy, pro které jsou tyto druhy zajištění ochrany utajovaných informací nezbytné.

2.11. STÁTNÍ DOZOR

Na základě § 137 písm. b) zákona vykonává Úřad v oblasti ochrany utajovaných informací a bezpečnostní způsobilosti státní dozor, čímž se rozumí dozor nad tím, jak orgány státu, právnické osoby, podnikající fyzické osoby a fyzické osoby dodržují právní předpisy v dané oblasti. Podle zákona státnímu dozoru nepodléhá činnost zpravodajských služeb a ve stanovených případech činnost Ministerstva vnitra.

Cílem státního dozoru je především zjistit skutečný stav ochrany utajovaných informací, resp. plnění povinností v oblasti bezpečnostní způsobilosti u kontrolovaných osob, ověřit praktickou aplikaci právních norem upravujících kontrolovanou oblast a zároveň přispět k zabezpečení ochrany utajovaných informací předcházením neoprávněnému nakládání s utajovanými informacemi a k posilování právního vědomí kontrolovaných osob a sjednocování způsobu aplikace právních předpisů v této oblasti.

Na začátku roku 2014 bylo provedeno metodické proškolení zaměstnanců Úřadu, kteří se podílejí na výkonu státního dozoru. Školení bylo zaměřeno na aplikaci nové procesní právní úpravy kontrolního postupu – zákona č. 255/2012 Sb., o kontrole (kontrolní řád), který nabyl účinnosti 1. ledna 2014.

2.11.1. Kontroly provedené v roce 2014

Stejně jako v předchozích letech byly i v tomto roce kontroly prováděny na základě průběžně doplňovaných půlročních plánů kontrol schvalovaných ředitelem Úřadu. Z hlediska rozsahu byly realizovány komplexní kontroly zaměřené na ověření skutečného stavu ve všech druzích zajištění ochrany utajovaných informací, které byly kontrolovanými osobami realizovány, a tematické kontroly, při kterých byla kontrolována pouze určitá dílčí oblast. V závěru roku 2014 byla dále provedena 1 kontrola v oblasti bezpečnostní způsobilosti (spolu s kontrolou v oblasti ochrany utajovaných informací). Dokončení této kontroly se předpokládá v lednu nebo únoru 2015.

Do plánů kontrol byly, pro zachování určité časové periodicity, zařazovány opakované kontroly u subjektů, u kterých vznikají nebo jim jsou poskytovány utajované informace. Dále byly vybírány subjekty, u kterých ještě kontrola nebyla provedena. Jednotlivé kontroly byly do plánů kontrol zařazovány rovněž z podnětu organizačních celků Úřadu, na základě konkrétních poznatků získaných vlastní činností Úřadu nebo z podnětu vnějších subjektů.

V roce 2014 provedl Úřad celkem 81 kontrol, z toho 12 v orgánech státu, jejich složkách nebo jimi zřizovaných příspěvkových organizacích, 10 v krajských úřadech a 59 u podnikatelů. Souhrnné údaje o kontrolách a přehled jednotlivých kontrolních akcí realizovaných v roce 2014 je uveden v následujících tabulkách.

Kontroly provedené v roce 2014

Kontroly	Komplexní	Tematické	Následné	Celkem
Orgány státu	10	2	0	**12**
Krajské úřady	10	0	0	**10**
Podnikatelé	30	29	0	**59**
Celkem	**50**	**31**	**0**	**81**

Kontroly v orgánech státu a jejich součástech v roce 2014

Kontrolovaná osoba	Kontrolovaná osoba
Česká národní banka	Ministerstvo zahraničních věcí – zastupitelský úřad ČR v Haagu
Ministerstvo dopravy	
Ministerstvo kultury	Ministerstvo zahraničních věcí – zastupitelský úřad ČR v Pretorii
Ministerstvo práce a sociálních věcí	
Ministerstvo spravedlnosti	Ministerstvo zahraničních věcí – zastupitelský úřad ČR ve Washingtonu
Ministerstvo životního prostředí	
Státní úřad pro jadernou bezpečnost	Úřad vlády ČR
Ředitelství silnic a dálnic ČR (kontrola dosud nebyla ukončena)	

Kontroly v krajských úřadech v roce 2014

Kontrolovaná osoba	Kontrolovaná osoba
Krajský úřad Jihočeského kraje	Krajský úřad Moravskoslezského kraje
Krajský úřad Jihomoravského kraje	Krajský úřad Pardubického kraje
Krajský úřad kraje Vysočina	Krajský úřad Plzeňského kraje
Krajský úřad Královéhradeckého kraje	Krajský úřad Středočeského kraje
Krajský úřad Libereckého kraje	Krajský úřad Zlínského kraje

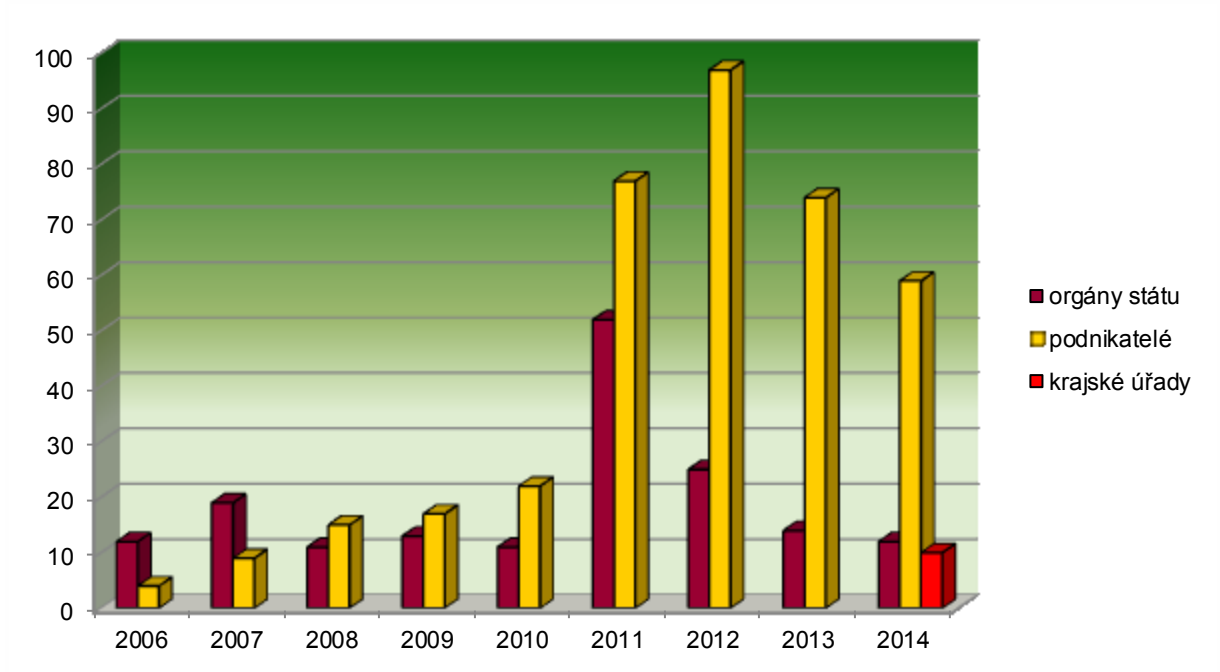
Kontroly u podnikatelů v roce 2014

Kontrolovaná osoba	Kontrolovaná osoba
AERO TRADE a.s.	ALKOM Security, a.s.
AERO Vodochody a.s.	ALZAKOM, spol. s r.o.
AERO Vodochody AEROSPACE a.s.	ASTOR-KOMPLEX s.r.o.
AG COM, s.r.o.	Blue Partners s.r.o.

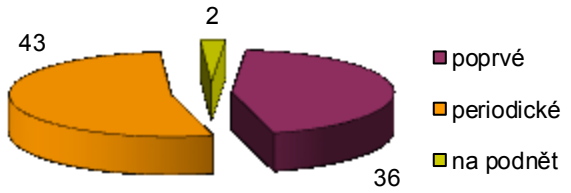
Kontrolovaná osoba	Kontrolovaná osoba
COMINFO, a.s.	LABOX spol. s r.o.
CSC Computer Sciences s.r.o.	LOM Praha s.p.
Česká pošta, s.p.	MARCO-CZECH s.r.o.
České aerolinie a.s.	MARHOLD a.s.
České Radiokomunikace, a.s.	MESIT přístroje spol. s r.o.
ČEZ Distribuce, a. s.	MPI CZ s.r.o.
ČEZ ICT Services, a. s.	OHL ŽS, a.s.
DBD CONTROL SYSTEMS s.r.o.	OVA!!!CLOUD.net a.s.
DELINFO spol. s r.o.	Řízení letového provozu České republiky, státní podnik
DICOM, spol. s r.o.	
DMS s.r.o.	S com s.r.o.
EKOKLIMA akciová společnost	S u b t e r r a a.s.
FASS, s.r.o.	S&T CZ s.r.o.
GEOtest, a.s.	Sellier & Bellot a.s.
GORDIC spol. s r.o.	SILBA-Elstav s.r.o.
GTS Czech s.r.o.	STAEG Facility, spol. s r.o.
HELIKA, a.s.	STAEG, spol. s r.o.
HES, s.r.o.	STÁTNÍ TISKÁRNA CENIN, státní podnik
INSTALACE Praha, spol. s r.o.	SUPTel a.s.
INTAR a.s.	SYNER Morava, a.s.
Integoo s.r.o.	TERMOMONT s.r.o.
INTRIPLE, a.s.	TEZAO s.r.o.
INTV spol. s r.o.	T-SOFT a.s.
ITS akciová společnost	Vegacom a.s.
JOHNSON CONTROLS INTERNATIONAL, spol. s r.o.	Vodohospodářské stavby, společnost s ručením omezeným
KONSIT a.s.	Zeppelin CZ s.r.o.

V následujících grafech jsou znázorněny počty a poměr jednotlivých kontrol z hlediska typu a důvodu provedení (periodické kontroly, kontroly na základě vnějšího nebo vnitřního podnětu, následné kontroly zaměřené na ověření odstranění nedostatků zjištěných při předcházející kontrole).

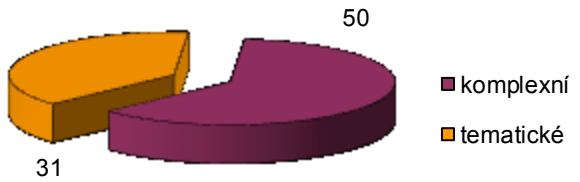
Kontroly v letech 2006 až 2014



Kontroly 2014 – podle důvodu



Kontroly 2014 – podle typu



2.11.2. Výsledky kontrol

Nedostatky zjištěné při kontrolách, vyplývající z porušení nebo nedodržení jednotlivých ustanovení zákona a dalších právních předpisů, byly uváděny jako kontrolní zjištění v protokolech o jednotlivých kontrolách. Z celkového počtu 80 kontrol dokončených v roce 2014 (1 kontrola v současné době stále probíhá) byly nedostatky zjištěny ve 41 případech (51 %). V 15 případech (téměř 19 %) byl, vzhledem k charakteru zjištěných nedostatků, podán podnět k zahájení správního řízení pro podezření ze spáchání přestupku nebo správního deliktu.

Nedostatky zjišťované při výkonu státního dozoru se, jako v předcházejících letech, objevovaly téměř ve všech druzích zajištění ochrany utajovaných informací. Jejich příčinou bylo ve většině případů selhání lidského činitele. Při kontrolách provedených v roce 2014 byly zjištěny zejména níže uvedené nedostatky.

Obecné nedostatky

- nesplnění některé z podmínek pro výkon funkce bezpečnostního ředitele,

- klasifikace utajované informace (dokumentu) nesprávným stupněm utajení,

- nesoulad postupu stanoveného vnitřním předpisem pro manipulaci s utajovanou informací s platnou právní úpravou.

Personální bezpečnost

- přístup k utajované informaci zjištěný u fyzické osoby, která nesplňovala všechny zákonem stanovené podmínky pro tento přístup (neprovedení poučení, absence osvědčení fyzické osoby nebo oznámení o splnění podmínek pro přístup k utajované informaci stupně utajení Vyhrazené, případně dokladu, nedodržení principu „need to know“),

- nesplnění všech podmínek pro přístup k utajované informaci u osoby vykonávající činnost nebo funkci, pro kterou to vyžaduje právní předpis (výkon správy informačních systémů),

- neprovádění pravidelného školení osob, které mají přístup k utajovaným informacím,

- nezaslání výtisku poučení Úřadu podle § 11 odst. 2 zákona,

- neprovedení ověření, zda fyzická osoba po uplynutí zákonem stanovené lhůty i nadále splňuje podmínky pro přístup k utajované informaci stupně utajení Vyhrazené,

- nezaslání písemného oznámení o skončení služebního poměru nebo pracovněprávního, členského nebo obdobného vztahu, ve kterém byl fyzické osobě umožněn přístup k utajované informaci stupně utajení Přísně tajné, Tajné nebo Důvěrné, Úřadu,

- neplnění dalších zákonem stanovených povinností (nevyhotovení písemného záznamu o zániku platnosti oznámení o splnění podmínek pro přístup k utajované informaci stupně utajení Vyhrazené),

- formální nedostatky vyhotovených písemných dokladů (chybějící údaje na výtisku poučení, forma poučení neodpovídala vzoru stanovenému platnou právní úpravou).

Průmyslová bezpečnost

- přístup k utajované informaci zjištěný u podnikatele, který nesplňoval zákonem stanovené podmínky pro tento přístup (absence osvědčení podnikatele).

Administrativní bezpečnost

- nedostatky ve způsobu vedení evidence utajovaných dokumentů a ve vedení dalších administrativních pomůcek (neúplné nebo nesprávné zápisy, chybně prováděné opravy, neuzavírání zápisů v jednacím protokolu na konci

kalendářního roku, neuvádění některých osob, které se seznámily s obsahem utajovaného dokumentu, v kontrolním listu),

- používání administrativních pomůcek, které nesplňovaly požadavky stanovené právním předpisem na jejich obsah a úpravu (autentizace),

- neuložení kontrolního listu u jednacího protokolu po odeslání nebo vyřazení utajovaného dokumentu vyhotoveného po 31. prosinci 2011,

- nedostatky ve vyznačování náležitostí utajovaných dokumentů (nevyznačený nebo chybně vyznačený stupeň utajení, nesprávné nebo chybějící další povinné náležitosti vlastního nebo doručeného utajovaného dokumentu),

- neplnění dalších povinností stanovených v oblasti administrativní bezpečnosti právními předpisy (např. při předávání utajovaných informací, při změně nebo zrušení stupně utajení nebo při změně osoby pověřené vedením evidence utajovaných informací, při vyhotovování opisu, kopie nebo výpisu z utajovaného dokumentu, neuvádění údajů o skartaci).

Činnost registrů utajovaných informací

- nedostatky v evidenci utajovaných informací (dokumentů) poskytnutých cizí mocí a ve vedení dalších administrativních pomůcek (nesplnění požadavku na oddělenou evidenci utajovaných dokumentů podle původce, slučování více utajovaných dokumentů pod 1 evidenční označení, chybné nebo neúplné záznamy).

Fyzická bezpečnost

- nedostatky v realizaci opatření fyzické bezpečnosti (nefunkčnost použitých technických prostředků, jejich nesprávná instalace nebo nastavení, nesplnění minimálních požadavků stanovených právními předpisy),

- nesoulad skutečného stavu opatření fyzické bezpečnosti se stavem deklarovaným v projektu fyzické bezpečnosti (nesprávné bodové hodnocení jednotlivých opatření a technických prostředků v projektu),

- ukládání utajovaných informací mimo zabezpečené oblasti,

- porušení režimových pravidel pro pohyb osob v objektu nebo zabezpečené oblasti (vstup neoprávněných osob bez doprovodu osoby oprávněné ke vstupu),

- neplnění dalších povinností stanovených v oblasti fyzické bezpečnosti právními předpisy (např. absence průběžného ověřování vyhodnocení rizik).

Bezpečnost informačních a komunikačních systémů

- nesplnění požadavků na provoz informačního systému (neaktualizovaná databáze antivirového programu).

V rámci výkonu státního dozoru Úřad mj. získává poznatky, které pomáhají vyhodnotit efektivitu právní úpravy a konkrétních řešení jednotlivých oblastí ochrany utajovaných informací a bezpečnostní způsobilosti, a je konfrontován s problémy při aplikaci právních předpisů a při praktické realizaci ochrany utajovaných informací. Výkon státního dozoru je tak významným zdrojem potřebné zpětné vazby využitelné například při přípravě novelizací právních předpisů. V rámci metodické činnosti vůči orgánům státu i podnikatelům majícím přístup k utajovaným informacím se Úřad rovněž zaměřuje právě na problémové oblasti a konkrétní nedostatky zjištěné při výkonu státního dozoru.

2.12. METODICKÁ ČINNOST ÚŘADU

Metodickou činnost vůči orgánům státu a jejich organizačním složkám a vůči podnikatelům vykonával Úřad v roce 2014 především v rámci odborné činnosti jednotlivých organizačních celků Úřadu, a to prostřednictvím poskytování osobních konzultací, odpovídání na telefonické, písemné nebo elektronickou formou položené dotazy a rovněž při výkonu státního dozoru a provádění tzv. dohlídek v průběhu bezpečnostního řízení u podnikatelů.

Stěžejními tématy metodické činnosti byla oblast bezpečnostního řízení, podání, respektive vyplnění samotné žádosti o vydání osvědčení nebo dokladu, způsob a forma hlášení změn, proces bezpečnostního řízení, certifikace informačních systémů, postupy při zpracovávání bezpečnostní dokumentace včetně projektu fyzické bezpečnosti, a v neposlední řadě i konkrétní postupy při aplikaci právních předpisů v oblasti administrativní a fyzické bezpečnosti.

Nejčastěji kladené dotazy a odpovědi stejně jako vydávaná stanoviska a jednotné návody Úřad uveřejňuje na svých internetových stránkách (viz kap. 2.13.2.).

2.12.1. Metodická činnost v oblasti bezpečnostního řízení

Metodická činnost Úřadu v oblasti bezpečnostního řízení je nezbytným, trvalým a kontinuálním procesem, který probíhal i v roce 2014. Členění této činnosti korespondovalo s jednotlivými fázemi bezpečnostního řízení.

První oblastí bylo poskytování konzultací a metodických doporučení fyzickým osobám, podnikatelům, odpovědným osobám a bezpečnostním ředitelům pro přípravu a realizaci žádosti o vydání osvědčení fyzické osoby nebo osvědčení podnikatele nebo dokladu.

Druhá oblast je spojena s postupem Úřadu podle § 102 zákona, kdy Úřad při podání žádosti, pokud je to možné, pomáhá účastníkovi řízení s odstraněním nedostatků žádosti na místě, nebo s postupem podle § 103 zákona, podle kterého je Úřad oprávněn požadovat upřesnění údajů uvedených v žádosti nebo sdělení

doplňujících údajů k ověření splnění podmínek pro vydání osvědčení fyzické osoby nebo podnikatele nebo dokladu.

Jako třetí oblast metodické činnosti lze označit metodické vedení držitelů osvědčení nebo dokladu formou konzultací a informací uveřejňovaných na internetových stránkách Úřadu.

Čtvrtou oblastí bylo poskytování konzultací a metodických doporučení při přípravě a zpracování opakovaných žádostí v souvislosti se zachováním přístupu k utajovaným informacím. V této rovině lze označit za velmi významnou metodickou činnost Úřadu především ve směru k držitelům osvědčení podnikatele, kteří i bezprostředně po uplynutí doby platnosti dosavadního osvědčení nadále předpokládali přístup k utajovaným informacím, protože případné nedodržení zákonem stanovené lhůty pro podání žádosti podnikatele k vydání navazujícího osvědčení by u podnikatelů, u kterých se vyskytují utajované informace, mohlo mít za následek přerušení kontinuity ochrany utajovaných informací a fakticky zapříčinit situace, ve kterých může nastat porušení zákona spolu s reálným ohrožením utajovaných informací.

V hodnoceném roce byla metodická činnost orientována především do oblastí poskytování prvotních informací a metodických doporučení před podáním žádosti, poskytování pomoci, konzultací a metodických doporučení při odstraňování nedostatků v žádosti a do oblasti metodického vedení fyzických osob a podnikatelů, kteří jsou již držiteli osvědčení, a dále poskytování informací a metodické pomoci pro podnikatelské subjekty, které hodlaly učinit prohlášení podnikatele podle § 15a zákona.

V souvislosti s konzultační a metodickou činností Úřadu nelze opomenout účast jeho zaměstnanců na přednáškách, seminářích a školeních organizovaných různými státními, ale i soukromými subjekty. Tato metodická činnost Úřadu byla zaměřena na poskytnutí informací k zákonu, otázkám bezpečnostního řízení a povinnostem držitelů osvědčení podnikatele, a dále na změny, které v oblasti personální a průmyslové bezpečnosti a v oblasti bezpečnostní způsobilosti přinesla zásadní novela zákona (zákon č. 255/2011 Sb.) a aktuální vyhlášky o personální bezpečnosti a o bezpečnostní způsobilosti a o průmyslové bezpečnosti. S velkým zájmem a pozitivními ohlasy se Úřad setkával i v rámci otázek věnovaných prohlášení podnikatele.

2.13. VĚSTNÍK ÚŘADU A INTERNETOVÉ STRÁNKY ÚŘADU

2.13.1. Věstník Úřadu

Úřad vydává, v souladu se zákonem, Věstník Úřadu jako periodickou tiskovinu, která vychází dvakrát ročně, v případě potřeby i vícekrát. V roce 2014 byla vydána dvě pravidelná čísla.

Obsahem Věstníku Úřadu je především seznam certifikovaných technických prostředků a seznam podnikatelů, kteří jsou držiteli osvědčení podnikatele.

Ve Věstníku Úřadu jsou dále zveřejňovány informace z oblasti personální, administrativní, průmyslové a fyzické bezpečnosti, bezpečnosti informačních a komunikačních systémů, kryptografické ochrany utajovaných informací a bezpečnostní způsobilosti. Dále jsou zveřejňovány metodické návody, různé pokyny, návody a instrukce, žádosti a informace určené odborné veřejnosti.

Věstník Úřadu není distribuován formou volného prodeje. Lze jej zakoupit pouze předplatitelskou formou (v současné době je registrováno cca 2 500 předplatitelů). Věstník lze rovněž objednat přímo v obchodním oddělení Tiskárny Ministerstva vnitra.

Obsah Věstníku Úřadu je zveřejňován také na internetových stránkách Úřadu.

2.13.2. Internetové stránky Úřadu

Na internetových stránkách Úřadu www.nbu.cz jsou zveřejňovány relevantní informace, které se týkají činnosti Úřadu a jeho hlavních úkolů. Jsou zde uvedeny odborné i všeobecné informace, včetně aktualit a kontaktních spojení. Všechny údaje jsou průběžně aktualizovány.

Internetové stránky Úřadu obsahují především podrobné informace pro účastníky bezpečnostního řízení a pro držitele osvědčení, a to ohledně podání žádosti o vydání osvědčení nebo dokladu, oznamování změn apod. Dále je na nich zveřejňován přehled všech platných právních předpisů upravujících oblast ochrany utajovaných informací a bezpečnostní způsobilosti, průběžně aktualizovaný o jejich novelizace. Internetové stránky také obsahují seznamy platných a neplatných osvědčení podnikatele a osvědčení podnikatele pro cizí moc, seznamy osvědčení fyzické osoby a dokladů o bezpečnostní způsobilosti, jejichž platnost byla zrušena nebo zanikla poškozením osvědčení či doručením oznámení o jeho odcizení nebo ztrátě, seznamy certifikovaných technických prostředků apod. Zveřejňovány jsou rovněž aktuální metodické návody a zpřístupněny jsou i elektronické verze dotazníků a žádostí. Je zde umístěn i odkaz na protikorupční linku 199. Internetové stránky vždy obsahují poslední číslo Věstníku Úřadu.

Obsahem svých internetových stránek Úřad také reaguje na nejčastěji kladené dotazy tak, aby na nich jejich uživatelé nalezli vše, co potřebují vědět o problematice utajovaných informací, bezpečnostní způsobilosti i o Úřadu samotném. V roce 2014 zůstaly nejvíce vyhledávanými informace týkající se bezpečnostního řízení.

V souvislosti s problematikou kybernetické bezpečnosti, jejímž gestorem a zároveň národní autoritou pro tuto oblast je Úřad, jsou pod hlavičkou NCKB provozovány stránky www.govcert.cz, na kterých uživatelé naleznou aktuality z této oblasti, informace o činnosti Rady pro kybernetickou bezpečnost, informační servis a preventivní upozornění.

Internetové stránky Úřadu splňují pravidla přístupnosti podle vyhlášky č. 64/2008 Sb., o formě uveřejňování informací souvisejících s výkonem veřejné

správy prostřednictvím webových stránek pro osoby se zdravotním postižením (vyhláška o přístupnosti), a s jejich obsahem se tak mohou seznámit i osoby se zdravotním postižením.

Záznam Internetových stránek Úřadu je součástí bibliografie a katalogu Národní knihovny ČR. Stránky jsou opatřeny logem Webarchiv.

2.14. POSKYTOVÁNÍ INFORMACÍ PODLE ZÁKONA Č. 106/1999 SB., O SVOBODNÉM PŘÍSTUPU K INFORMACÍM

V roce 2014 bylo Úřadu podáno 9 žádostí o informace podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů.

8 žádostem bylo v plném rozsahu vyhověno a požadované informace byly žadatelům poskytnuty. 1 žádost byla rozhodnutím odmítnuta. Proti tomuto rozhodnutí byl uplatněn opravný prostředek – rozklad – viz kap. 2.9.3.

V roce 2014 nebyla poskytnuta žádná výhradní licence. Podána byla 1 stížnost podle § 16a zákona č. 106/1999 Sb., které ředitel Úřadu vyhověl.

2.15. INSPEKCE ŘEDITELE ÚŘADU

Inspekce ředitele Úřadu v průběhu roku 2014 prováděla, v rámci plnění dlouhodobých úkolů, činnosti související s výkonem interní kontroly určených oblastí působnosti Úřadu.

V roce 2014 inspekce ředitele Úřadu řešila 2 stížnosti, které byly vyhodnoceny jako nedůvodné.

3. BEZPEČNOSTNÍ, EKONOMICKÉ A PERSONÁLNÍ ZABEZPEČENÍ ÚŘADU

3.1. OCHRANA UTAJOVANÝCH INFORMACÍ A KRIZOVÉ ŘÍZENÍ V ÚŘADU

3.1.1. Vnitřní kontrola ochrany utajovaných informací

Ochranu utajovaných informací v rámci Úřadu zajišťuje odbor bezpečnostní, který rovněž provádí vnitřní kontrolu jejího dodržování.

V roce 2014 byla kontrolní činnost zaměřena na dodržování povinností stanovených zákonem a interními akty řízení Úřadu, zejména směrnicí ředitele Úřadu č. 13/2007, o provozním řádu Národního bezpečnostního úřadu (dále jen „provozní řád“).

Kontrolní činnost byla vykonávána v následujícím rozsahu: zabezpečení pracoviště při krátkodobé a dlouhodobé nepřítomnosti zaměstnance, uložení klíčů od pracoviště, ukládání utajovaných informací do úschovných objektů, zabezpečení úschovných objektů z hlediska jejich uzamčení a neporušenosti hologramů, zabezpečení ostatních neutajovaných dokumentů a zabezpečení výpočetní techniky proti jejímu zneužití nepovolanou osobou.

V roce 2014 nebylo zjištěno závažné porušení ochrany utajovaných informací zaměstnanci Úřadu. Rovněž ustanovení provozního řádu byla v roce 2014 zaměstnanci Úřadu dodržována a při kontrolách nebyly zjištěny závažné nedostatky.

3.1.2. Personální bezpečnost v rámci Úřadu

Odbor bezpečnostní zajišťuje a provádí bezpečnostní řízení o vydání osvědčení fyzické osoby u uchazečů o zaměstnání v Úřadu a u zaměstnanců Úřadu, vydává osvědčení pro cizí moc a realizuje bezpečnostní řízení o zrušení platnosti osvědčení zaměstnanců Úřadu. V případě potřeby vydává uvedeným osobám také oznámení o splnění podmínek pro přístup k utajované informaci stupně utajení Vyhrazené. Dále zajišťuje poučení fyzických osob – zaměstnanců Úřadu, před prvním přístupem k utajované informaci, vede evidenci poučených osob a posuzuje, zda i nadále splňují podmínky pro vydání osvědčení.

V souladu s § 67 odst. 1 písm. b) zákona bylo provedeno každoroční proškolení zaměstnanců Úřadu z právních předpisů v oblasti ochrany utajovaných informací.

V roce 2014 bylo evidováno 76 žádostí o vydání osvědčení fyzické osoby, na jejichž základě bylo vydáno 55 osvědčení fyzické osoby. Ve zbývajících případech nebyla bezpečnostní řízení k 31. prosinci 2014 ukončena.

Vydaná osvědčení fyzické osoby v rámci Úřadu v roce 2014

Důvěrné	9
Tajné	50
Přísně tajné	25
Celkem	**84**

Důvody zániku platnosti osvědčení fyzické osoby v rámci Úřadu v roce 2014

Doručení nového osvědčení	54
Změna některého z údajů uvedených v osvědčení	2
Celkem	**56**

Vydaná osvědčení fyzické osoby pro cizí moc v rámci Úřadu v roce 2014

COSMIC TOP SECRET ATOMAL	3
COSMIC TOP SECRET	14
NATO SECRET	13
Celkem	**30**

V roce 2014 bylo dále vydáno 7 oznámení o splnění podmínek pro přístup k utajované informaci stupně utajení Vyhrazené.

3.1.3. Fyzická bezpečnost v rámci Úřadu

V roce 2014 započala rekonstrukce elektrické požární signalizace pro objekty areálu Úřadu v Praze.

V loňském roce Úřad převzal zrealizovanou zakázku zabezpečení objektu NCKB v Brně. V areálu NCKB byly nainstalovány technologie poplachového zabezpečovacího a tísňového systému (PZTS), uzavřeného kamerového televizního okruhu (CCTV), elektronické kontroly vstupu (EKV), elektrické požární signalizace (EPS), stabilního hasicího zařízení (SHZ) a bezpečnostního oplocení. V průběhu roku 2014 byly bezpečnostní systémy „oživeny“ a bylo zprovozněno online propojení obou areálů Úřadu.

V roce 2014 byl dále vydán Provozní řád areálu Úřadu v Brně.

3.1.4. Krizové řízení v rámci Úřadu

V roce 2014 se zástupci Úřadu účastnili jednání se zástupci Ministerstva vnitra, Ministerstva obrany, Generálního ředitelství Hasičského záchranného sboru a s Výborem pro civilní nouzové plánování. Uvedeným subjektům byla poskytována nezbytná součinnost.

Odbor bezpečnostní koordinuje činnost jednotlivých organizačních celků Úřadu při přípravě a realizaci úkolů v rámci mezinárodních cvičení krizových situací. Pokynem ředitele Úřadu byl v roce 2014 zřízen pracovní tým pro koordinaci přípravy a účasti Úřadu na cvičeních orgánů krizového řízení v ČR.

Vydán byl rovněž nový Statut krizového štábu Úřadu.

3.1.5. Ostatní činnosti

Odbor bezpečnostní zajišťuje rovněž evidenční ochranu zaměstnanců Úřadu v případě jejich ohrožení v souvislosti s výkonem povolání. V roce 2014 byla provedena periodická aktualizace seznamu chráněných osob.

V rámci bezpečnostní agendy boje proti korupci byla v roce 2014 vytvořena analýza korupčních rizik, která slouží k aktualizaci Interního protikorupčního programu Úřadu, který byl rovněž vydán v loňském roce.

V rámci zajišťování provozu vozového parku v Úřadu byl v roce 2014 dokončen nákup 5 nových vozidel. Na základě výsledků interního auditu zaměřeného na využívání motorových vozidel Úřadu byl v závěru roku vypracován harmonogram obměny vozového parku pro roky 2015 – 2017. V průběhu roku 2014 byla novelizována směrnice ředitele Úřadu upravující provoz a používání motorových vozidel Úřadu.

3.2. ARCHIV NÁRODNÍHO BEZPEČNOSTNÍHO ÚŘADU

Archiv Národního bezpečnostního úřadu (dále jen „Archiv“) vykonává od roku 2005 činnosti bezpečnostního archivu a od roku 2010 činnosti specializovaného archivu.

Archiv v rámci činnosti bezpečnostního archivu pečuje o archiválie označené stupněm utajení a v rámci činnosti specializovaného archivu o neutajované archiválie. Archiv dohlíží na výkon spisové služby Úřadu a pravidelně provádí výběr archiválií ve skartačním řízení. Archiválie jsou vedeny v základní evidenci Národního archivního dědictví. V roce 2014 bylo provedeno 14 archivních prohlídek. Celkový rozsah archiválií je v bezpečnostním archivu 9,62 běžných metrů a ve specializovaném archivu 10,24 běžných metrů. Ve druhé polovině roku 2014 byla zahájena reevidence všech uložených archiválií v souladu s odborným předpisem vydaným odborem archivní správy a spisové služby Ministerstva vnitra. V roce 2014 nenavštívil bezpečnostní archiv žádný badatel a specializovaný archiv navštívil 1 interní badatel.

V roce 2014 bylo ředitelem Úřadu vydáno rozhodnutí o výstavbě specializovaného a bezpečnostního digitálního archivu.

3.3. EKONOMICKÉ ZABEZPEČENÍ ÚŘADU

Úřad je od 1. listopadu 1998 samostatnou kapitolou státního rozpočtu „308“. V roce 2014 byla jeho činnost financována jednak ze státního rozpočtu a také ze strukturálních fondů EU (dále jen „SF EU“) v rozsahu 10,72 % z celkového čerpání rozpočtu. Všechny projekty, které Úřad tímto způsobem kofinancoval, byly v roce 2014 ukončeny.

Naplňování příjmů státního rozpočtu souvisí se správní činností Úřadu. Daňové příjmy, správní poplatky, byly vybrány ve výši 170 tis. Kč. Nedaňové příjmy byly odvedeny za uložené pokuty ve výši 383,50 tis. Kč, za nahodilé příjmy, jako jsou přeplatky z předcházejících let a drobné příjmy ve výši 377,82 tis. Kč. Dále jsou to příjmy z rozpočtu Evropské unie ve výši 6.654,45 Kč. Celkem Úřad odvedl do státního rozpočtu 7.585,77 tis. Kč.

Konečný rozpočet výdajů činil v roce 2014, po rozpočtových opatřeních, 403.333,78 tis. Kč. Nejdůležitější rozpočtová opatření v kompetenci Ministerstva financí se týkala výdajů NCKB, kdy byl rozpočet navýšen o 29,97 tis. Kč na jeho vybudování v souladu s unesením vlády ČR č. 781 ze dne 19. října 2011, o ustavení Národního bezpečnostního úřadu gestorem problematiky kybernetické bezpečnosti. Projekt byl spolufinancován ze SF EU. Další činnost byla Úřadu nově svěřena v souvislosti s usnesením vlády ČR č. 71 ze dne 30. ledna 2013, k Akčnímu plánu implementace veřejné regulované služby programu Galileo (PRS) v České republice. Obě problematiky jsou řešeny i z důvodu efektivity vynaložených nákladů jako integrované součásti Úřadu se sídlem v Brně.

Rozpočet roku 2014 byl dále posílen o nespotřebované výdaje roku 2013 ve výši 63.881,04 tis. Kč. Důvodem nespotřebování těchto výdajů byl zejména fakt, že bylo vládou odloženo čerpání výdajů ve výši 12.108,47 Kč na plnění úkolů souvisejících s implementací veřejné regulované služby programu Galileo (PRS). Dále byly do rozpočtu roku 2014 převedeny nespotřebované finanční prostředky v objemu 41.408,50 Kč, a to na dobudování NCKB, zejména jeho zařízení speciální technikou. Rozpočet roku 2014 byl čerpán ve výši 336.908,63 tis. Kč. Největší objem běžných výdajů tvořily, jako každým rokem, mzdové výdaje a zákonem dané odvody, které byly vyčerpány na 98 %. Nevyužitá mzdová část z nenaplněných tabulek z Národního centra Public Regulated Services (dále jen „NCPRS“), které není zatím plně funkční, viz výše uvedené usnesení, nebyla uplatněna v nárocích nespotřebovaných výdajů, tj. byla vrácena do státního rozpočtu.

V roce 2014 byl zahájen a též dokončen projekt spolufinancovaný ze SF EU „Realizace technologického centra pro provoz Národního centra kybernetické bezpečnosti“.

Běžné výdaje na provoz, zejména platby v oblasti energií, nezbytných služeb a nákupů k zajištění činnosti Úřadu, NCKB a NCPRS, činily po rozpočtových změnách 89.668,13 tis. Kč (posíleny byly o nespotřebované výdaje roku 2013) a byly čerpány na úrovni 93,68 %.

Kapitálové výdaje byly posíleny o nespotřebované výdaje roku 2013 a konečné čerpání činilo 119.032,03 tis. Kč, z čehož největší objem prostředků, 82.363,63 tis. Kč, byl určen opět na budování NCKB, a to konkrétně v oblasti zabezpečovacích a informačních technologií. Celkem bylo vydáno za pořízení hmotného a nehmotného investičního majetku, včetně služeb 62.545,52 tis. Kč. Kapitálové výdaje ve výši 9.014,90 tis. Kč byly vyčerpány na projekty výzkumu a vývoje.

Výzkum a vývoj byl v plném rozsahu financován z vlastních prostředků kapitoly, tj. bez dotací výzkumu a vývoje státního rozpočtu, v celkové výši 18.472,80 tis. Kč. Vyčerpáno bylo 15.715,51 tis. Kč. Z toho v rámci uzavřených smluvních závazků s externími řešiteli bylo na výzkumné projekty vyčerpáno 9.014,90 tis. Kč a v rámci vlastních výzkumných kapacit bylo vyčerpáno 6.700 tis. Kč.

Celkem činí nároky nespotřebovaných výdajů z rozpočtu roku 2014 částku 68.295,85 tis. Kč. Velký objem převáděných finančních prostředků tvoří dotace,

poukázané ze SF EU, které Úřad obdržel v závěru roku 2014, jako uznatelné náklady, za pořízení Technologického centra NCKB. Tyto finanční prostředky jsou určeny zejména na nákup IT technologií pro NCKB a NCPRS, na nákup speciálních přístrojů a technologií potřebných pro řádné fungování těchto institucí. Dále jsou výdaje určeny na pokrytí smluvních závazků nerealizovaných v roce 2014.

Každoroční tlak Ministerstva financí na snižování rozpočtu, především na činnosti spojené se zákonem, se podařilo od roku 2013 stabilizovat tím, že rozpočet je od tohoto roku vyrovnaný. Rozpočet se navyšuje pouze o financování nově svěřených činností podle výše uvedených usnesení vlády, tj. že bylo vládou pro rok 2014 uvolněno na financování budování NCKB 60.546,20 tis. Kč. Tyto výdaje jsou vykazované a sledované zvlášť, včetně tabulkových počtů, mezd a zákonem daných odvodů, tj. mimo rozpočet na provoz Úřadu, stejně tak výdaje na NCPRS, na které Úřad obdržel na rok 2014 částku 6.298,49 tis. Kč. V obou případech jde o značnou úsporu státních prostředků vzhledem k tomu, že budova, kde sídlí, byla převedena bezúplatně z Ministerstva obrany jako nevyužitá.

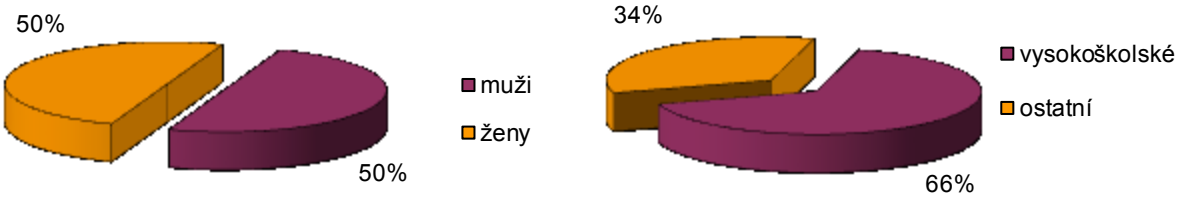
Veškeré finanční prostředky určené na financování činností Úřadu, tj. vyplývajících ze zákona a svěřených na základě výše uvedených usnesení vlády ČR, procházely, v souladu se zákonem o finanční kontrole, předběžnou a průběžnou finanční kontrolou. Následná kontrola byla prováděna jak příkazci operací, tak hlavní účetní a u vybraných finančních operací průřezově i správcem rozpočtu.

3.4. PERSONÁLNÍ ZABEZPEČENÍ ÚŘADU

Pro rok 2014 měl Úřad systemizovaných 310 pracovních míst, z tohoto počtu bylo 29 míst určeno pro NCKB, resp. problematiku kybernetické bezpečnosti, a 6 míst pro NCPRS. V průběhu roku byla všechna pracovní místa v NCKB v Praze i v Brně obsazena novými, převážně mladými odborníky. Dále se rozvíjí spolupráce s vysokými školami a dalšími subjekty působícími v této oblasti. 4 pracovní místa v NCPRS byla koncem roku neobsazena, protože zatím nebyly vládou ČR schváleny příslušné dokumenty a činnosti na pracovišti nemohou být vykonávány v plném rozsahu.

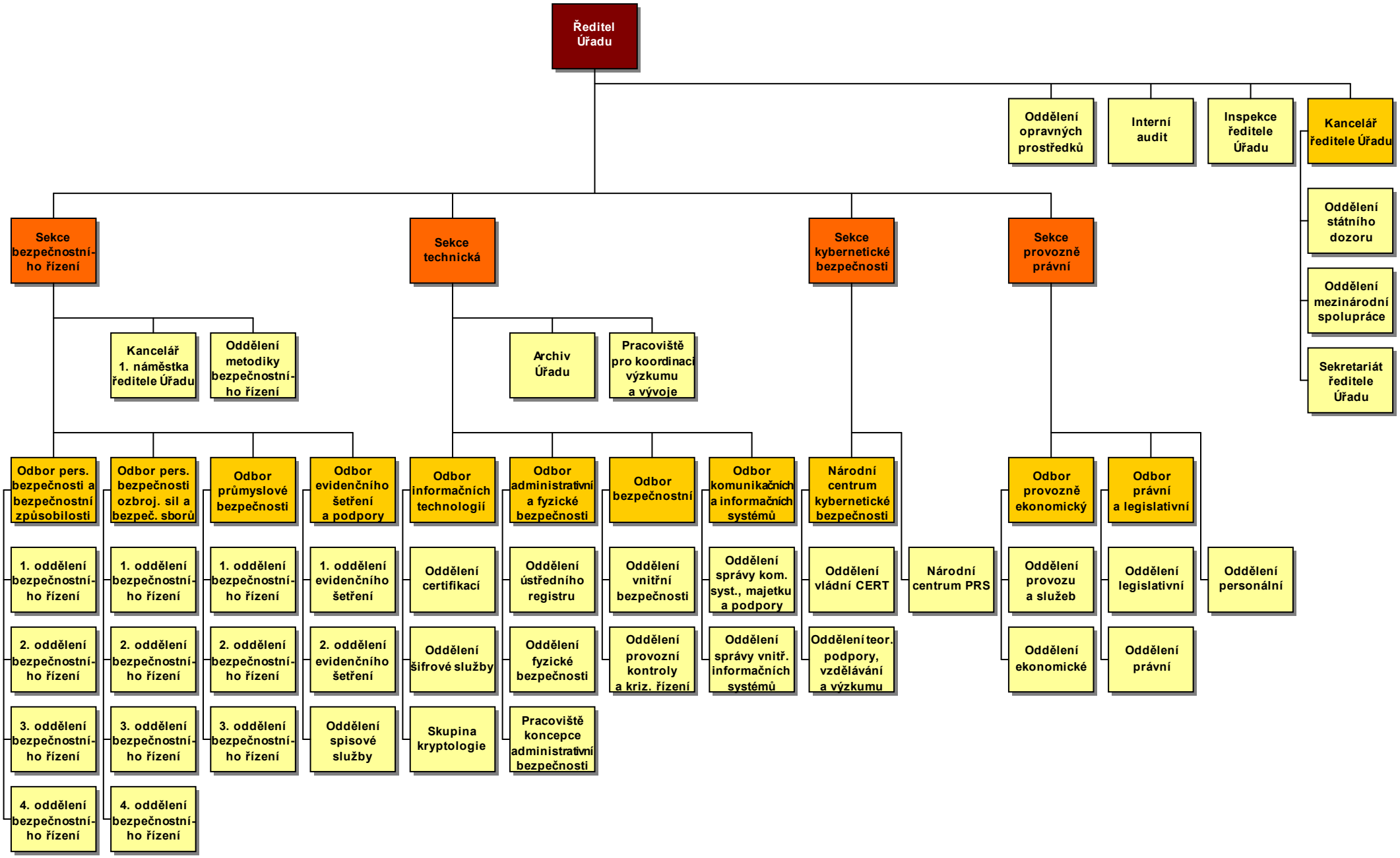
K 31. prosinci 2014 bylo aktuálně obsazeno 304 pracovních míst, z toho bylo 152 mužů a 152 žen. Průměrný věk zaměstnanců byl 47 let, více než 66 % zaměstnanců mělo vysokoškolské vzdělání. Úřad vyvíjí maximální úsilí, aby pracovní místa byla obsazena kvalifikovanými a schopnými zaměstnanci s odpovídající praxí, kteří zároveň splňují požadavky pro přístup k utajovaným informacím.

Struktura zaměstnanců Úřadu – muži/ženy a podle vzdělání



V Úřadu je průběžně realizován systém vzdělávání zaměstnanců. V roce 2014 pokračovalo skupinové i individuální jazykové vzdělávání, kterého se pravidelně účastní více než 70 zaměstnanců. Kromě výuky angličtiny, němčiny a francouzštiny byla zahájena i výuka ruštiny. Dále probíhala odborná školení především v oblasti informačních technologií a kybernetické bezpečnosti, a to v ČR i v zahraničí, pracovníci NCKB se také účastnili odborných konferencí. Pozornost byla věnována zdokonalení komunikačních dovedností zaměstnanců, kteří přicházejí do kontaktu s veřejností. Školení byla účastníky hodnocena velmi kladně, s velkým přínosem pro praxi. Zaměstnanci měli možnost se dále vzdělávat v oblastech, které bezprostředně souvisejí s jejich pracovními činnostmi, tj. především v oblasti právní, ekonomické a technické. Možnost odborného a jazykového vzdělávání zaměstnanců je jedním z motivačních prvků, které Úřad využívá.

Organizační schéma Národního bezpečnostního úřadu v roce 2014



PŘÍLOHA – SEZNAM NĚKTERÝCH ZKRATEK A POJMŮ POUŽITÝCH V TEXTU K OBLASTI KYBERNETICKÉ BEZPEČNOSTI

AFCEA – Armed Forces Communications and Electronics Association

CBMS – Confidence Building Measures

CCDCOE – Cooperative Cyber Defence Centre of Excellence

CECSP – Central European Cyber Security Platform

CERT – Computer Emergency Response Team

CESNET – sdružení založené v roce 1996 českými veřejnými vysokými školami a Akademií věd ČR

CMX – cvičení Crisis Management Exercise

CSIRT – Computer Security Incident Response Team

CSIRT-MU – bezpečnostní tým pro dohled nad sítí Masarykovy univerzity v Brně

CZ.NIC – zájmové sdružení právnických osob založené předními poskytovateli internetových služeb v roce 1998, hlavní činností je provozování registru domén

DDoS/DoS – Distributed Denial of Service / Denial of Service

EC3 – European Cybercrime Centre – Evropské centrum pro boj s kybernetickou kriminalitou

EU – Evropská unie

FENIX – nové označení projektu Bezpečná VLAN

GovCERT.CZ – představuje vládní koordinační místo pro okamžitou reakci na kybernetické bezpečnostní incidenty (vládní CERT – Computer Emergency Response Team), které je organizační složkou Úřadu, respektive jeho specializovaného pracoviště NCKB

ICS ISAC – Industrial Control System Information Sharing and Analysis Center

IDG konference – International Data Group konference

KII – Kritická informační infrastruktura

KYBERKRIMINALITA – specifický druh kriminality páchané prostřednictvím výpočetních a komunikačních technologií

MALWARE – počítačový program určený ke vniknutí nebo poškození počítačového systému

NATO – Severoatlantická aliance (North Atlantic Treaty Organization)

NCKB – Národní centrum kybernetické bezpečnosti

OBSE – Organizace pro bezpečnost a spolupráci v Evropě

PHISHING – podvodná technika k získávání citlivých údajů od uživatelů na internetu

RIA – Hodnocení dopadu regulace (Regulatory Impact Assessment)

SCADA systémy – Supervisory Control And Data Acquisition

SIEM – Security Information and Event Management

SPEAR-PHISHING – podvodná technika k získávání citlivých údajů se zaměřením na určitou organizaci

TABLE-TOP – je cvičení navrženo k testování teoretických schopností cvičících reagovat ve skupině na určitou krizovou situaci. Velkou výhodu tohoto druhu cvičení představuje možnost vyzkoušet si jakoukoliv hypotetickou situaci bez rizika způsobení škody či jiných důsledků

TF-CSIRT – Task Force Computer Security Incident Response Team

TURLA – pojmenování jednoho druhu malwaru

VIS – Významný informační systém

VLAN – virtual LAN

OBSAH

1. ÚVOD 3

2. ČINNOST ÚŘADU 3

2.1. LEGISLATIVNÍ A PRÁVNÍ ČINNOST ÚŘADU 3

2.1.1. Vnější legislativní činnost 3

2.1.2. Vnitřní legislativní činnost 5

2.1.3. Vyjádření k oznámení podle § 69 odst. 1 písm. r) zákona 5

2.1.4. Právní činnost 6

2.2. MEZINÁRODNÍ SPOLUPRÁCE ÚŘADU 7

2.2.1. Mezinárodní smlouvy 7

2.2.1.1. Hodnocení sjednávání smluv o ochraně utajovaných informací za rok 2014 7

2.2.1.2. Výhled na rok 2015 9

2.2.2. Aktivity v rámci NATO a EU a spolupráce s bezpečnostními úřady partnerských států 9

2.2.3. Mezinárodní aktivity v oblasti kybernetické bezpečnosti 10

2.3. PERSONÁLNÍ BEZPEČNOST 12

2.3.1. Bezpečnostní řízení o žádostech fyzických osob 13

2.3.2. Prověřování splňování podmínek po vydání osvědčení 14

2.3.3. Analýza důvodů nevydání nebo zrušení platnosti osvědčení fyzické osoby 14

2.3.4. Přehled ostatních důvodů zániku platnosti osvědčení fyzické osoby 15

2.3.5. Statistické přehledy 16

2.3.6. Personální projekt 18

2.4. BEZPEČNOSTNÍ ZPŮSOBILOST 19

2.4.1. Statistické přehledy 21

2.5. PRŮMYSLOVÁ BEZPEČNOST 21

2.5.1. Bezpečnostní řízení o žádostech podnikatelů 22

2.5.2. Prověřování splňování podmínek po vydání osvědčení podnikatele 23

2.5.3. Analýza důvodů nevydání nebo zrušení platnosti osvědčení podnikatele 23
2.5.4. Přehled ostatních důvodů zániku platnosti osvědčení podnikatele 23
2.5.5. Statistické přehledy 24
2.6. BEZPEČNOST INFORMAČNÍCH A KOMUNIKAČNÍCH SYSTÉMŮ A KRYPTOGRAFICKÁ OCHRANA 25
2.6.1. Certifikační a akreditační činnost 26
2.6.1.1. Certifikace a akreditace informačních systémů 26
2.6.1.2. Certifikace kryptografických prostředků 29
2.6.1.3. Certifikace kryptografických pracovišť 31
2.6.1.4. Certifikace stínicích komor 32
2.6.2. Další odborná činnost 32
2.6.2.1. Výroba kryptografického materiálu 32
2.6.2.2. Měření kompromitujícího vyzařování (TEMPEST) 33
2.6.2.2.1. TEMPEST měření elektronických zařízení 33
2.6.2.2.2. Zónové měření, instalační záznamy, obranné prohlídky 33
2.6.2.2.3. Přehled provedených měření 34
2.6.2.3. Schvalování projektů bezpečnosti komunikačních systémů 34
2.6.2.4. Školení pracovníků kryptografické ochrany a zkoušky odborné způsobilosti 35
2.6.3. Problémové oblasti bezpečnosti informačních a komunikačních systémů a kryptografické ochrany 35
2.7. ADMINISTRATIVNÍ A FYZICKÁ BEZPEČNOST, ÚSTŘEDNÍ REGISTR 36
2.7.1. Administrativní bezpečnost 36
2.7.2. Fyzická bezpečnost 36
2.7.2.1. Certifikace technických prostředků 37
2.7.2.2. Posuzování bezpečnostní dokumentace podnikatele z hlediska fyzické bezpečnosti 39
2.7.2.3. Problémové oblasti fyzické bezpečnosti 40
2.7.3. Ústřední registr 40
2.8. KYBERNETICKÁ BEZPEČNOST 42
2.8.1. Budování NCKB/GovCERT.CZ 42
2.8.2. Vývoj legislativy v oblasti kybernetické bezpečnosti 43

2.8.3. Tvorba kybernetické bezpečnostní politiky ČR 44

2.8.3.1. Národní strategie kybernetické bezpečnosti ČR a Akční plán kybernetické bezpečnosti ČR 44

2.8.4. Informační systémy důležité pro stát a komunikace se subjekty, které provozují KII a VIS 45

2.8.5. Spolupráce Úřadu v oblasti kybernetické bezpečnosti 46

2.8.6. Zvyšování povědomí a osvěta 47

2.8.6.1. Vzdělávací a osvětové kampaně a konference 48

2.8.6.2. Ostatní přednášky a konference 48

2.9. OPRAVNÉ PROSTŘEDKY 49

2.9.1. Bezpečnostní řízení 49

2.9.1.1. Statistické přehledy 49

2.9.1.1.1. Rozklady 49

2.9.1.1.2. Žaloby správní 50

2.9.1.1.3. Kasační stížnosti 50

2.9.1.1.4. Ústavní stížnosti 50

2.9.1.2. Hodnocení rozhodovací praxe Úřadu 50

2.9.2. Správní řízení o pokutě 51

2.9.3. Řízení podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím 51

2.10. VÝZKUMNÁ A VÝVOJOVÁ ČINNOST ÚŘADU 51

2.10.1. Cíle a organizace výzkumu a vývoje 51

2.10.2. Projekty realizované v roce 2014 51

2.11. STÁTNÍ DOZOR 52

2.11.1. Kontroly provedené v roce 2014 52

2.11.2. Výsledky kontrol 55

2.12. METODICKÁ ČINNOST ÚŘADU 58

2.12.1. Metodická činnost v oblasti bezpečnostního řízení 58

2.13. VĚSTNÍK ÚŘADU A INTERNETOVÉ STRÁNKY ÚŘADU 59

2.13.1. Věstník Úřadu 59

2.13.2. Internetové stránky Úřadu 60

2.14. POSKYTOVÁNÍ INFORMACÍ PODLE ZÁKONA Č. 106/1999 SB., O SVOBODNÉM PŘÍSTUPU K INFORMACÍM 61

2.15. INSPEKCE ŘEDITELE ÚŘADU 61

3. BEZPEČNOSTNÍ, EKONOMICKÉ A PERSONÁLNÍ ZABEZPEČENÍ ÚŘADU 61

3.1. OCHRANA UTAJOVANÝCH INFORMACÍ A KRIZOVÉ ŘÍZENÍ V ÚŘADU 61

3.1.1. Vnitřní kontrola ochrany utajovaných informací 61

3.1.2. Personální bezpečnost v rámci Úřadu 62

3.1.3. Fyzická bezpečnost v rámci Úřadu 63

3.1.4. Krizové řízení v rámci Úřadu 63

3.1.5. Ostatní činnosti 63

3.2. ARCHIV NÁRODNÍHO BEZPEČNOSTNÍHO ÚŘADU 64

3.3. EKONOMICKÉ ZABEZPEČENÍ ÚŘADU 64

3.4. PERSONÁLNÍ ZABEZPEČENÍ ÚŘADU 66

PŘÍLOHA – SEZNAM NĚKTERÝCH ZKRATEK A POJMŮ POUŽITÝCH V TEXTU K OBLASTI KYBERNETICKÉ BEZPEČNOSTI 69