Z P R Á V A

O ČINNOSTI

NÁRODNÍHO BEZPEČNOSTNÍHO ÚŘADU

ZA ROK 2013

Praha 2014

1. ÚVOD

Činnost Národního bezpečnostního úřadu (dále jen „Úřad“) byla, v souladu s jeho působností a úkoly stanovenými zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů (dále jen „zákon“), v roce 2013, obdobně jako v předcházejících letech, 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 a konkrétní činnosti v této oblasti (spolupráce se zainteresovanými subjekty v ČR i v zahraničí, účast na seminářích a přednáškách, průzkum stavu zabezpečení národní informační infrastruktury, poskytování informací veřejnosti atp.).

2. ČINNOST ÚŘADU

2.1. LEGISLATIVNÍ A PRÁVNÍ ČINNOST ÚŘADU

2.1.1. Vnější legislativní činnost

Zákon byl v roce 2013 jednou novelizován, a to zákonem č. 303/2013 Sb., kterým se mění některé zákony v souvislosti s přijetím rekodifikace soukromého práva. Uvedená novela změnila s účinností od 1. ledna 2014 ve svém článku LXX zákon v souvislosti se změnou pojetí problematiky způsobilosti k právním úkonům v soukromém právu hmotném a zavedla tak slovní spojení „svéprávnost“ do oblasti zákona.

Úřad, který je gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast, a to na základě usnesení vlády ČR č. 781 ze dne 19. října 2011, zpracoval v roce 2013 návrh zákona o kybernetické bezpečnosti. Na vytvoření návrhu spolupracovala odborná mezirezortní pracovní skupina složená ze zástupců Ministerstva vnitra, Ministerstva obrany, zástupců Českého telekomunikačního úřadu a zástupců zpravodajských služeb. Při tvorbě návrhu zákona o kybernetické bezpečnosti byly rovněž využity aktuální poznatky z praxe (včetně využití poznatků odborné veřejnosti) a současně teoretické analýzy učiněné akademickou sférou. Vypracovaný návrh zákona o kybernetické bezpečnosti předložil Úřad počátkem roku 2013 odborné veřejnosti. Po vyhodnocení připomínek odborné veřejnosti byl zákon o kybernetické bezpečnosti rozeslán do mezirezortního připomínkového řízení, které proběhlo v termínu od 15. dubna do 15. května 2013. Po vypořádání připomínek byl návrh zákona o kybernetické bezpečnosti předložen, v souladu s termínem stanoveným zmiňovaným usnesením vlády, k projednání vládě ČR, a to dne 28. června 2013. Následně byl dne 8. srpna 2013 návrh zákona o kybernetické bezpečnosti projednán Legislativní radou vlády, která s ohledem na velké množství připomínek formulačního a legislativně technického charakteru vyzvala Úřad k přepracování návrhu. Přepracovaný návrh zákona o kybernetické bezpečnosti zaslal Úřad vládě ČR dne 9. prosince 2013 a ta jej svým usnesením č. 2 ze dne 2. ledna 2014 schválila.

V souvislosti s rekodifikací soukromého práva hmotného došlo k novelizaci vyhlášky č. 363/2011 Sb., o personální bezpečnosti a o bezpečnostní způsobilosti. Vyhláška č. 415/2013 Sb., kterou se mění vyhláška č. 363/2011 Sb., o personální bezpečnosti a o bezpečnostní způsobilosti, nabyla účinnosti dnem 1. ledna 2014.

Ze stejného důvodu byla rovněž novelizována vyhláška č. 405/2011 Sb., o průmyslové bezpečnosti. Vyhláška č. 416/2013 Sb., kterou se mění vyhláška č. 405/2011 Sb., o průmyslové bezpečnosti, nabyla účinnosti dnem 1. ledna 2014.

Při přezkumu účinnosti regulace stanovené vyhláškou č. 432/2011 Sb., o zajištění kryptografické ochrany utajovaných informací, byla zjištěna nutnost novelizace této vyhlášky. Vyhláška č. 417/2013 Sb., kterou se mění vyhláška č. 432/2011 Sb., o zajištění kryptografické ochrany utajovaných informací, nabyla účinnosti dnem 1. ledna 2014.

Úřad se dále 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.

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

2.1.2. Vnitřní legislativní činnost

V průběhu roku 2013 bylo vydáno celkem 44 nových interních aktů řízení ředitele Úřadu. Konkrétně se jednalo o 14 směrnic a 30 pokynů ředitele Úřadu, které

byly vydány z důvodu změn v právním řádu a s ohledem na snahu o zefektivnění činnosti Úřadu. K významnému nárůstu počtu interních aktů řízení oproti předcházejícímu období došlo z důvodu změn při zadávání veřejných zakázek.

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

Od 1. ledna 2012 Úřad zabezpečuje novu agendu podle § 138 odst. 1 písm. l) zákona, a to vydávání vyjádření k oznámení podle § 69 odst. 1 písm. r) zákona. Tato činnost spočívá v posuzování oznámení, z hlediska ochrany utajovaných informací, učiněných zadavateli, ve kterých 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 stanovili kvalifikační předpoklad osvědčení podnikatele. V roce 2013 Úřad posoudil celkem 79 podaných oznámení, jejichž přehledy pravidelně zasílá Úřadu pro ochranu hospodářské soutěže.

2.1.4. Právní činnost

V roce 2013 bylo pro porušení povinností stanovených zákonem ukončeno 20 správních řízení, z toho ve 14 případech s fyzickými osobami a v 6 případech s právnickými osobami. Ve 3 případech bylo správní řízení zastaveno a ve 22 případech byla uložena sankce (peněžitá pokuta). Ve 12 dalších případech dosud nebylo správní řízení ukončeno. Celková výše uložených pokut dosáhla částky 68.000 Kč. V 10 případech nebyla řízení prozatím zahájena, neboť jsou Úřadem činěny patřičné kroky v rámci přípravného řízení.

V 38 dalších případech byla věc odložena nebo správní řízení nebylo zahájeno (ve 27 případech u fyzických osob, v 11 případech u právnických osob). Ve 40 případech byla věc z důvodu nepříslušnosti postoupena k projednání příslušnému služebnímu funkcionáři.

Správní řízení v roce 2013

	Fyzická osoba	Právnická osoba	Celkem
Ukončená správní řízení	14	6	**20**
Počet uložených sankcí	16	6	**22**
Zastavená správní řízení	2	1	**3**
Dosud neukončená správní řízení	8	4	**12**

V souvislosti s novou úpravou zadávání veřejných zakázek provedenou směrnicí ředitele Úřadu č. 5/2013, o zadávání veřejných zakázek v Národním bezpečnostním úřadu, ve znění směrnice č. 12/2013, převzal odbor právní a legislativní nově působnost v oblasti zadávání veřejných zakázek. V gesci odboru právního a legislativního je tak od 1. prosince 2013 mimo jiné 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. Tyto úkoly plní nově zřízená skupina veřejných zakázek.

V oblasti právní činnosti bylo v roce 2013 dále uzavřeno cca 80 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 dvěma 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 2013

V roce 2013 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 2013 pokračovalo expertní jednání o smlouvě.

- **Bezpečnostní smlouva mezi vládou České republiky a vládou Lucemburského velkovévodství o vzájemné výměně a ochraně utajovaných informací**

  Smlouva vstoupila v platnost 1. srpna 2013.

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

  Smlouva vstoupila v platnost 1. září 2013.

- **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 zahájit expertní jednání.

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

  V roce 2013 pokračovalo expertní jednání o smlouvě.

- **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.

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

  V roce 2013 pokračovalo expertní jednání o smlouvě.

- **Smlouva mezi vládou České republiky a vládou Brazilské federativní republiky o vzájemné ochraně utajovaných informací**

  Brazilská strana ztratila zájem smlouvu sjednat.

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

  Australská strana ztratila zájem smlouvu sjednat.

- **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 Republikou Kosovo o výměně a vzájemné ochraně utajovaných informací**

  Expertní jednání bylo ukončeno, smlouva bude zaslána do mezirezortního připomínkového řízení.

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

  Expertní jednání probíhají.

2.2.1.2. Výhled na rok 2014

V roce 2014 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 vyplývající z členství ČR v NATO a EU

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

Orgány NATO

NATO
Bezpečnostní výbor na nejvyšší úrovni (Security Committee in Principals Level Format)
Pracovní skupina 1 pro bezpečnost informačních systémů (Working Group 1 on Information Assurance (WG1 IA)-AC/35(WG/1) – od roku 1998)
Information Assurance and Cyber Defence Panel (IACD CaP/4-AC/322(CP/4))
Pracovní skupina panelu CP/4 pro problematiku kybernetické bezpečnosti (Cyber Defence Capability Team)
Pracovní skupina panelu CP/4 pro kryptografické služby (Crypto Capability Team)
Archivní výbor NATO (NATO Archives Committee)
Bezpečnostní výbor ve formátu odborníků na bezpečnostní politiku (Security Committee in Security Policy Format)

NATO
Pracovní skupina IICWG pro vývoj a standardizaci univerzálního komunikačního protokolu pro přenos utajovaných informací v heterogenním komunikačním prostředí (SCIP)

Orgány EU

EU
Council Security Committee – Bezpečnostní výbor Rady EU
Commission Security Policy Advisory Group (CSPAG) – Poradní orgán Komise pro bezpečnostní politiku
European External Action Service Security Committee – Bezpečnostní výbor Evropské služby vnější akce
Council Security Committee Information Assurance (CSC(IA)) – Bezpečnostní výbor Rady EU pro informační bezpečnost
sTESTA Accreditation Board – Akreditační výbor informačního systému sTESTA
Global Navigation Satelite Systems Security Board – Bezpečnostní otázky satelitních navigačních systémů
GALILEO Security Accreditation Board – Bezpečnostní otázky systému GALILEO
Working Group for Public Regulated Services (WG – PRS) – Pracovní skupina pro otázky šifrované navigační služby systému GALILEO
European Space Agency – Security Committee (ESA SB) – Bezpečnostní výbor Evropské kosmické agentury
European Space Agency (ESA) – INFOSEC Panel – pracovní skupina pro přípravu bezpečnostních směrnic ESA pro oblast informačních a komunikačních systémů
BdL Network Security Accreditation Panel – Akreditační orgán sítě Bureau de Liaison
Security Accreditation Board (SAB) – Akreditační výbor pro součinnostní informační systémy Rady EU
Pracovní skupiny Implementation Tempest Task Force (ITTF) a Technical Tempest Task Force (TTTF) – Pracovní skupiny pro oblasti problematiky TEMPEST

Orgány NATO:

- **Bezpečnostní výbor na nejvyšší úrovni** byl zřízen Severoatlantickou Radou (NAC) jako její poradní orgán. Je složen ze zástupců členských zemí a odpovídá Severoatlantické Radě za prověřování otázek týkajících se bezpečnostní politiky NATO a za přípravu příslušných doporučení. Z titulu funkce se jeho jednání účastní ředitelé příslušných bezpečnostních úřadů členských států. Schází se dvakrát ročně.

- **Pracovní skupina 1 pro bezpečnost informačních systémů** působí v rámci NATO Office of Security a poskytuje podporu Security Committee (SC) v oblasti Information Assurance a koordinaci schvalovacích procesů pro dokumenty z oblasti Information Assurance vytvářené SC a NC3B. Skupina je odpovědná za vyhodnocování hrozeb a zranitelností informačních systémů, revidování a vytváření bezpečnostních politik a vytváření směrnic, nařízení a příruček v oblastech managementu Information Assurance, ohodnocování

a řízení bezpečnosti rizik, bezpečnostního schvalování a akreditací, bezpečnostních inspekcí a dalších aspektů oblasti Information Assurance.

- **Information Assurance and Cyber Defence Panel** působí v rámci NATO Consultation, Command and Control Board (NC3B). Je zřízen NC3B ke stanovování ochrany informací NATO při jejich ukládání, zpracování nebo přenosu v komunikačních, informačních a jiných elektronických systémech. Panel také spolupracuje s Vojenským výborem NATO a SC v záležitostech provozních nebo bezpečnostních politik informačních a komunikačních systémů používaných v NATO.

- **Pracovní skupina panelu CP/4 pro problematiku kybernetické bezpečnosti** se zabývá tvorbou směrnic pro zajištění kybernetické bezpečnosti komunikačních a informačních systémů (KIS) nakládajících s utajovanými informacemi – stanovením minimálních bezpečnostních požadavků KIS v rámci agentur NATO, členských zemí NATO a ostatních partnerů (např. Partnership for Peace (PfP), Combined Joint Task Forces (CJTF), EU, veřejné sítě).

- **Pracovní skupina panelu CP/4 pro kryptografické služby** je zřízena v rámci Information Assurance and Cyber Defence Panel. Jedná se o pracovní skupinu připravující dokumenty z oblasti implementace kryptografických prostředků a kryptografické ochrany utajovaných informací zpracovávaných v komunikačních a informačních systémech NATO a standardy pro zadávání, hodnocení a schvalování kryptografických prostředků pro NATO a členské státy NATO. V této pracovní skupině vznikají návrhy direktiv a prováděcích dokumentů pro projektování a aplikaci kryptografických prostředků, klíčových materiálů a nekryptografických funkcí PKI. Úřad se podílí na jejich tvorbě a využívá výsledky při certifikaci kryptografických prostředků a kryptografických pracovišť, při tvorbě prováděcích předpisů pro jejich provozování a při jejich kontrolách.

- **Archivní výbor NATO** spoluvytváří koncepci odtajňování historicky důležitých dokumentů NATO a jejich zpřístupňování veřejnosti. Výbor dále rozvíjí a zdokonaluje archivní politiku, řídí archivy vytvořené vojenskými a civilními složkami NATO a spolupodílí se na tvorbě příslušných interních předpisů NATO.

- **Bezpečnostní výbor ve formátu odborníků na bezpečnostní politiku** je odpovědný za přípravu, revidování a vytváření bezpečnostních politik NATO. Výbor doporučuje směrnice, nařízení a příručky prováděcích předpisů NATO v jednotlivých oblastech bezpečnosti.

- **Pracovní skupina IICWG** zastřešuje aktivity, které směřují ke standardizaci komunikačního protokolu pro bezpečný přenos utajovaných informací SCIP (Secure Communication Interoperability Protocol) v heterogenním komunikačním prostředí pro potřeby NATO, ale i národní. V rámci IICWG působí řada dílčích pracovních skupin podle odborného zaměření. Jejich činnosti a výsledky jsou monitorovány s důrazem na získávání informací pro

rozhodování o vlastnostech a podmínkách potenciální aplikace protokolu nebo používání zařízení s implementovaným protokolem.

Orgány EU:

- **Bezpečnostní výbor Rady EU** je orgánem, jehož hlavní úlohou je rozhodování o otázkách spadajících do oblasti společné bezpečnostní politiky a navrhování stanovisek Evropské radě, a to z vlastní iniciativy či na její žádost. Bezpečnostní výbor Rady EU má i další funkce – koordinuje a sleduje diskuse různých pracovních skupin o společné bezpečnostní politice a získává informace o výsledcích jejich činnosti.

- **Poradní orgán Komise pro bezpečnostní politiku** je orgánem, jehož hlavní úlohou je poskytovat Komisi poradní stanoviska ve věcech bezpečnostní politiky.

- **Bezpečnostní výbor Evropské služby vnější akce** je orgánem, který řeší komplexně otázky bezpečnosti v rámci této služby, včetně ochrany utajovaných informací.

- **Council Security Committee Information Assurance** je orgánem Rady EU odpovědným za schvalování a prosazování bezpečnostních politik, směrnic a nařízení v oblasti informačních a komunikačních systémů nakládajících s utajovanými informacemi EU. Organizuje i inspekční činnost v členských státech.

- **sTESTA Accreditation Board** je orgánem Evropské komise odpovědným za schvalování bezpečnostních politik, směrnic a nařízení pro informační systém sTESTA, který je určen k přenosu utajovaných informací Evropské komise.

- **Global Navigation Satelite Systems Security Board a GALILEO Security Accreditation Board** jsou výbory pro bezpečnostní otázky projektu globálních navigačních satelitních systémů a projektu GALILEO. Výbory řeší bezpečnostní problematiku výstavby a provozu systému GALILEO, jeho vazby na další satelitní navigační systémy (např. EGNOS, GPS), uvolňování citlivých a utajovaných informací, technologií a know-how členským i nečlenským zemím EU, otázku akreditace pracovišť pro provoz systému, kryptografickou ochranu pro službu Public Regulated Services (PRS), která je určena pro bezpečnostní složky členských států.

- **Working Group for Public Regulated Services** řeší bezpečnostní problematiku výstavby a provozu služby Public Regulated Services (PRS) systému GALILEO, která je určena pro bezpečnostní složky členských států. Připravuje dokumenty pro akreditace pracovišť pro provoz systému, kryptografickou ochranu atd.

- **European Space Agency – Security Committee** je výbor, který je odpovědný za vývoj a schvalování bezpečnostních politik, směrnic a pravidel pro zajištění bezpečnosti informací v systémech Evropské kosmické agentury.

- **European Space Agency – INFOSEC Panel** je pracovní skupina pro přípravu bezpečnostních směrnic a pravidel ESA pro oblast informačních a komunikačních systémů a ochranu utajovaných informací v nich zpracovávaných, vytvářených, přenášených a ukládaných.

- **BdL Net Security Accreditation Panel** je akreditačním orgánem sítě Bureau de Liaison, ustanoveným nově v roce 2006 pro bezpečnostní akreditaci této součinnostní sítě protiteroristických policejních útvarů zemí EU.

- **Security Accreditation Board (SAB)** je orgánem Rady EU pro bezpečnostní akreditaci součinnostních informačních systémů EU s přípojnými body v členských zemích EU, provozovaných Generálním sekretariátem Rady (GSC).

- **Pracovní skupiny Implementation Tempest Task Force (ITTF) a Technical Tempest Task Force (TTTF) jsou** pracovní skupiny EU, které mají za úkol připravit nové technické standardy v oblasti kompromitujícího elektromagnetického vyzařování. Zastoupení členské země EU v těchto skupinách je podmíněno dostatečnou úrovní odborných znalostí a schopností.

Dalším mezinárodním fórem, jehož činnosti se Úřad aktivně účastní, je Mezinárodní pracovní skupina pro průmyslovou bezpečnost MISWG (Multinational Industrial Security Working Group). Cílem této pracovní skupiny, která aktivně spolupracuje s NATO a EU, je přiblížení národních standardů v otázkách průmyslové bezpečnosti.

2.2.3. Spolupráce s bezpečnostními úřady partnerských států

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) a jižního Kavkazu (Ázerbájdžán, Gruzie). Úřad se všemi uvedenými státy sjednal nebo v současnosti sjednává smlouvy o výměně a vzájemné ochraně utajovaných informací.

V roce 2013 uspořádal Úřad workshopy v oblasti bezpečnostního řízení, opravných prostředků, bezpečnosti informačních systémů, TEMPEST a kybernetické bezpečnosti pro zástupce národních bezpečnostních úřadů Bosny a Hercegoviny, Makedonie, Kosova a Chorvatska. Dále v Úřadu proběhly semináře a školení pro zástupce národních bezpečnostních úřadů a dalších institucí z Polska, Norska, Finska, Dánska, Maďarska a Slovinska, specializované na oblast měření kompromitujícího vyzařování. Zástupce skupiny TEMPEST byl pozván na návštěvu CESG ve Spojeném království a SHAPE NATO (měřící laboratoř a pak v rámci konference NIAS 2013), aby prezentoval výsledky výzkumu a vývoje zajišťovaného

Úřadem v oblasti TEMPEST. Dále se zástupci skupiny TEMPEST aktivně podíleli na obsahu a průběhu odborného semináře pro desítku zemí v rámci programu TAIEX EU.

2.2.4. Mezinárodní aktivity Úřadu v oblasti kybernetické bezpečnosti

Úřad dále, vzhledem k působnosti nově získané v roce 2011, spolupracuje se zahraničními partnery v oblasti kybernetické bezpečnosti, a to jak formou výměny informací v rámci jednotlivých národních středisek CERT, tak formou komunikace s odborníky na tuto problematiku, účastí na konferencích a workshopech týkajících se tématu kybernetické bezpečnosti. V minulém roce byla navázána spolupráce s příslušnými orgány majícími ve své kompetenci kybernetickou bezpečnost v Rakousku, Spojených státech amerických, Švédsku, Izraeli a Francii.

Úřad také spoluzaložil Středoevropskou platformu kybernetické bezpečnosti, která sdružuje vládní, národní a vojenské CERT států Visegrádské 4 a Rakouska. Cílem platformy, která byla ustavena v květnu 2013 Praze, je posílit spolupráci v oblasti kybernetické bezpečnosti, sdílet informace, koordinovat vědu a výzkum, koordinovat společné postoje na mezinárodních fórech a organizovat společná cvičení kybernetické bezpečnosti.

V roce 2013 Úřad zahájil přistupování k NATO Cooperative Cyber Defence Centre of Excellence, jehož cílem je zvyšovat obranné schopnosti svých členů a NATO v oblasti kybernetické bezpečnosti. Zapojení ČR schválila vláda dne 4. prosince 2013 usnesením č. 926, o zapojení České republiky do NATO Cooperative Cyber Defence Centre of Excellence v Tallinnu. Oficiální přistoupení k centru se očekává v únoru 2014, nicméně pracovník Úřadu bude vyslán do centra k 1. lednu 2014.

V minulém roce Úřad v různých pracovních orgánech Evropské unie aktivně participoval na projednávání Směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii.

Pokud jde o aktivity v rámci Evropské unie, je nutno rovněž zmínit, že Úřad získal zastoupení ve vedení Evropské agentury pro bezpečnost sítí a informací (ENISA).

Pracovníci Úřadu se v listopadu 2013 zúčastnili cvičení NATO Cyber Coalition 2013, které mělo za cíl otestovat připravenost států NATO na několik současně probíhajících hrozeb v oblasti kybernetické bezpečnosti.

2.3. PERSONÁLNÍ BEZPEČNOST

V oblasti personální bezpečnosti Úřad prováděl bezpečnostní řízení o žádostech fyzických osob, vydával osvědčení fyzické osoby a osvědčení fyzické osoby pro cizí moc, potvrzující cizí moci vydání osvědčení fyzické osoby, vydával rozhodnutí o nevydání osvědčení fyzické osoby, dále prověřoval, zda fyzické osoby,

které již jsou držiteli osvědčení fyzické osoby, i nadále splňují podmínky pro jeho vydání, vydával rozhodnutí o zrušení platnosti osvědčení fyzické osoby a realizoval řadu dalších úkonů s tím spojených, např. zakládání, vedení, doplňování, evidenci a vyřazování bezpečnostních svazků, vedení evidence fyzických osob, které jsou držiteli osvědčení fyzické osoby atd.

Z hlediska legislativního rámce v oblasti personální bezpečnosti byl rok 2013 charakterizován především implementací zákona č. 89/2012 Sb., občanský zákoník, do zákona a prováděcího právního předpisu, a to 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 2013 na velmi dobré úrovni. V souladu s usnesením vlády České republiky č. 1381 ze dne 12. prosince 2007 byla vzájemná spolupráce dále upravována. V průběhu roku byla uzavřena jedna realizační dohoda a jeden dodatek k již dříve uzavřené dohodě. Jednalo se o Dohodu o informační spolupráci s Generálním ředitelstvím cel ze dne 19. dubna 2013, která nahradila Dohodu o informační spolupráci s Generálním ředitelstvím cel ze dne 10. července 2008, a Dodatek č. 1 k Dohodě o postupu při poskytování informací mezi Národním bezpečnostním úřadem a Ministerstvem obrany, Inspekcí ministra obrany, Vojenskou policií a Ředitelstvím personální podpory ze dne 28. března 2013.

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 154 osobám a na základě jejich žádostí prováděl šetření k 35 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 2013 bylo Úřadem přijato 5.091 žádostí o vydání osvědčení fyzické osoby. Oproti předchozímu roku tak došlo ke zvýšení tohoto počtu o 1.713 žádostí. Největší podíl tvořily žádosti o vydání osvědčení fyzické osoby pro stupeň utajení Tajné (63 %), nejméně pak bylo žádostí pro nejvyšší stupeň utajení Přísně tajné (5 %). Obdobně jako v předchozích letech byl největší počet žádostí přijat v posledním čtvrtletí hodnoceného roku, a to 1.729, což činí jednu třetinu z celkového počtu přijatých žádostí. O většině těchto žádostí tak bude rozhodnuto až v roce 2014.

Celkem bylo v loňském roce rozhodnuto ve 4.538 případech o vydání osvědčení fyzické osoby a v 19 případech o nevydání osvědčení. Ve 186 případech pak bylo bezpečnostní řízení zastaveno. Nejčastějším důvodem zastavení bezpečnostního řízení bylo zpětvzetí žádosti účastníkem řízení (65 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 (56 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

Také v roce 2013 zahrnovalo významný objem činnosti Úřadu v oblasti personální bezpečnosti provádění prověřování, zda fyzická osoba, která je držitelem osvědčení fyzické osoby, i nadále splňuje podmínky pro jeho vydání. Prověřeno takto bylo celkem 2.643 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 234 případech toto prověřování vyústilo v zahájení řízení o zrušení platnosti osvědčení fyzické osoby, které bylo v 67 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 v 19 případech nebylo žadateli osvědčení vydáno a v 67 případech bylo rozhodnuto o zrušení platnosti osvědčení.

Převládajícím důvodem pro nevydání nebo zrušení platnosti osvědčení fyzické osoby bylo, jako v roce 2012, 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 2013 měly tyto důvody opětovně příčinnou souvislost se skutečnostmi vyplývajícími z trestního či přestupkového řízení, dále souvisely s porušováním právních předpisů (v rozhodovací praxi Úřadu nejčastěji v oblasti daňových předpisů) a interních normativních aktů (zejména u osob ve služebním poměru). Převážnou motivací zde bylo získání majetkového či jiného prospěchu. Nejčetnější shledání uvedeného bezpečnostního rizika bylo v případech neodpovědného až laxního přístupu účastníků řízení (žadatelů či držitelů osvědčení) k jejich závazkovým vztahům, díky němuž se ocitli v neudržitelné finanční, potažmo majetkové situaci, čímž se stali osobami významně ovlivnitelnými, což mohlo mít až

fatální dopad na jejich schopnost, resp. ochotu utajovat informace. Tyto případy většinou doprovázela rovněž neochota účastníků řízení takové finanční problémy Úřadu vůbec uvést, respektive je objasnit. V některých případech souviselo shledání tohoto bezpečnostního rizika s nadměrným zneužíváním návykových látek, především v konzumaci alkoholických nápojů.

Ostatní rizika uvedená v § 14 odst. 2 a 3 zákona byla konstatována v roce 2013 pouze u jednotlivých případů, nicméně byl zaznamenán nárůst obligatorního bezpečnostního rizika – závažná nebo opakovaná činnost proti zájmům ČR, a to v souvislosti s takovou činností účastníků řízení v procesu zadávání veřejných zakázek. Bezpečnostní riziko, rovněž obligatorní povahy – činnost spočívající v potlačování základních práv a svobod, anebo podpora takové činnosti, nebylo tak četné jako v minulosti, avšak i v roce 2013 se vyskytly případy, kdy Úřad toto shledal u osob spjatých s minulým režimem, které nejen vědomě s tímto režimem spolupracovaly, ale i svým konáním způsobily újmu osobám, které byly vůči tomuto režimu v opozici. V tomto ohledu je nutno zmínit i případ shledání tohoto bezpečnostního rizika u osoby, která nejen mírou svých sympatií ke scéně pravicového extremismu v ČR, ale i projevy násilí, podporovala činnost v potlačování základních práv a svobod.

Dalším významným důvodem nevydání či zrušení platnosti osvědčení fyzické osoby bylo nesplnění podmínky bezúhonnosti podle § 6 odst. 2 písm. c) zákona, na jejíž menší četnosti oproti roku 2012 se odrazila amnestie prezidenta republiky.

2.3.4. Přehled ostatních důvodů zániku platnosti osvědčení fyzické osoby

V uplynulém období zanikla platnost celkem 6.265 osvědčení, oproti loňskému roku tak došlo k navýšení tohoto počtu o více než 100%.

Největší část případů představoval zánik platnosti osvědčení doručením nového osvědčení fyzické osoby, a to v celkovém počtu 3.039. 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 (1.111 případů).

Z výše uvedeného je zřejmé, že se pozitivně projevil princip novely zákona, jímž je fyzické osobě umožněn přístup k utajované informaci na základě pouze jednoho osvědčení. Uplatněním tohoto ustanovení v praxi se snížil počet vydaných osvědčení, a tím došlo ke snížení administrativní zátěže Úřadu.

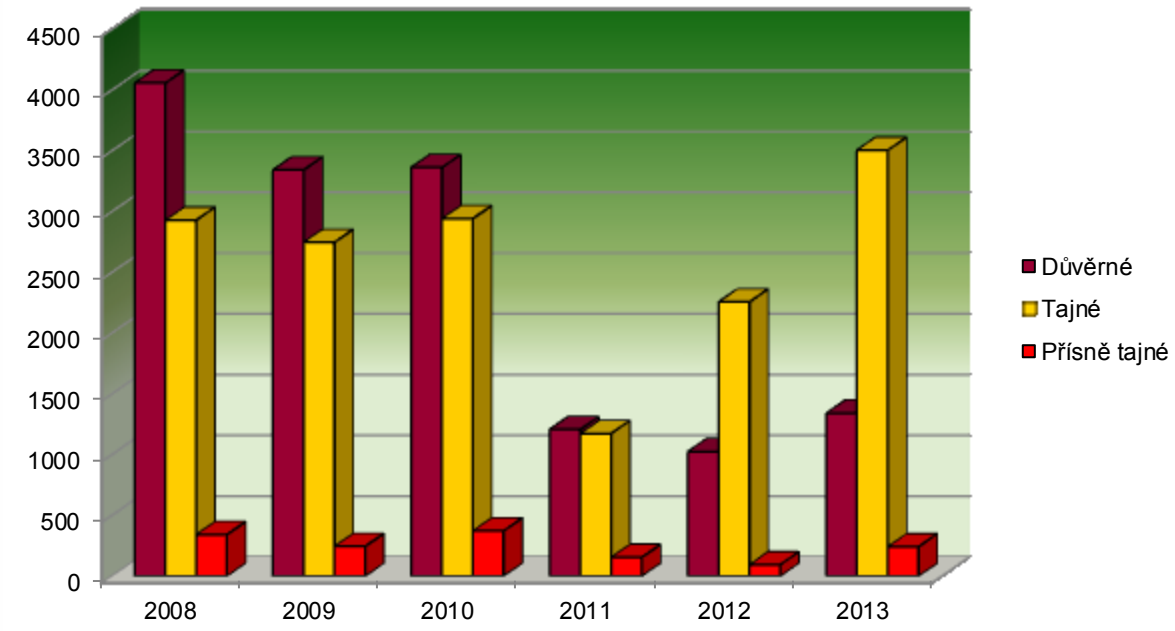
Počet případů zániku platnosti osvědčení fyzické osoby v roce 2013 podle jednotlivých důvodů je přehledně uveden v následující kapitole 2.3.5.

2.3.5. Statistické přehledy

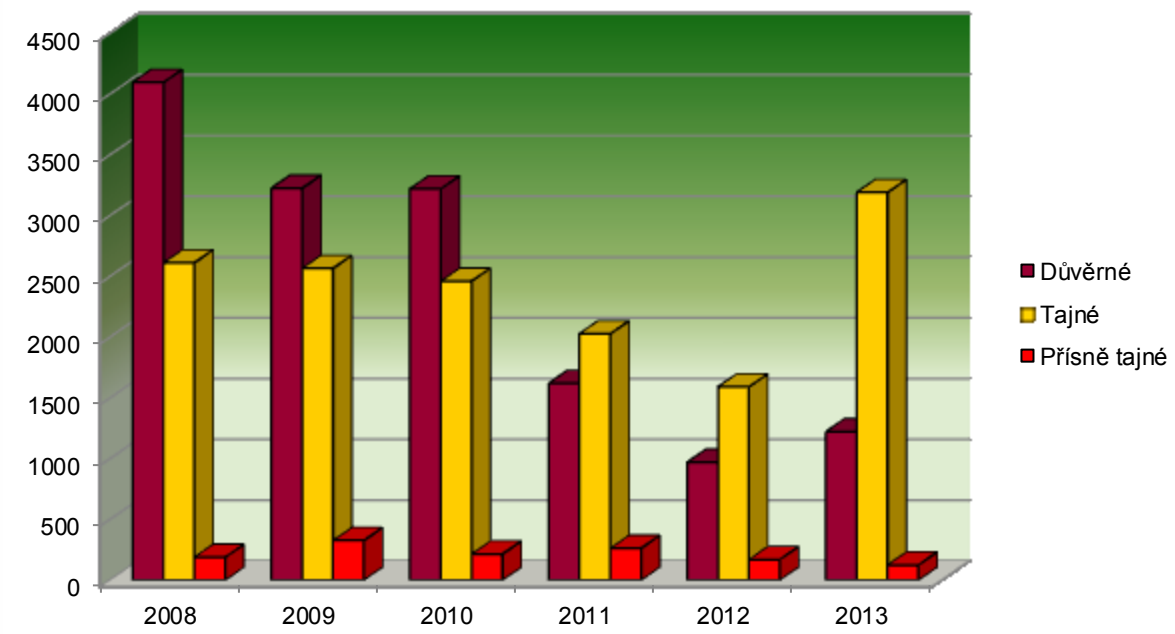
Přijaté žádosti a ukončená bezpečnostní řízení v roce 2013

	Důvěrné	Tajné	Přísně tajné	Celkem
Přijaté žádosti	1.342	3.506	243	**5.091**
Osvědčení vydáno	1.222	3.191	125	**4.538**
Osvědčení nevydáno	6	11	2	**19**
Řízení zastaveno	106	73	7	**186**

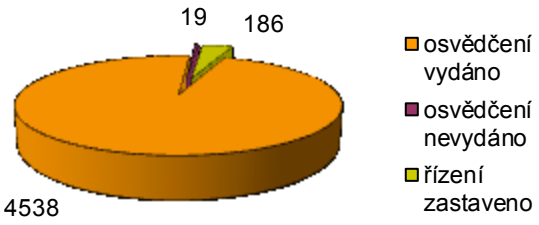
Přijaté žádosti o vydání osvědčení fyzické osoby v letech 2008 až 2013



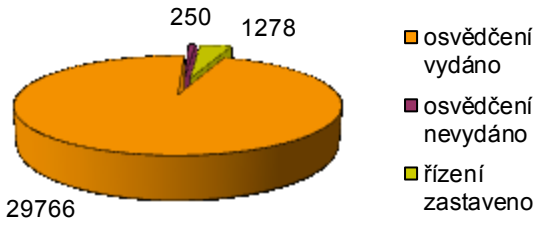
Vydaná osvědčení fyzické osoby v letech 2008 až 2013



Ukončená bezpečnostní řízení v roce 2013



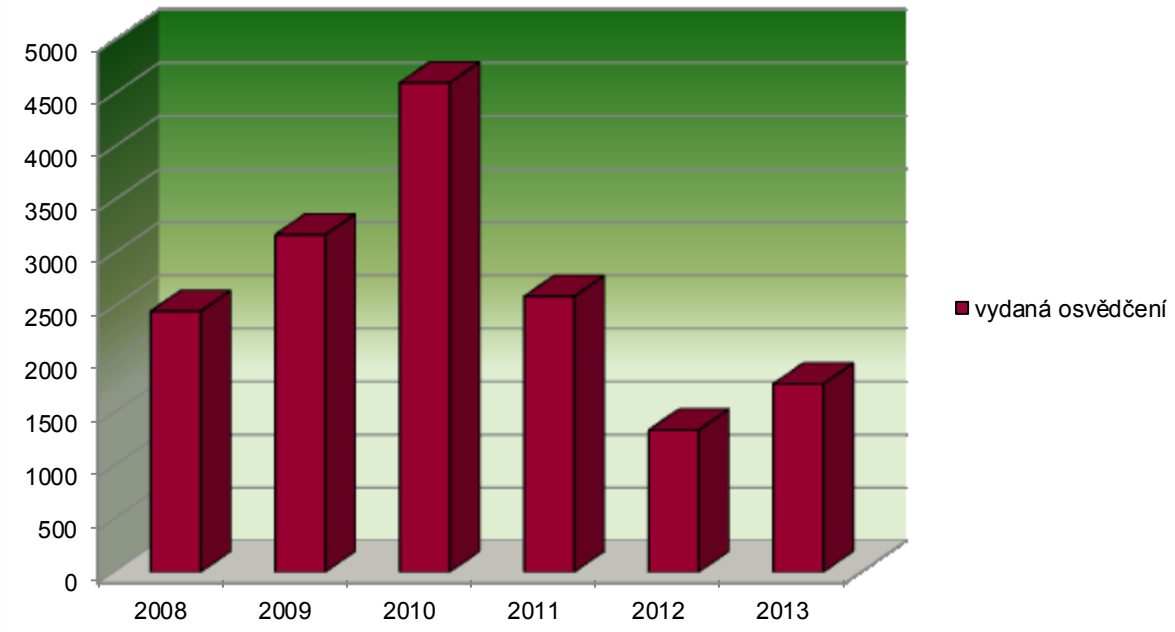
Ukončená bezpečnostní řízení v letech 2008 až 2013



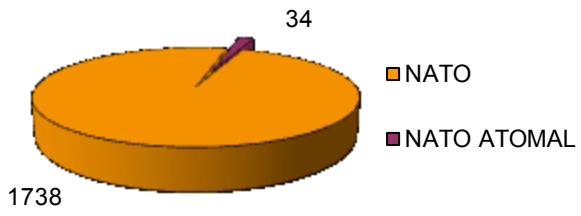
Vydaná osvědčení fyzické osoby pro cizí moc v roce 2013

COSMIC TOP SECRET	171
COSMIC TOP SECRET ATOMAL	29
NATO SECRET	1.440
NATO SECRET ATOMAL	5
NATO CONFIDENTIAL	127
Celkem	**1.772**

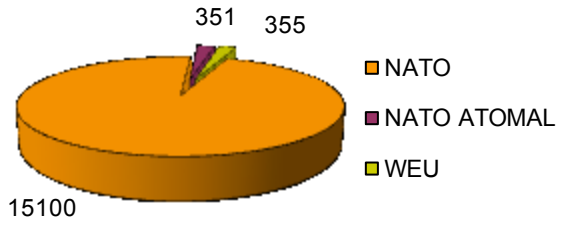
Vydaná osvědčení fyzické osoby pro cizí moc v letech 2008 až 2013



Osvědčení pro cizí moc v roce 2013



Osvědčení pro cizí moc v letech 2008 až 2013[1)]



Zánik platnosti osvědčení fyzické osoby podle důvodu v roce 2013

Uplynutí doby platnosti osvědčení	1.689
Zrušení platnosti osvědčení	67
Úmrtí držitele osvědčení	27
Ohlášení odcizení nebo ztráty osvědčení	80
Poškození osvědčení	37
Změna některého z údajů uvedených v osvědčení	166
Vrácení osvědčení	1.111
Doručení nového osvědčení	3.039
Vznik služebního nebo pracovního poměru u ZS	49
Celkem	**6.265**

Zastavení bezpečnostního řízení v roce 2013

Nedání souhlasu podle § 107 zákona	5
Ve stanovené lhůtě nebyly odstraněny nedostatky v žádosti	24
Uvedení nepravdivé nebo neúplné výpovědi	9
Nesplnění podmínek – dosažení 18 let věku, svéprávnosti, bezúhonnosti	1
Odpadnutí důvodu řízení	1
Oznámení odpovědné osoby, že pominuly skutečnosti, kterými byla žádost odůvodněna	56
Zpětvzetí žádosti	65
Ostatní	25
Celkem	**186**

2.3.6. Personální projekt

V souladu s § 72 zákona předložila ministerstva a další ústřední správní úřady své personální projekty. Usnesením vlády České republiky ze dne 19. června 2012 č. 439 byl schválen Postup při zpracovávání personálních projektů a jejich ověřování Národním bezpečnostním úřadem. V něm bylo uloženo členům vlády a vedoucím

[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.

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 2013 bylo vyjádření Úřadu k personálním projektům předloženo do připomínkového řízení dotčeným ministerstvům a orgánům státní správy. Největší počet žádostí na rok 2014 je plánován rezortem Ministerstva obrany, a to v celkovém počtu 2.999 žádostí. 60 % z tohoto počtu by však měly tvořit žádosti v případě, kdy fyzická osoba potřebuje mít přístup k utajované informaci i bezprostředně po uplynutí doby platnosti dosavadního osvědčení fyzické osoby, tzv. opakované žádosti.

Na základě předložených personálních projektů a vypořádání vznesených připomínek zpracoval Úřad materiál pro jednání vlády, který vláda ČR projednala dne 4. prosince 2013 a vydala usnesení č. 920, 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 2013 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 citlivé činnosti v oblasti zahraničního obchodu s vojenským materiálem a v oblasti nakládání s jaderným materiálem. V tomto roce také byla stanovena nová citlivá činnost. Dne 1. srpna 2013 nabyl účinnosti zákon č. 185/2013 Sb., kterým byl změněn zákon č. 312/2006 Sb., o insolvenčních správcích, který v § 2a nově stanovil za citlivou činnost výkon činnosti insolvenčního správce dlužníka podle § 3 odst. 2.

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

V roce 2013 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.

2.4.1. Statistické přehledy

Přehled přijatých žádostí a ukončených bezpečnostních řízení v roce 2013

Citlivá činnost podle	Přijaté žádosti	Doklad vydán	Doklad nevydán	Řízení zastaveno	Zrušení platnosti dokladu
§ 8 zákona č. 38/1994 Sb.[2)]	55	51	1	2	3
§ 2a zákona č. 18/1997 Sb.[3)]	46	50	1	0	0
§ 5 zákona č. 310/2006 Sb.[4)]	1	1	0	0	0
§ 25c odst. 10 zákona č. 61/1988 Sb.[5)]	2	2	0	2	0
§ 157a zákona č. 137/2006 Sb.[6)]	16	18	0	0	0
§ 2a zákona č. 312/2006 Sb.[7)]	10	2	0	0	0
Ostatní	5	3	0	3	0
Celkem	**135**	**127**	**2**	**7**	**3**

[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. 310/2006 Sb., o nakládání s některými věcmi využitelnými k obranným a bezpečnostním účelům na území České republiky a o změně některých dalších zákonů (zákon o nakládání s bezpečnostním materiálem), ve znění pozdějších předpisů.
[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.

2.5. PRŮMYSLOVÁ BEZPEČNOST

V oblasti průmyslové bezpečnosti Úřad realizoval bezpečnostní řízení o žádostech podnikatelů, vydával osvědčení podnikatele a osvědčení podnikatele pro cizí moc, potvrzující cizí moci vydání osvědčení podnikatele, vydával rozhodnutí o nevydání osvědčení podnikatele, dále prověřoval, zda podnikatelé, kteří již jsou držiteli osvědčení podnikatele, i nadále splňují podmínky pro jeho vydání, vydával rozhodnutí o zrušení platnosti osvědčení podnikatele a realizoval řadu dalších úkonů s tím spojených, např. zakládání, vedení, doplňování, evidenci a vyřazování bezpečnostních svazků, vedení evidence podnikatelů, kteří jsou držiteli osvědčení podnikatele atd.

Ve vztahu k podnikatelům, kteří jsou držiteli osvědčení podnikatele, se činnost Úřadu vyznačovala především prováděním úkonů k prověřování, zda podnikatelé nadále splňují podmínky stanovené zákonem pro vydání osvědčení, a to jak v návaznosti na hlášení změn údajů v žádosti podnikatele oznamovaných jednotlivými držiteli osvědčení podnikatele, tak i na základě skutečností získaných Úřadem z vlastní činnosti nebo informací poskytnutých Úřadu orgány státu, jinými orgány či osobami. Oblast prověřování splňování podmínek se promítala i do oblasti bezpečnostního řízení a rozhodování o zrušení platnosti osvědčení podnikatele.

Z hlediska legislativního rámce v oblasti průmyslové bezpečnosti byl rok 2013 charakterizován především implementací zákona č. 89/2012 Sb., občanský zákoník, a zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích), do zákona a prováděcího právního předpisu pro oblast průmyslové bezpečnosti, kterým je vyhláška č. 405/2011 Sb., o průmyslové bezpečnosti.

Z hlediska organizačního se rok 2013 vyznačoval zejména převedením agendy ověřování a prověřování realizace administrativní bezpečnosti podnikateli do působnosti sekce bezpečnostního řízení. Do organizačních procesů v oblasti průmyslové bezpečnosti se výrazně promítaly i činnosti spojené s přípravami postupů praktických činností k zavedení nových právních předpisů soukromého práva.

Součinnost, kterou Úřadu v rámci bezpečnostního řízení poskytuje Policie ČR, zpravodajské služby a další spolupracující orgány státu a právnické osoby, lze označit jako velmi dobrou a efektivní. Konkrétní úpravy součinnosti a spolupráce se také promítly do nově uzavíraných realizačních dohod a jejich dodatků (viz kap. 2.3.).

2.5.1. Bezpečnostní řízení o žádostech podnikatelů

V průběhu roku 2013 bylo Úřadem přijato 65 žádostí podnikatelů o vydání osvědčení podnikatele. Z tohoto počtu bylo k 31. prosinci 2013 rozhodnuto o 31 žádostech, u zbylých 34 žádostí k tomuto datu bezpečnostní řízení o žádosti podnikatele probíhala.

Ve srovnání s rokem 2012 je patrný nárůst počtu přijatých 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 zrušení 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 České republiky 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

Rok 2013 byl v oblasti průmyslové bezpečnosti nadále charakterizován nárůstem četnosti a rozsahu úkonů při prověřování splňování podmínek u držitelů osvědčení podnikatele.

V této oblasti však lze pozitivně hodnotit dopad změn daných novelou zákona (zákon č. 255/2011 Sb.) a novou vyhláškou o průmyslové bezpečnosti ve vztahu k povinnosti hlášení změn po vydání osvědčení, zejména změny v datu pravidelného ročního hlášení podle § 68 písm. d) zákona. Rok 2013 byl již druhým, kdy byly tyto změny uplatňovány, a lze tak objektivně hodnotit jejich dopady. Přes prvotní potíže s akceptovatelností změn ze strany podnikatelů lze konstatovat, že změny jsou pozitivně přijímány podnikateli a výrazně pozitivně dopadají i do činnosti Úřadu, neboť došlo k rovnoměrnějšímu rozložení jeho zatíženosti i zatíženosti s ním spolupracujících orgánů a organizací.

2.5.3. Analýza důvodů nevydání nebo zrušení platnosti osvědčení podnikatele

V roce 2013 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. Důvody a počty zrušení platnosti osvědčení podnikatele lze charakterizovat následovně:

- nesplnění podmínky ekonomické stability podle § 16 odst. 1 písm. a) zákona – 2 případy,

- nesplnění podmínky bezpečnostní spolehlivosti podle § 16 odst. 1 písm. b) zákona – 3 případy.

2.5.4. Přehled ostatních důvodů zániku platnosti osvědčení podnikatele

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

V roce 2013 mezi důvody zániku platnosti osvědčení podnikatele převažoval zánik osvědčení jeho vrácením držitelem, celkem 48 případů. Druhým nejčastějším důvodem zániku osvědčení pak byl zánik platnosti osvědčení podnikatele z důvodu doručení nového osvědčení podnikatele pro stejnou formu přístupu podnikatele k utajované informaci, celkem 20 případů.

Počet případů zániku platnosti osvědčení podnikatele v roce 2013 podle jednotlivých důvodů je uveden v kapitole 2.5.5.

2.5.5. Statistické přehledy

Přijaté žádosti o vydání osvědčení podnikatele v roce 2013

Důvěrné	Tajné	Přísně tajné	Celkem
37	27	1	**65**

Stav zpracování žádostí o vydání osvědčení podnikatele přijatých v roce 2013

Osvědčení vydáno	Osvědčení nevydáno	Řízení zastaveno	Probíhalo k 31.12.2013	Celkem
23	1	7	34	**65**

Vydaná osvědčení podnikatele v roce 2013

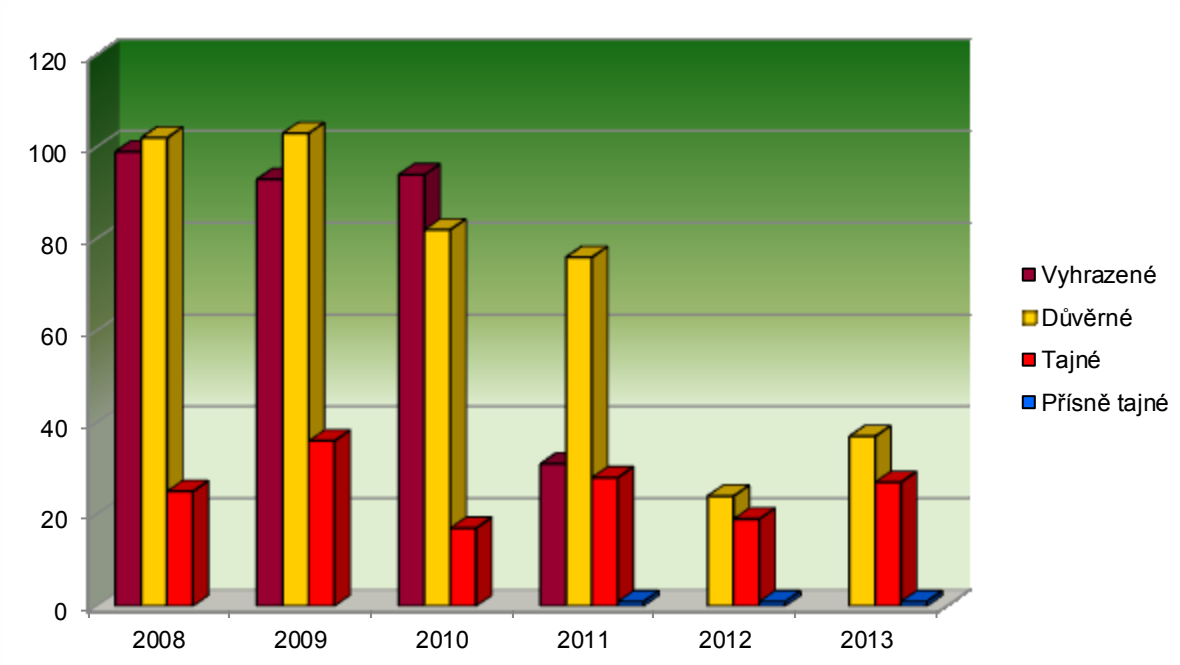
Důvěrné	Tajné	Přísně tajné	Celkem
63	36	1	**100**[8)]

Řízení o zrušení platnosti osvědčení podnikatele v roce 2013

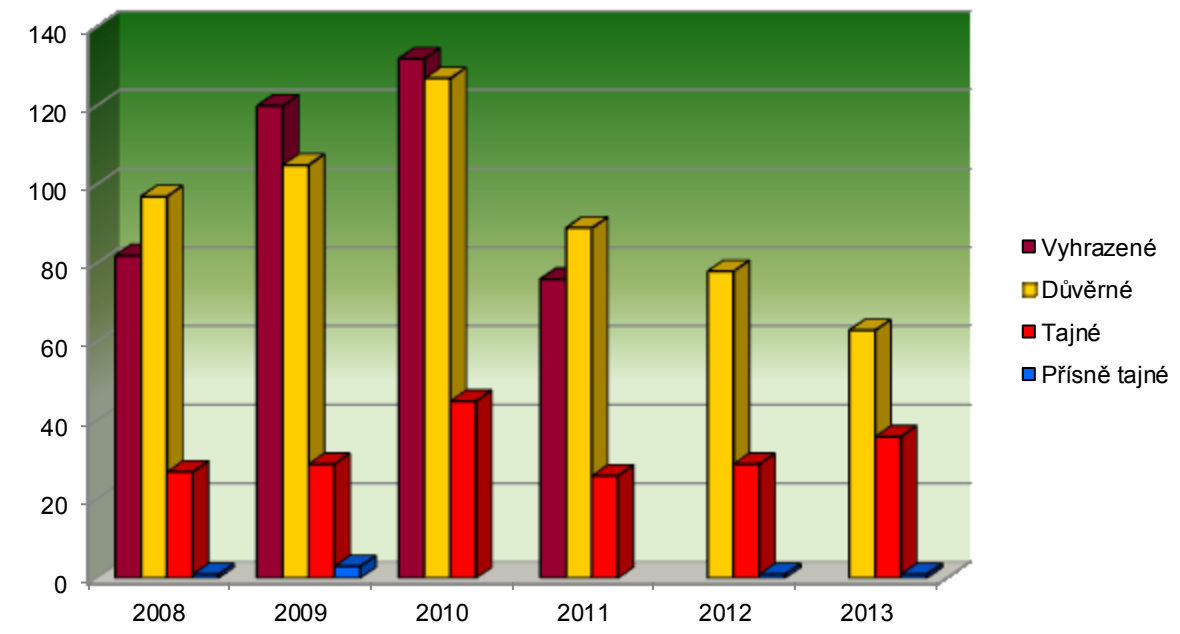
Zahájená řízení	Platnost zrušena	Řízení zastaveno	Probíhalo k 31.12.2013
27	5	7	17

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

Přijaté žádosti o vydání osvědčení podnikatele v letech 2008 až 2013



Vydaná osvědčení podnikatele v letech 2008 až 2013



Zánik platnosti osvědčení podnikatele podle důvodu v roce 2013

Uplynutí doby platnosti osvědčení	4
Zrušení platnosti osvědčení	5
Zrušení podnikatele	2
Ohlášení odcizení nebo ztráty osvědčení	0[9)]
Poškození osvědčení	0[9)]
Změna některého z údajů uvedených v osvědčení	1[9)]
Vrácení osvědčení	48
Doručení nového osvědčení pro stejnou formu přístupu k UI	20
Doručení rozhodnutí o nevydání osvědčení pro stejnou formu přístupu k UI	0
Celkem	**80**

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 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 2013 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 1.0. Bezpečnostní standardy NBÚ jsou poskytovány v souladu s jejich stupněm utajení a s uplatněním zásady „need to know“.

[9)] Počet případů zániku platnosti osvědčení podnikatele, při kterých by nebyl uplatněn postup výměny osvědčení podle § 56 odst. 4 zákona, a došlo by 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.

Dále byla novelizována vyhláška č. 432/2011 Sb., o zajištění kryptografické ochrany utajovaných informací, s cílem řešit některé praktické problémy při výkonu kryptografické ochrany.

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 2013 dalších 114 žádostí, včetně žádostí o opakovanou certifikaci, a to jak ze státní správy, tak ze soukromé sféry. Pouze v 18 případech byla podána žádost o certifikaci nově budovaného informačního systému, z toho pouze 4 žádosti pocházely ze státní správy.

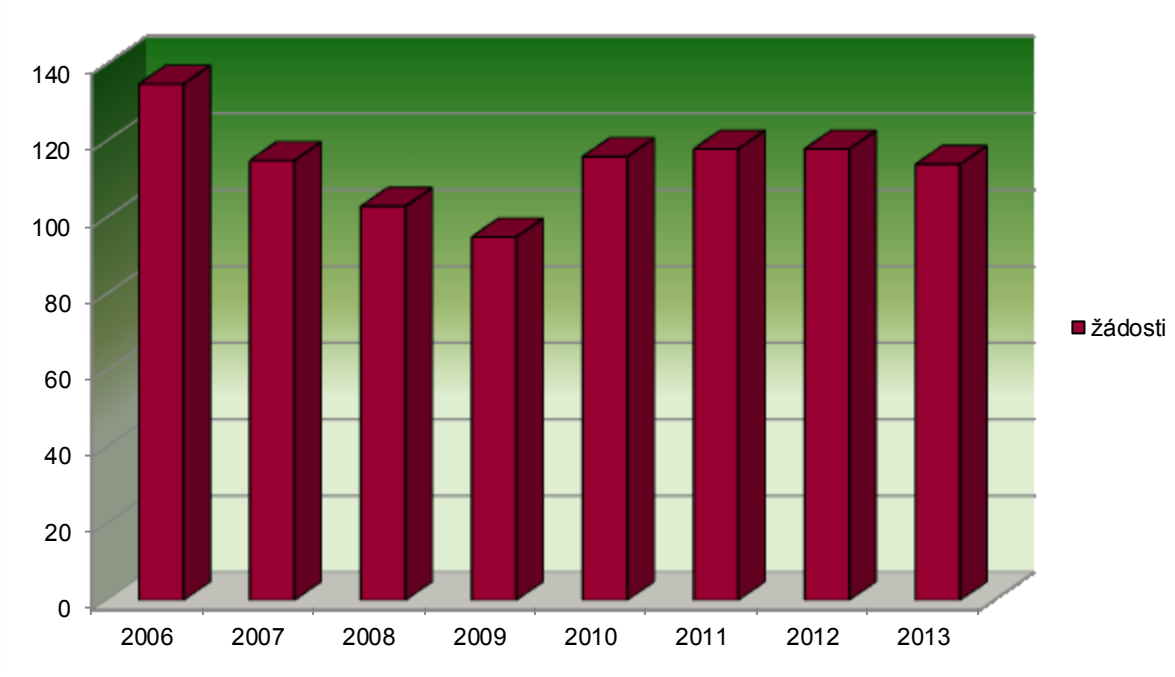
Bylo vydáno 118 certifikátů informačních systémů, z toho 62 pro žadatele ze státní správy nebo samosprávy. Celkem 72 certifikátů bylo vydáno na žádost podanou v roce 2013. Z celkového počtu certifikátů vydaných v roce 2013 se jednalo pouze v 19 případech o první certifikaci informačního systému, z toho bylo 5 certifikátů vydáno pro informační systémy státní správy.

V 11 případech provozovatel informačního systému s certifikátem platným do data spadajícího do roku 2013 nepožádal o opakovanou certifikaci a platnost certifikátu automaticky skončila. Celkem v 7 případech byl v roce 2013 proces certifikace ukončen bez vydání certifikátu, a to vesměs na žádost žadatele o certifikaci, z důvodu nesplnění podmínek pro získání osvědčení podnikatele nebo skončení platnosti osvědčení podnikatele během certifikačního řízení.

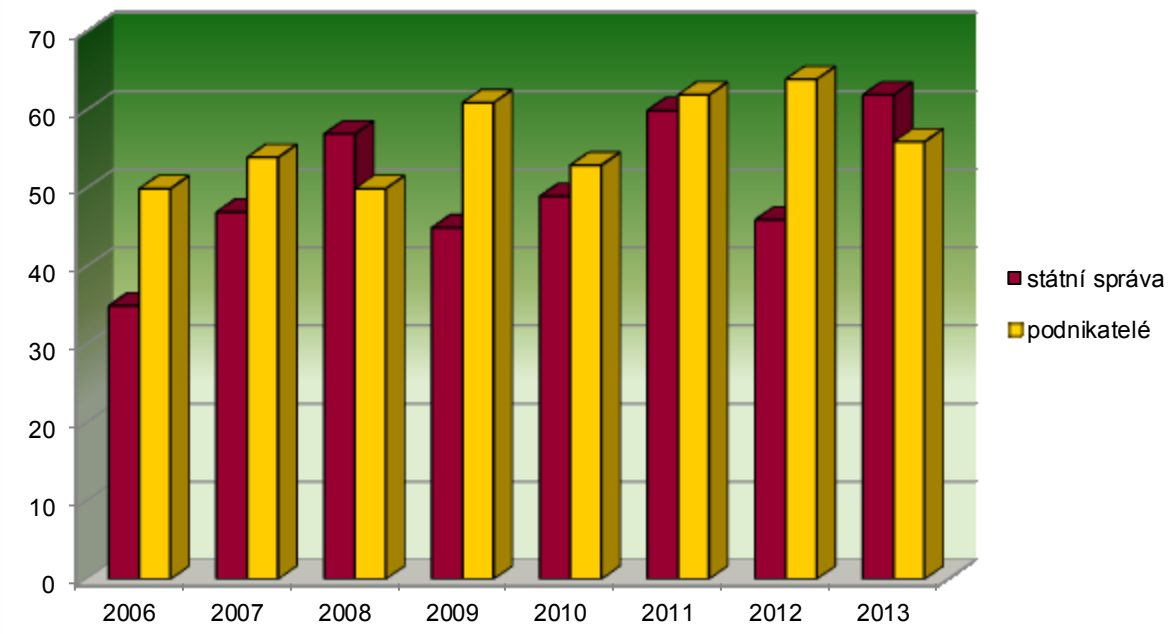
Certifikace informačních systémů v roce 2013

Přijaté žádosti	Ukončeno bez vydání certifikátu nebo uplynutím doby platnosti certifikátu		Vydané certifikáty	
	státní správa	podnikatelé	státní správa	podnikatelé
114	8	10	62	56

Přijaté žádosti o certifikaci informačního systému v letech 2006 až 2013



Vydané certifikáty informačních systémů v letech 2006 až 2013



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 a schváleny Úřadem. Před uplynutím doby platnosti certifikátu pak musí být certifikace pro další období opakována.

Lze konstatovat, že v roce 2013 přibylo pouze 5 žádostí o certifikaci nově budovaného informačního systému ze státní správy a 13 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 způsobem nesnižujícím úroveň jejich zabezpečení. Výkyvy v počtu provedených certifikací souvisejí také s cykly, v nichž se provádí opakovaná certifikace (zpravidla 5 let pro informační systémy určené pro nakládání s utajovanými informacemi stupně utajení Vyhrazené, 3 roky pro stupeň utajení Důvěrné a 2 roky pro stupeň utajení Tajné nebo Přísně tajné). Ke snížení počtu informačních systémů nově budovaných pro zpracování utajovaných informací ve státní správě přispívá pravděpodobně také omezení finančních prostředků, které lze pro tento účel vyčlenit.

V roce 2013, kromě opakované certifikace menších informačních systémů v několika ministerstvech a úřadech (Ministerstvo průmyslu a obchodu, Ministerstvo zdravotnictví, Ministerstvo životního prostředí, Ministerstvo financí, Ministerstvo pro místní rozvoj, Ministerstvo spravedlnosti, Ministerstvo školství, mládeže a tělovýchovy, Úřad vlády, Kancelář Senátu Parlamentu ČR, Generální ředitelství cel, Generální finanční ředitelství, Česká národní banka, několik krajských a městských úřadů), proběhla opakovaná certifikace řady významných a rozsáhlých informačních systémů v Ministerstvu vnitra, 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 2013 Úřad zajistil pro rezort Ministerstva obrany národní akreditaci lokalit jednoho z nejdůležitějších součinnostních systémů NATO a pro Ministerstvo vnitra národní akreditaci systému EUROPOL, což je nutnou podmínkou pro prodloužení jejich stávajícího připojení k příslušným počítačovým sítím. Zároveň byla příslušným orgánům NATO nebo EU pro bezpečnostní akreditaci vydána požadovaná prohlášení o shodě s bezpečnostními požadavky kladenými na tyto systémy. Stálou pozornost vyžaduje i hodnocení a schvalování změn prováděných v uvedených systémech a jejich rozšiřování.

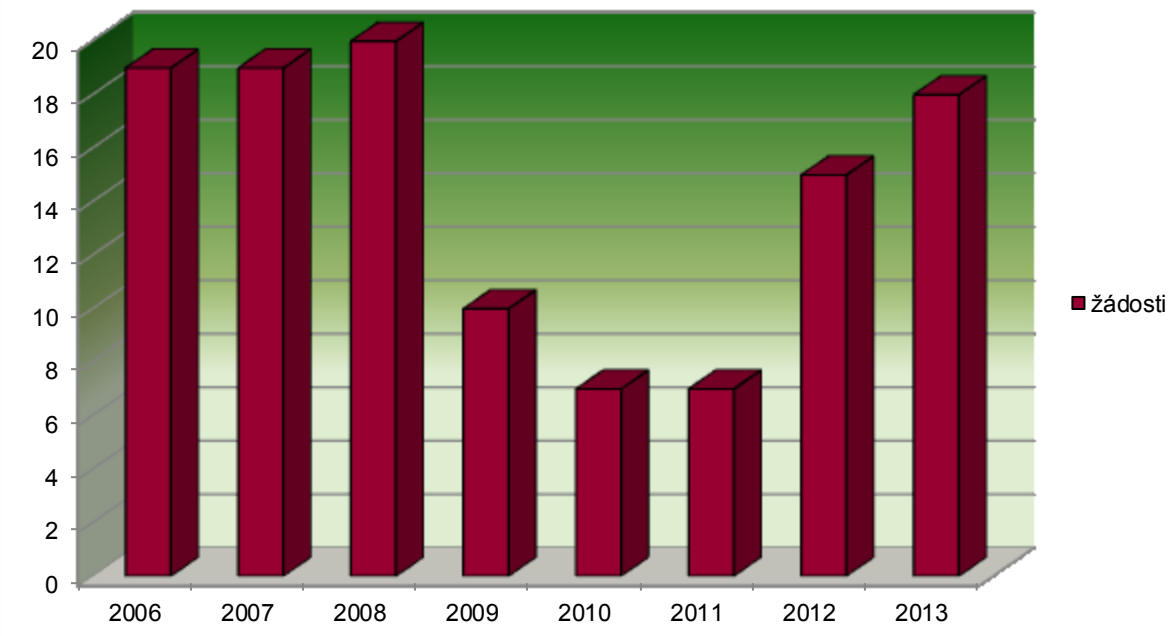
2.6.1.2. Certifikace kryptografických prostředků

V roce 2013 bylo Úřadu podáno celkem 18 žádostí o certifikaci kryptografického prostředku, z toho 5 na nový kryptografický prostředek. V řízeních k certifikaci kryptografického prostředku bylo vydáno celkem 16 certifikátů, 3 řízení byla ukončena 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.

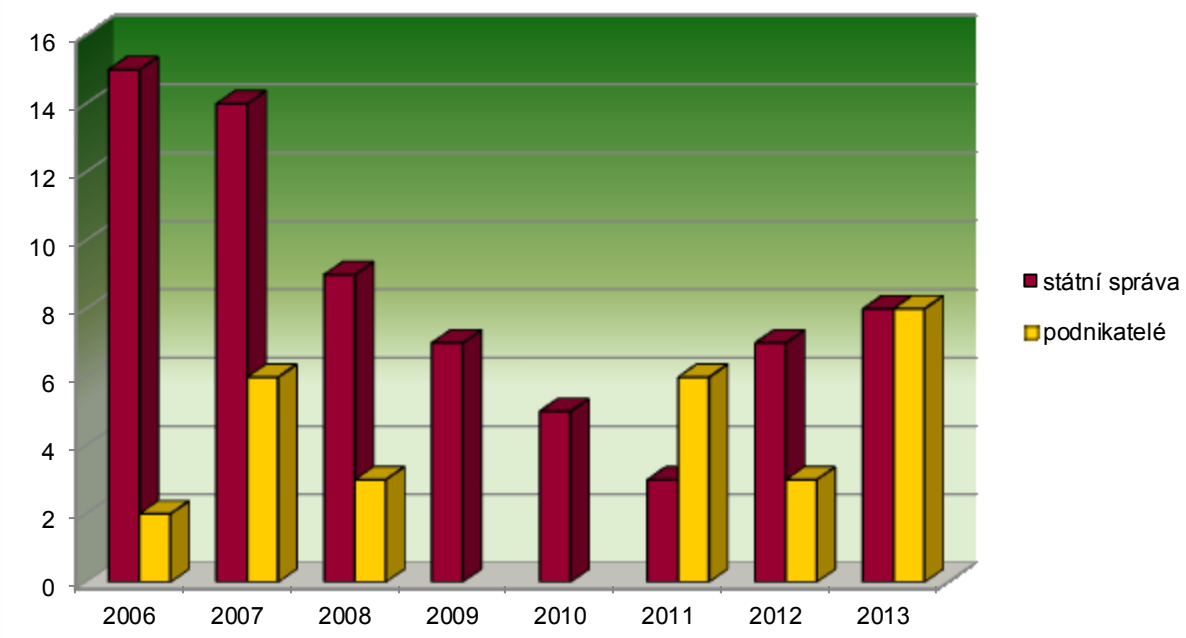
Certifikace kryptografických prostředků v roce 2013

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
18	5	13	3	1	8	8	9	9

Přijaté žádosti o certifikaci kryptografického prostředku v letech 2006 až 2013



Vydané certifikáty kryptografických prostředků v letech 2006 až 2013



Úřad provedl v roce 2013 opakovanou certifikaci kryptografických prostředků TCE 621 verze CZ, SECTRA Tiger verze XS a Office, PCS1, RF1302S, HCryptC, ELCRODAT verze 4-2 a 6-2S. Nově byly certifikovány kryptografické prostředky RF13250S, SECTRA Panthon 3 a prostředky pro potřeby součinnostního spojení. Nebyla prováděna opakovaná certifikace kryptografických prostředků třídy KRYDAT a SINA BOX S, čímž jejich certifikáty zanikly. Zastavena byla certifikace kryptografických prostředků třídy R150.

V návaznosti na nové poznatky k provozu byly upraveny, formou doplňku, certifikační zprávy kryptografických prostředků KRYDEC a HCryptW. Úřad vydal aktualizovaný bezpečnostní standard upravující provoz a správu kryptografických prostředků třídy TCE 621 a prostředků jejich správy TCE 671.

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“ byly zařazeny kryptografické prostředky TCE 621 verze CZ a RF13250S a komponenty kryptografických prostředků PCS1 a SECTRA Panthon 3.

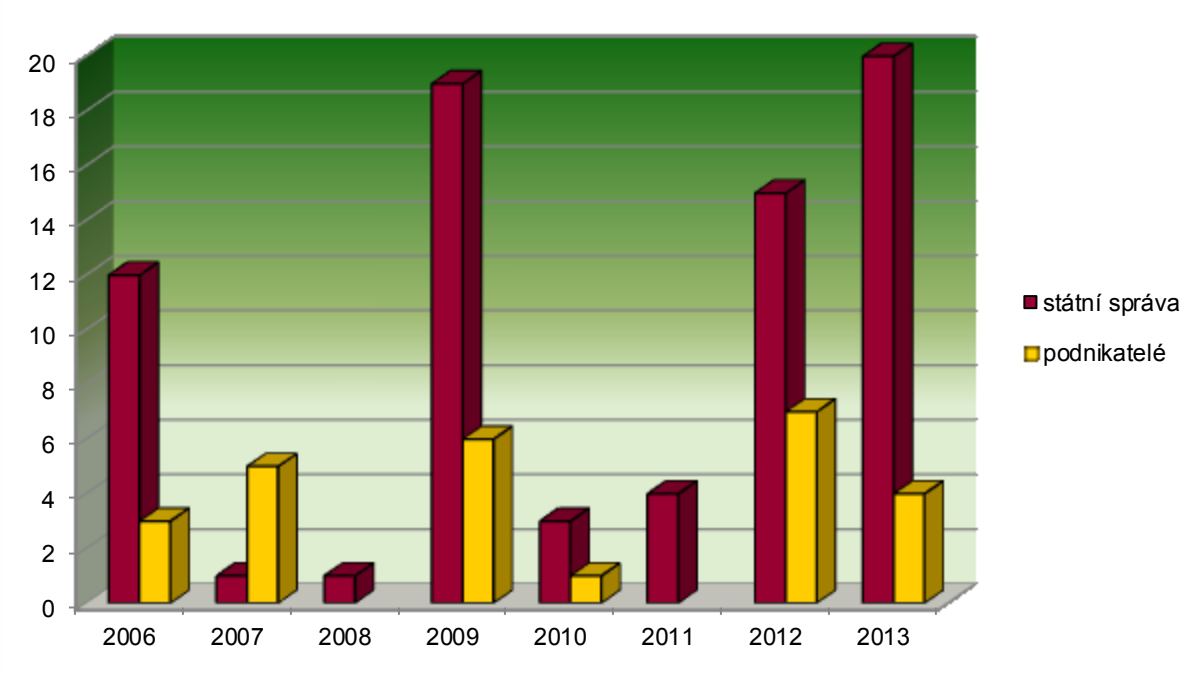
2.6.1.3. Certifikace kryptografických pracovišť

Většina žádostí o certifikaci kryptografických pracovišť spadá do kategorie opakovaných žádostí. Poprvé bylo certifikováno 5 kryptografických pracovišť u 2 nových žadatelů. Jedno certifikační řízení bylo na žádost žadatele zastaveno. Z provedených certifikací vyplynulo, že umístění většiny kryptografických pracovišť a provoz na nich je v souladu s reálnými potřebami příslušných organizací. Stav řízení je shrnut v následující tabulce.

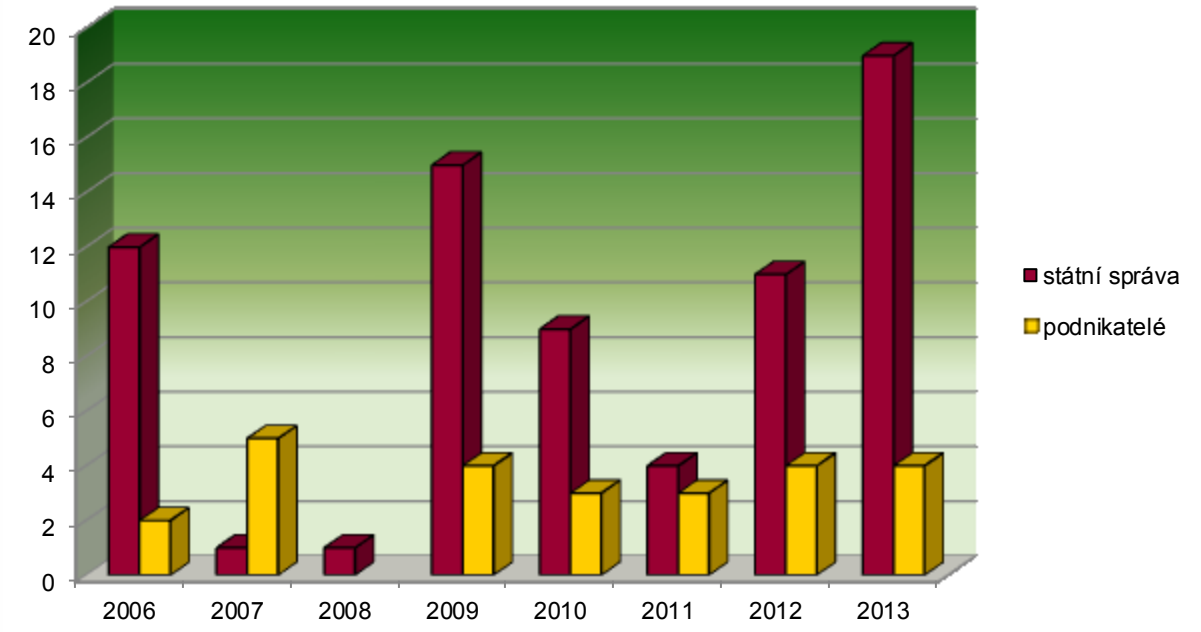
Certifikace kryptografických pracovišť v roce 2013

	Přijaté žádosti	Rozpracováno	Certifikováno	Zamítnuto
Státní správa	20	0	19	0
Podnikatelé	4	0	4	0
Celkem	**24**	**0**	**23**	**0**

Přijaté žádosti o certifikaci kryptografického pracoviště v letech 2006 až 2013



Vydané certifikáty kryptografických pracovišť v letech 2006 až 2013



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 38 certifikátů stínicích komor, přičemž bylo využíváno i podkladů z měření provedených pracovníky Ministerstva zahraničních věcí 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 2013 bylo v Úřadu vygenerováno celkem 70.649 kryptografických klíčů a hesel uložených na 8.010 nosičích různých typů a dalších 177 kusů jiného kryptografického materiálu (procesory, paměti, kryptografická dokumentace, instalační a šifrovací SW).

Úřad vzal do evidence a provedl distribuci celkem 1.625 ks nového kryptografického a CCI materiálu a dále zajistil servis a opravy na území ČR u 13 ks kryptografických prostředků a mimo ČR u 27 ks kryptografických prostředků.

Pro zjednodušení objednávání klíčového materiálu pro kryptografické prostředky třídy TCE byla vytvořena elektronická objednávka. Na základě nově zpracované dokumentace byl pro kryptografické pracoviště Úřadu vydán nový certifikát.

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 2013 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 2013 hodnoceno více než 40 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 dle 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 2013 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 2013, je uveden v následující tabulce.

Měřená zařízení a objekty v roce 2013

Typ měření[10)]	**Počet**
Zónové měření	15 objektů + vojenské kontejnery
Kryptografické prostředky	2 typy
PC sestavy	2 typy – třída 0; přes 40 typů – třída 1 a 2
Audiotechnika	2 typy zařízení
Obrané prohlídky i v rámci certifikace IS	15 objektů
Mobilní systémy	3 systémy

[10)] U zónového měření 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.

2.6.2.3. Schvalování projektů bezpečnosti komunikačních systémů

V roce 2013 nebyla podána žádná žádost o schválení projektu bezpečnosti nového komunikačního systému ani nebyla činnost některého z provozovaných komunikačních systémů ukončena.

Komunikační systém pro výměnu utajovaných informací může být podle zákona provozován pouze na základě Úřadem schváleného projektu bezpečnosti. V roce 2013 byly provozovány 2 rezortní komunikační systémy (Bezpečnostní informační služba, Ministerstvo vnitra) a mezirezortní komunikační systém MODUS.

Projekty bezpečnosti uvedených komunikačních systémů jsou nadále vyhovující a byly schváleny Úřadem, avšak vzhledem k tomu, že platnost schválení je dána také platností certifikátu použitých kryptografických prostředků, může být rezortní komunikační systém Ministerstva vnitra provozován pouze do 31. října 2014.

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 2013 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.

Zastaralý komunikační systém vládního utajovaného spojení založený na použití kryptografických prostředků Sectel 9600 Toro je nahrazen novým systémem vládního utajovaného spojení realizovaného informačním systémem Vega-T (pro nakládání s utajovanými informacemi do stupně utajení Tajné) a informačním systémem Vega-D (pro nakládání s utajovanými informacemi do stupně utajení Důvěrné). Oba informační systémy jsou certifikovány podle zákona a jsou provozovány Ministerstvem vnitra. V roce 2013 pokračovalo připojování dalších lokalit IS 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 2013 organizačně zajistil a provedl, v souladu se zákonem, celkem 19 školení skupin pracovníků kryptografické ochrany a po následující zkoušce odborné způsobilosti vydal 83 osvědčení o zvláštní odborné způsobilosti pracovníka kryptografické ochrany. 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 2013 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 smlouvy 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 2013 bez větších problémů.

- Národní certifikace některých kryptografických prostředků, vyvinutých a certifikovaných v členské zemi NATO nebo EU, i nadále vázne v určitých případech na pomalé reakci NCSA příslušné země na žádost Úřadu o poskytnutí podkladů z jí provedeného hodnocení kryptografického prostředku, které jsou potřebné pro provedení certifikace Úřadem.

- Z hlediska zajištění praktické ochrany utajovaných informací v informačních nebo komunikačních systémech a zajištění kryptografické ochrany všeobecně ve státní správě byl i v roce 2013 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. K tomu se připojuje fluktuace již vyškolených odborníků z důvodu nižšího finančního ohodnocení ve státní správě a rovněž negativní vliv častých organizačních změn v některých rezortech. 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 elektronizace a digitalizace veřejné správy – viz tiskovou zprávu v příloze.

2.7.1. Administrativní bezpečnost

Dne 1. dubna 2013 vzniklo pracoviště koncepce administrativní bezpečnosti. Jeho primárním úkolem je zpracování a zobecnění poznatků získaných při kontrolách administrativní bezpečnosti u orgánů státu, právnických či samostatně podnikajících fyzických osob. Tyto podklady jsou využívány k úpravě 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 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 4 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) zřízené u Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví pro poplachové systémy při zavádění evropských norem a aktualizaci stávajících norem pro tuto oblast,

- metodickou pomoc v rámci certifikace technických prostředků, v souvislosti s instalací technických prostředků a s návrhy opatření fyzické bezpečnosti na vyžádání u podnikatelů nebo orgánů státu (např. Metrostav a.s., Retia, a.s., AERO Vodochody a.s., Ministerstvo školství, mládeže a tělovýchovy, Ministerstvo spravedlnosti, Poslanecká sněmovna Parlamentu ČR, Kancelář prezidenta republiky aj.),

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

2.7.2.1. Certifikace technických prostředků

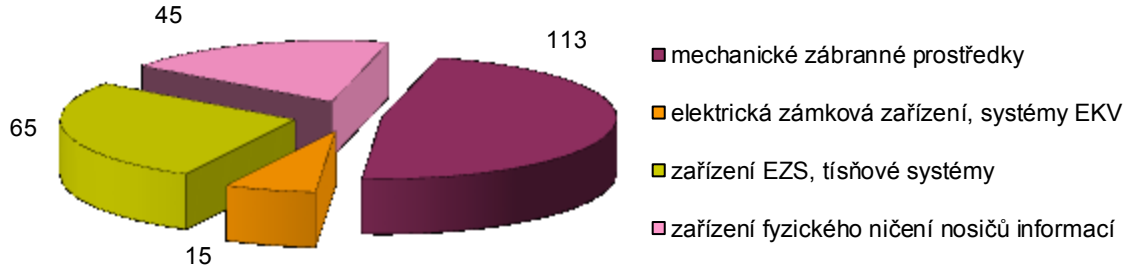
Nezbytnou zákonnou podmínkou pro používání technických prostředků k ochraně utajovaných informací je mj. i jejich certifikace. Úřad v roce 2013 přijal celkem 102 žádostí o certifikaci pro 258 technických prostředků. V rámci posuzovaní a vyhodnocování podkladů pro certifikaci bylo u 11 % žádostí vyžádáno jejich doplnění a upřesnění. V 1 případě byl certifikační proces ukončen bez vydání certifikátu, a to z důvodu nedostatečně provedené zkoušky výrobku.

Úřad vydal celkem 238 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.

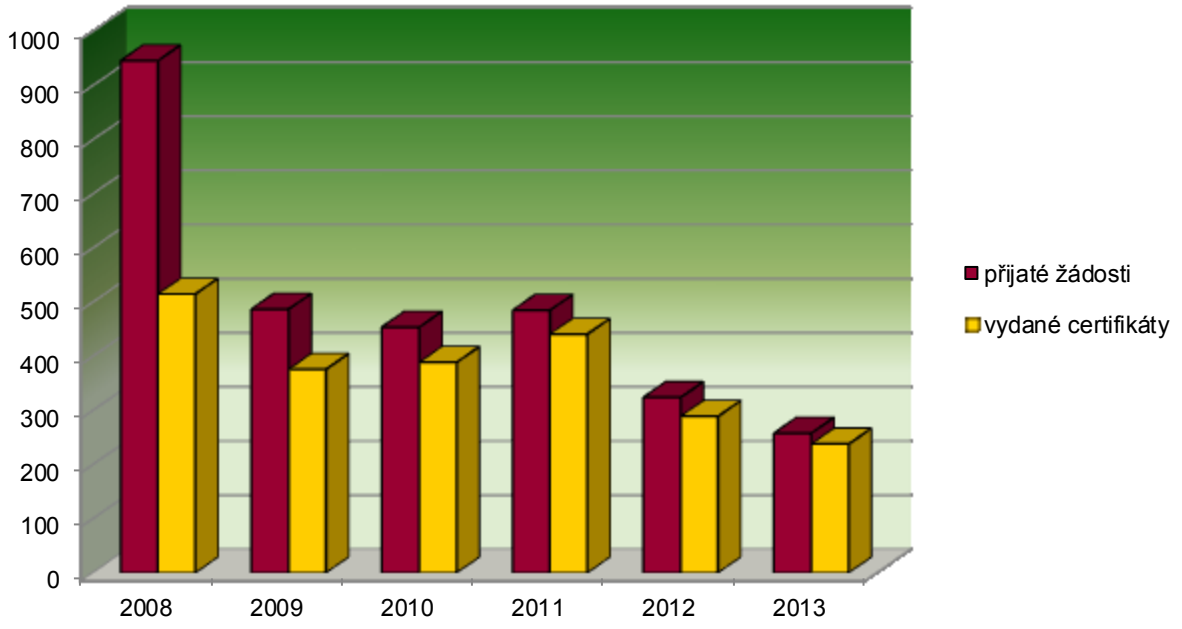
Vydané certifikáty technických prostředků v roce 2013

Mechanické zábranné prostředky[11)]	113
Elektrická zámková zařízení, systémy pro kontrolu vstupu[12)]	15
Zařízení elektrické zabezpečovací signalizace a tísňové systémy[13)]	65
Zařízení fyzického ničení nosičů informací[14)]	45
Celkem	**238**

Certifikáty technických prostředků v roce 2013



Certifikace technických prostředků v letech 2008 až 2013

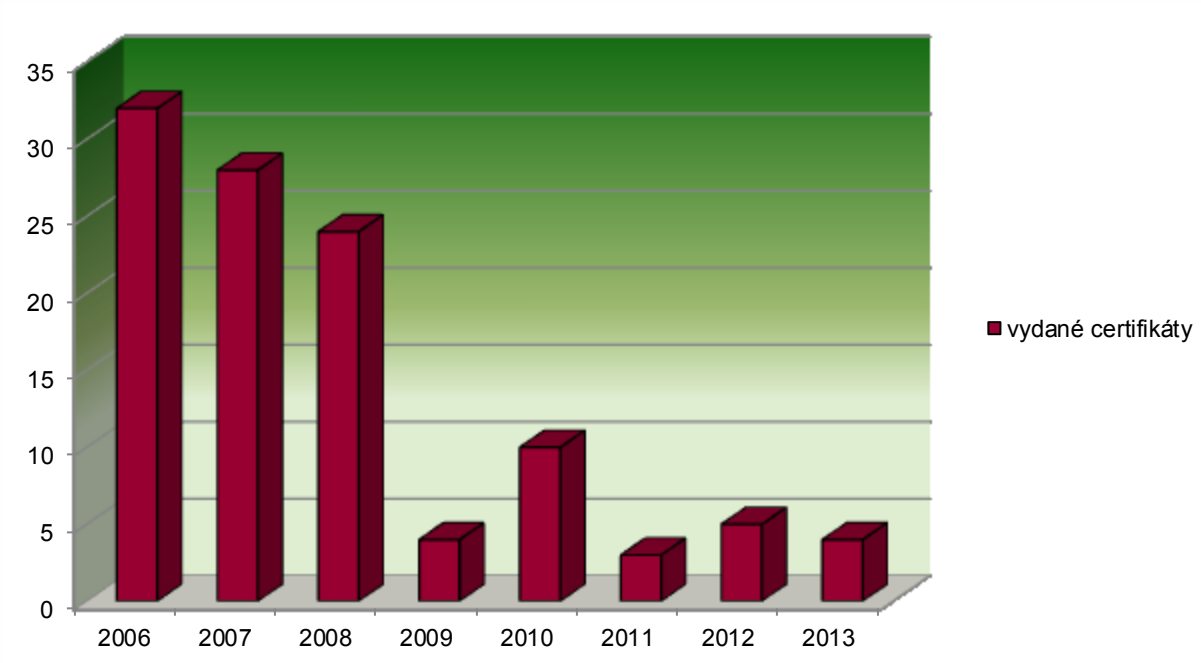


Kromě certifikátů uvedených v předchozí tabulce a grafech byly v roce 2013, na základě podaných žádostí, vydány 4 certifikáty pro jednotlivé technické prostředky

[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.

– 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 2013



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.

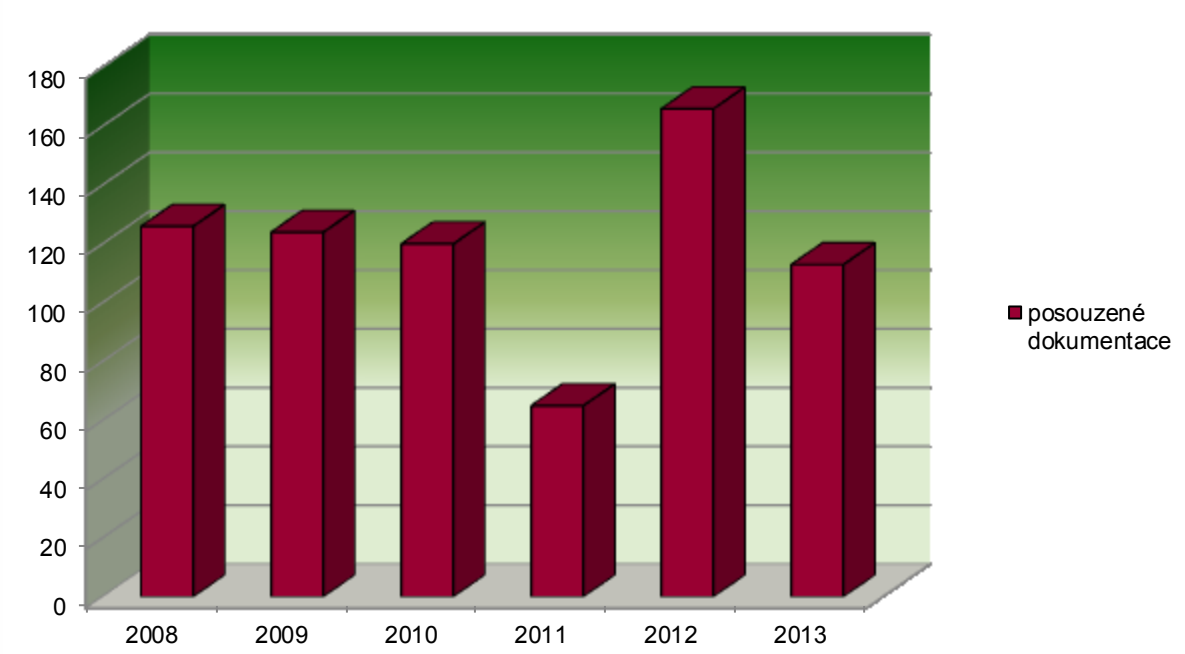
2.7.2.2. Posuzování bezpečnostní dokumentace podnikatele z hlediska fyzické bezpečnosti

V rámci vedených bezpečnostních řízení o vydání osvědčení podnikatele nebo při aktualizaci bezpečnostní dokumentace podnikatele, který je držitelem osvědčení podnikatele, bylo v roce 2013 přijato celkem 123 žádostí o stanovisko k bezpečnostní dokumentaci podnikatele z hlediska zajištění ochrany utajovaných informací fyzickou bezpečností. Při posuzování dokumentací byla v 38 % případů provedena konzultace s podnikatelem v Úřadu nebo přímo v sídle podnikatele. Bylo posouzeno 113 bezpečnostních dokumentací podnikatele a bylo provedeno 83 tzv. dohlídek, při kterých byla v sídle podnikatele ověřena jeho schopnost zabezpečit ochranu utajovaných informací z hlediska fyzické bezpečnosti. K 1. lednu 2014 zbývalo posoudit 10 bezpečnostních dokumentací podnikatele. Přehled přijatých žádostí, členěný podle kategorií zabezpečených oblastí, je uveden v následující tabulce.

Přijaté žádosti a posouzené bezpečnostní dokumentace podnikatele v roce 2013

Kontroly	Důvěrné	Tajné	Přísně tajné	Celkem
Přijaté žádosti	99	24	0	**123**
Posouzené dokumentace	90	23	0	**113**

Posouzené bezpečnostní dokumentace podnikatele v letech 2008 až 2013



2.7.2.3. Problémové oblasti fyzické bezpečnosti

Certifikace technických prostředků:

- nedostatečné podkladové materiály k žádosti o certifikaci technického prostředku a s tím spojená zvýšená administrativní zátěž.

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

- nedostatky ve zpracování projektů fyzické bezpečnosti,
- nekompletní popis režimových opatření fyzické bezpečnosti (označování a evidence klíčů, neaktualizované seznamy oprávněných osob),
- vady při instalaci technických prostředků (obrácené instalace dveří, nesprávná funkčnost systému kontroly vstupu).

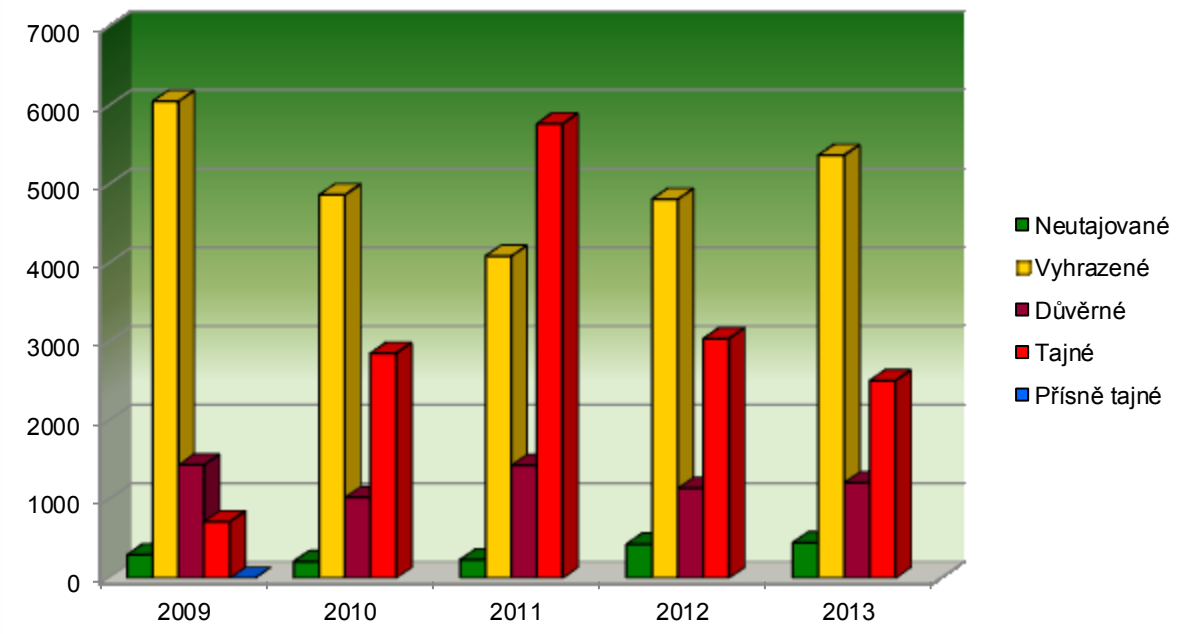
2.7.3. Ústřední registr

Prostřednictvím ústředního registru je realizováno poskytování utajovaných informací v rámci mezinárodního styku. V roce 2013 vykonával ústřední registr evidenci a ukládání těchto utajovaných informací. Zejména se jednalo o utajované informace 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	2009	2010	2011	2012	2013	Celkem
Neutajované	299	212	235	434	454	**1.634**
Vyhrazené	6.058	4.869	4.092	4.814	5.374	**25.207**
Důvěrné	1.440	1.026	1.433	1.143	1.213	**6.255**
Tajné	719	2.858	5.774	3.044	2.511	**14.906**
Přísně tajné	1	0	0	0	0	**1**
Celkem	**8.517**	**8.965**	**11.534**	**9.435**	**9.552**	**48.003**

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 14 kontrol podřízených registrů utajovaných informací. Zároveň se pracovníci ústředního registru účastnili výkonu státního dozoru u orgánů státu a podnikatelů, které mají zřízeny registry utajovaných informací. Zjištěné nedostatky se týkaly zejména autentizace a vedení administrativních pomůcek sloužících k evidenci utajovaných dokumentů.

V rámci metodického řízení bylo v roce 2013 provedeno školení vedoucích a jejich zástupců podřízených ATOMAL registrů, které bylo zaměřeno na bezpečnost utajovaných informací ATOMAL a prezentaci zkušeností získaných při cvičení ATOMAL.

Ústřední registr rovněž ověřoval splnění podmínek nezbytných pro zřízení registru utajovaných informací u 5 subjektů, které podaly žádost o souhlas ke zřízení registru utajovaných informací cizí moci. V roce 2013 byl zřízen u Úřadu v sekci bezpečnostního řízení 1 pomocný registr na odboru evidenčního šetření a podpory. V seznamu všech registrů zřízených na území ČR, vedeném v ústředním registru, bylo ke konci roku 2013 evidováno celkem 46 registrů utajovaných informací (bez pomocných registrů).

U utajovaných dokumentů cizí moci, u kterých uplynula skartační lhůta, byla prováděna skartační řízení.

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

Úřad je gestorem problematiky kybernetické bezpečnosti a národní autoritou pro tuto oblast. V rámci Úřadu bylo zřízeno Národní centrum kybernetické bezpečnosti (dále jen „NCKB“), jehož cílem je zabraňovat pokusům o průnik do infrastruktur důležitých pro chod státu. Součástí NCKB je tzv. vládní CERT (dále jen „GovCERT.CZ“), jehož úloha spočívá v monitorování kybernetického prostoru a odhalování a řešení kybernetických útoků, jejich prevenci apod. V průběhu roku 2013 pokračovaly práce spojené s vybudováním zázemí NCKB včetně GovCERT.CZ v Brně a se zajištěním jeho personálního obsazení (viz kap. 3.1.3., 3.1.4., 3.3. a 3.4.).

Od počátku roku 2013 pokračovala tvorba návrhu paragrafového znění zákona o kybernetické bezpečnosti, který byl předložen ke schválení vládě ČR (viz kap. 2.1.1.). Rovněž byly zahájeny práce na tvorbě vyhlášky o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních protiopatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti a vyhlášky o významných informačních systémech a jejich určujících kritériích, které probíhaly v průběhu celého roku 2013. Návrhy těchto prováděcích právních předpisů byly dokončeny v červnu 2013 a staly se součástí materiálu s návrhem zákona o kybernetické bezpečnosti, předloženého vládě dne 28. června 2013. V září 2013 zahájil Úřad ve spolupráci s mezirezortní pracovní skupinou přípravu konečného znění obou vyhlášek.

V roce 2013 Úřad dále spolupracoval se zástupci Generálního ředitelství Hasičského záchranného sboru ČR na tvorbě návrhu novely nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.

V oblasti kybernetické bezpečnosti Úřad rovněž spolupracuje se zahraničními partnery. Přehled mezinárodních aktivit v této oblasti je uveden v kapitole 2.2.4.

Na národní úrovni spolupracoval Úřad zejména se sdružením právnických osob CZ.NIC. Tato spolupráce se plně projevila během DDoS útoků začátkem roku 2013. Dalšími klíčovými partnery jsou CSIRT.MUNI (Computer Security Incident Response Team), neboli CSIRT Masarykovy Univerzity, který se řadí mezi špičková akademická pracoviště evropského formátu, a společnost Microsoft, s níž byla v roce 2013 podepsána smlouva upravující spolupráci v problematice botnetů. Mimo zmíněných partnerů na národní úrovni Úřad aktivně spolupracuje i s Bankovní asociací ČR, Asociací krajů ČR, Policií ČR v oblasti kybernetické kriminality, Policejním prezidiem a zpravodajskými službami ČR.

Ve spolupráci s Ministerstvem obrany byla připravena rámcová smlouva o spolupráci v oblasti informačních a komunikačních technologií a bezpečnosti. Pracovníci NCKB zároveň spolupracují i s armádním CSIRT za účelem výměny a sdílení zkušeností a informací o kybernetických událostech a incidentech.

I v tomto roce Úřad pokračoval v navazování spolupráce s akademickou sférou ČR formou smluv o spolupráci. V současné době jsou již uzavřeny smlouvy

s Masarykovou univerzitou v Brně, Vysokým učením technickým v Brně, Univerzitou obrany, Českým vysokým učením technickým v Praze a CEVRO institutem. Zároveň se připravují smlouvy s Policejní akademií, Vysokou školou báňskou v Ostravě a dalšími subjekty.

Zástupci NCKB také organizovali a účastnili se odborných seminářů a diskusí pro odbornou veřejnost (např. seminář pro poslance, senátory i pro širokou veřejnost na téma „Kybernetická bezpečnost v České republice a návrh zákona o kybernetické bezpečnosti“). Dále se aktivně účastnili seminářů pořádaných sdruženími CSIRT.CZ a AFCEA (Armed Forces Communications and Electronics Association). V říjnu 2013 NCKB podpořilo záštitou a prezentacemi mezinárodní kampaň „Evropský měsíc kybernetické bezpečnosti,“ kterou vyhlásila Evropská agentura pro bezpečnost sítí a informací (ENISA) a kterou organizovalo neziskové sdružení Národní centrum bezpečnějšího internetu. Mezi další fóra, kde zástupci NCKB přednášeli, patří např. Český institut manažerů informační bezpečnosti, ICT unie a Rada Asociace krajů ČR.

V průběhu roku 2013 navázal Úřad na průzkum zaměřený na stav zabezpečení informačních systémů státní správy a samosprávy, který prováděl v roce 2012. V rámci průzkumu bylo vyhodnoceno 44 veřejnoprávních subjektů, z nichž 28 spravovalo významné informační a komunikační systémy a 14 kritické informační a komunikační systémy. V roce 2013 bylo osloveno dalších 24 subjektů veřejné správy. Nedostatky zjištěné v průběhu tohoto průzkumu byly s dotčenými subjekty projednány na společných dvoustranných jednáních v průběhu prvního čtvrtletí roku 2013. Poznatky plynoucí z provedeného šetření budou dále využity pro vymezení kritické informační infrastruktury v ČR a pro řízení rizik spojených s jejím provozem a správou. Přestože je zákon o kybernetické bezpečnosti zatím ve fázi schvalování, NCKB již spolupracuje při mapování důležitých informačních a komunikačních systémů s budoucími povinnými subjekty. Tato spolupráce je nezbytná pro poskytnutí dostatečného prostoru povinným subjektům na přípravu ke splnění podmínek uvedeného zákona po nabytí jeho účinnosti. Ze zjištění Úřadu mimo jiné vyplynulo, že tato spolupráce má přímý a reálný přesah do vnitřního fungování jednotlivých subjektů, což vede ke zvýšení kybernetické bezpečnosti už před zavedením úpravy této oblasti do právního řádu ČR.

Dále se činnost NCKB v roce 2013 zaměřila na informační a komunikační systémy soukromoprávních subjektů a subjektů s majetkovou účastí státu. Jednalo se o ty systémy, které jsou významné či kritické pro fungování státu, jeho bezpečnost a ekonomické zájmy. V současné době probíhá oslovování a mapování situace v subjektech spadajících pod kritickou infrastrukturu podle průřezových a odvětvových kritérií pro určení prvků kritické infrastruktury podle přílohy k nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.

Nyní Úřad eviduje 184 důležitých informačních a komunikačních systémů, z toho 149 významných informačních systémů a 35 kritických informačních systémů. Vzhledem k dobíhajícímu mapování a vyhodnocování orgánů veřejné správy tento počet pravděpodobně není konečný.

Za rok 2013 bylo pracovníkům NCKB (GovCERT.CZ) oznámeno 100 incidentů. Z nich je 71 vyřešených a 29 otevřených. V souhrnu lze konstatovat, že

nejčastějšími typy útoků jsou útoky na bázi sociálního hackingu (např. phishing) a DDoS útoky. Tyto útoky probíhaly průběžně po celý rok, lišily se pouze intenzitou a napadeným subjektem (většinou státní organizace nebo organizace s velkým počtem zaměstnanců, případně zákazníků). V konkrétních číslech bylo 63 útoků zacíleno na veřejný sektor, 34 na soukromý sektor a 3 na kritickou infrastrukturu.

Na základě usnesení vlády ČR ze dne 19. října 2011 č. 781, o ustavení Národního bezpečnostního úřadu gestorem problematiky kybernetické bezpečnosti a národní autoritou pro tuto oblast, Úřad vytváří a předkládá vládě ČR „Zprávu o stavu kybernetické bezpečnosti České republiky“. Zpráva podrobně hodnotí úroveň dosažených cílů v oblasti budování kybernetické bezpečnosti České republiky za období roku 2013.

Aktuální informace zveřejňuje NCKB průběžně na svých internetových stránkách www.govcert.cz.

2.9. OPRAVNÉ PROSTŘEDKY

2.9.1. Bezpečnostní řízení

V roce 2013 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.

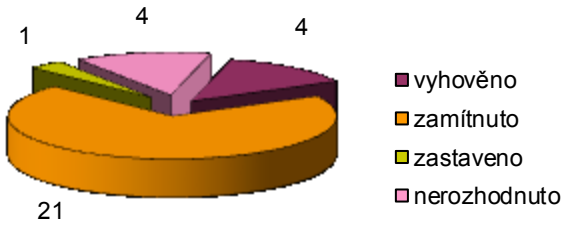
2.9.1.1. Statistické přehledy

2.9.1.1.1. Rozklady

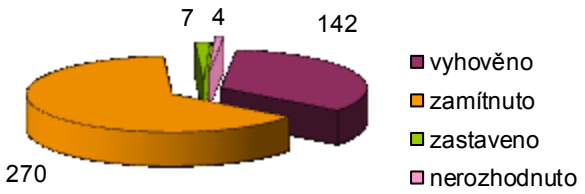
Rozklady proti rozhodnutím Úřadu v oblasti bezpečnostního řízení
(rozhoduje ředitel Úřadu)

Rok	Dosud nerozhodnuto	Vyhověno	Zamítnuto	Zastaveno	Celkem
2012	0	18	30	1	**49**
2013	4	4	21	1	**30**

Řízení o rozkladu v roce 2013



Řízení o rozkladu v letech 2006 – 2013



2.9.1.1.2. Žaloby správní

Žaloby proti rozhodnutím ředitele Úřadu o rozkladu v letech 2006 – 2013
(rozhoduje Městský soud v Praze)

Celkem	Dosud nerozhodnuto	Řízení zastaveno	Vyhověno	Zamítnuto	Odmítnuto
82	18	13	12	37	2

2.9.1.1.3. Kasační stížnosti

Kasační stížnosti proti rozhodnutím Městského soudu v Praze o zamítnutí žaloby v letech 2006 – 2013 *(rozhoduje Nejvyšší správní soud v Brně)*

Celkem	Dosud nerozhodnuto	Řízení zastaveno	Vyhověno	Zamítnuto	Odmítnuto
21	1	0	5	13	2

Kasační stížnosti podané Úřadem proti rozhodnutím Městského soudu v Praze o vyhovění žalobě v letech 2006 – 2013 *(rozhoduje Nejvyšší správní soud v Brně)*

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

2.9.1.2. Hodnocení rozhodovací praxe Úřadu

Jak vyplývá z výše uvedených údajů, v současné době je rozhodnuto v 64 případech o žalobách proti rozhodnutí ředitele Úřadu o rozkladu, přičemž pouze 12 žalob bylo shledáno důvodnými. „Úspěšnost“ Úřadu tedy činí cca 81 %.

2.9.2. Správní řízení o pokutě

V roce 2013 ředitel Úřadu rozhodoval ve 2 případech o opravných prostředcích – rozkladech – uplatněných ze strany fyzických a právnických osob ve správním řízení pro porušení povinností v oblasti ochrany utajovaných informací, přičemž obě podání byla na základě návrhu rozkladové komise zamítnuta.

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

V roce 2013 ředitel Úřadu nerozhodoval o žádných opravných prostředcích – rozkladech – uplatněných 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.

2.10. VÝZKUMNÁ A VÝVOJOVÁ ČINNOST ÚŘADU

2.10.1. Cíle a organizace výzkumu a vývoje

Základním cílem v oblasti výzkumu a vývoje pro rok 2013 byl pokračující rozvoj bezpečnostních technologií pro ochranu utajovaných informací v komunikačních a informačních systémech. Náročnost výzkumu a vývoje v oblasti bezpečnosti informačních technologií se neustále zvyšuje díky jejich rychlému rozvoji. S ohledem na kapacitní možnosti využívá Úřad pro řešení vývojových a výzkumných projektů kromě vlastních pracovišť i externí odborná pracoviště či jednotlivé externí odborníky.

2.10.2. Projekty realizované v roce 2013

Některé projekty realizované v roce 2013 navazovaly na projekty řešené v minulých letech. Hlavní příčinou této skutečnosti je výše zmíněný rychlý technologický pokrok, vzhledem k němuž je nutné neustálé monitorování a inovace již vyvinutých produktů.

V tomto roce byly řádně dokončeny 4 projekty zahájené v roce 2012, u dalších 4 projektů došlo k předání díla a počátkem roku 2014 proběhne oponentní jednání. Všechny uvedené projekty byly realizovány ve spolupráci s externími řešiteli. Dále bylo zahájeno 5 nových projektů, opět řešených ve spolupráci s externími řešiteli, z nichž 1 byl v témže roce ukončen a 1 bude v roce 2014 plynule pokračovat jako interní projekt výzkumu Úřadu.

Projekty se věnovaly oblasti kryptografické ochrany, ochrany proti úniku utajovaných informací kompromitujícím vyzařováním a kybernetické bezpečnosti. Samotná 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.

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 souvislosti s projekty řešenými v rámci výzkumu a vývoje došlo k zefektivnění a zdokonalení technologického vybavení vývojových, testovacích a měřících laboratoří v souladu s aktuálními potřebami.

V roce 2013 Úřad dále rozvíjel svou koncepci výzkumu a vývoje v oblasti kryptografické ochrany a ochrany proti úniku utajovaných informací kompromitujícím vyzařováním tak, aby mimo jiné 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.

2.11.1. Kontroly provedené v roce 2013

Stejně jako v předchozích letech byly i v roce 2013 kontroly prováděny na základě průběžně doplňovaných plánů kontrol schvalovaných ředitelem Úřadu na jednotlivá pololetí. 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 loňském roce nebyly provedeny kontroly v oblasti bezpečnostní způsobilosti.

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 vnějšího subjektu.

V roce 2013 provedl Úřad celkem 88 kontrol ochrany utajovaných informací, z toho 14 v orgánech státu a jejich složkách a 74 u podnikatelů. Souhrnné údaje o kontrolách a přehled jednotlivých kontrolních akcí realizovaných v roce 2013 je uveden v následujících tabulkách.

Kontroly provedené v roce 2013

Kontroly	Komplexní	Tematické	Následné	Celkem
Orgány státu	6	8	0	**14**
Podnikatelé	32	42	0	**74**
Celkem	**38**	**50**	**0**	**88**

Kontroly v orgánech státu a jejich součástech v roce 2013

Kontrolovaná osoba	Kontrolovaná osoba
Generální inspekce bezpečnostních sborů – oddělení Liberec	Ministerstvo zahraničních věcí – zastupitelský úřad ČR v Ankaře
Hasičský záchranný sbor Ústeckého kraje	Ministerstvo zahraničních věcí – zastupitelský úřad ČR v Prištině
Kancelář prezidenta republiky	
Kancelář veřejného ochránce práv	Ministerstvo zahraničních věcí – zastupitelský úřad ČR v Taškentu
Krajské ředitelství Policie Karlovarského kraje	
Krajské ředitelství Policie Libereckého kraje – územní odbor Liberec	Ministerstvo zahraničních věcí – zastupitelský úřad ČR ve Vídni a Stálá mise ČR při OSN, OBSE a ostatních mezinárodních organizacích ve Vídni
Ministerstvo financí	Okresní soud v Kladně
Ministerstvo pro místní rozvoj	Správa státních hmotných rezerv

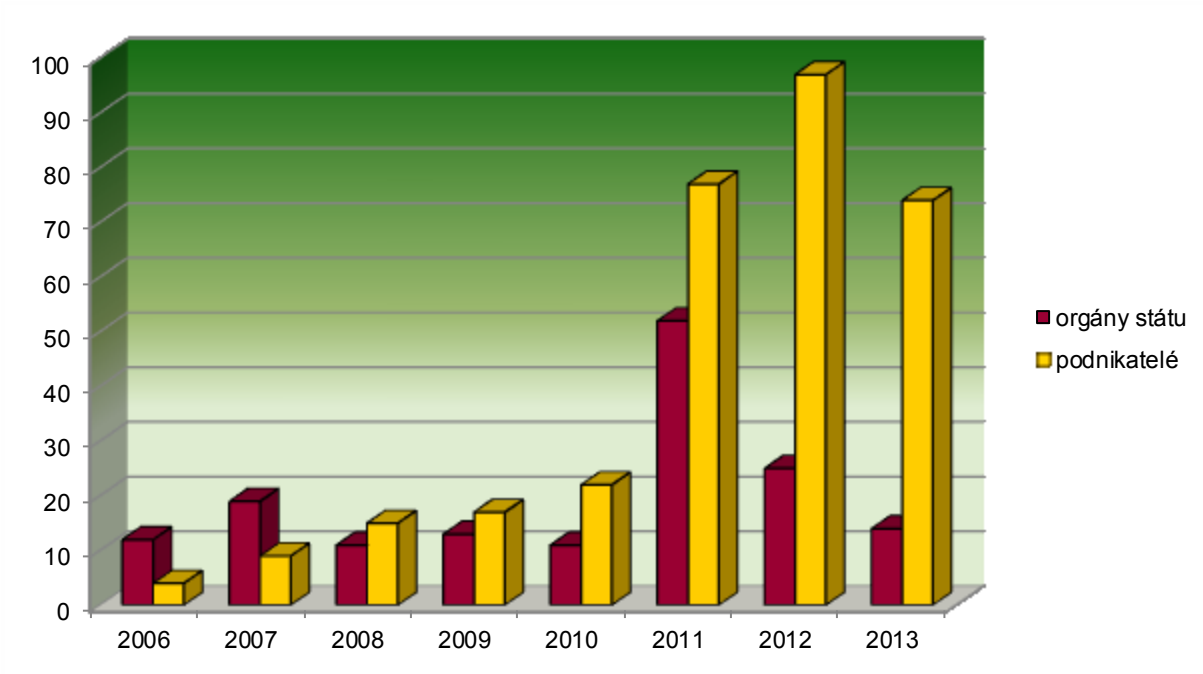
Kontroly u podnikatelů v roce 2013

Kontrolovaná osoba	Kontrolovaná osoba
ABAS IPS Management s. r. o.	ARGUS, spol. s r. o.
ALES, s. r. o.	ATICO s. r. o.
Allsat s. r. o.	ATS-TELCOM PRAHA a. s.

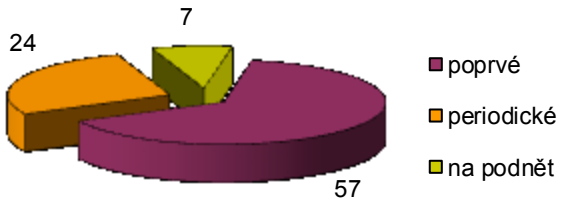
Kontrolovaná osoba	Kontrolovaná osoba
BARA HK spol. s r. o.	MERCATOR, s. r. o.
BEScom Security s. r. o.	MERIT GROUP a. s.
BLOCK a. s.	MONTSERVIS PRAHA, a. s.
CESA a. s.	NESS Czech s. r. o.
Colsys s. r. o.	oaza - net spol. s r. o.
Česká zbrojovka a. s.	OKsystem s. r. o.
České dráhy, a. s.	OM-KOMPLEX spol. s r. o.
DKNV stavební, s. r. o.	ORZO SECURITY, spol. s r. o.
E + M plus spol. s r. o.	PAMÁTKY TÁBOR, s. r. o.
EC Consulting a. s.	PKE ČR, s. r. o.
ELTES, s. r. o.	PMP Com s. r. o.
Europatron s. r. o.	Pontech s. r. o.
Explosia a. s.	PROBIN s. r. o.
F.S.C. BEZPEČNOSTNÍ PORADENSTVÍ, a. s.	Risk Analysis Consultants, s. r. o.
FATO a. s., člen holdingu FATO	S.ICZ a. s.
FORTE a. s.	Saab Czech s. r. o.
Fujitsu Technology Solutions s. r. o.	SECURITY TECHNOLOGIES s. r. o.
Hana Skálová	SEOS CZ s. r. o.
Heberger CZ s. r. o.	SINIT, a. s.
CHEMCOMEX Praha, a. s.	Skanska a. s.
I & C Energo a. s.	STAEG Stavby, spol. s r. o.
ICZ a. s.	STAVOS Brno, a. s.
INNA s. r. o.	TECHNISERV, spol. s r. o.
Institut mikroelektronických aplikací s. r. o.	TELECOM 21 CB s. r. o.
it&t s. r. o.	Telefónica Czech Republic, a. s.
Jiří Vrba	TELESPOJ, s. r. o.
KD Pragma, a. s.	TRIMR s. r. o.
Konstruktis Novostav a. s.	Triocom s. r. o.
LEC s. r. o.	VKUS-BUSTAN s. r. o.
Letiště Praha, a. s.	Vojenské lesy a statky ČR, s. p.
Logica Czech Republic s. r. o.	Vojenský technický ústav, s. p.
LUKAM s. r. o.	Vojenský výzkumný ústav s. p.
M - SILNICE a. s.	VOP CZ, s. p.
MAXPROGRES, s. r. o.	VPÚ DECO PRAHA a. s.

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

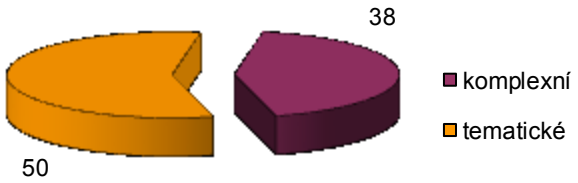
Kontroly v letech 2006 až 2013



Kontroly 2013 – podle důvodu



Kontroly 2013 – podle typu



V závěru roku 2013 intenzivně probíhaly organizační a metodické činnosti související s nabytím účinnosti nové procesní právní úpravy kontrolního postupu – zákona č. 255/2012 Sb., o kontrole (kontrolní řád), k 1. lednu 2014. Byl zpracován a schválen nový vnitřní interní akt řízení, který upravuje výkon státního dozoru v působnosti Úřadu. Rovněž bylo připraveno metodické proškolení zaměstnanců Úřadu, kteří se na výkonu státního dozoru podílejí, které bude realizováno počátkem roku 2014 tak, aby mohl Úřad kontinuálně vykonávat svou působnost v této oblasti.

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 88 kontrol provedených v roce 2013 byly nedostatky zjištěny v 58 případech (66 %). Ve 13 případech (15 %) 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 oblastech ochrany utajovaných informací. Jejich příčinou bylo ve většině případů selhání lidského činitele. Při kontrolách provedených v roce 2013 byly zjištěny zejména následující nedostatky.

Obecné nedostatky

- neoznámení jmenování bezpečnostního ředitele do funkce nebo nedodržení zákonné lhůty,
- nesplnění některé z podmínek pro výkon funkce bezpečnostního ředitele,
- vyznačení stupně utajení na dokument, který neobsahuje utajovanou informaci,
- 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,
- nesplnění všech podmínek pro přístup k utajované informaci u osoby vykonávající činnost nebo funkci, pro kterou to vyžaduje právní předpis,
- 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).

Průmyslová bezpečnost

- nedoložení splnění podmínek pro přístup podnikatele k utajované informaci (nepředložení originálu osvědčení podnikatele),

- nezaslání osvědčení podnikatele, jehož platnost zanikla, Úřadu podle § 68 písm. a) zákona,

- nedostatky ve zpracování a vedení bezpečnostní dokumentace podnikatele (neprovádění aktualizace, neúplnost, formální nebo věcné chyby apod.).

Administrativní bezpečnost

- nezaevidování utajovaných informací (dokumentů),

- neevidování seznámení se s obsahem utajovaného dokumentu (kontrolní list),

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

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

- neevidování administrativních pomůcek,

- 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).

Činnost registrů utajovaných informací

- nedostatky ve vedení evidence utajovaných informací (dokumentů) poskytnutých cizí mocí (nesplnění požadavku na oddělenou evidenci utajovaných dokumentů podle původce, chybné nebo neúplné evidenční záznamy),

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

Fyzická bezpečnost

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

- nesoulad skutečného stavu opatření fyzické bezpečnosti se stavem deklarovaným v projektu fyzické bezpečnosti (některé technické prostředky nebyly ve skutečnosti nainstalovány).

Bezpečnost informačních a komunikačních systémů

- nesplnění některých požadavků na ukládání záložních paměťových médií,

- nesplnění požadavků na instalaci informačního systému z hlediska fyzické bezpečnosti (zabezpečená oblast nesplňovala minimální požadavky pro danou kategorii) nebo z hlediska ochrany utajovaných informací před jejich únikem kompromitujícím vyzařováním.

Kryptografická ochrana

- nedostatky ve vedení evidencí kryptografického materiálu a kryptografických písemností.

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 může zaměřit 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 2013 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 2013. Členění této činnosti korespondovalo s jednotlivými fázemi bezpečnostního řízení a nadále bylo umocňováno změnami právních předpisů v oblasti ochrany utajovaných informací účinnými od 1. ledna 2012.

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. Metodickou činnost Úřadu v této rovině lze označit za velmi významnou 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.

Nadále bylo výraznou oblastí metodické činnosti poskytování konzultací, doporučení a stanovisek pro podnikatele v souvislosti s novým institutem prohlášení podnikatele podle § 15a zákona. Institut, zavedený novelou zákona účinnou od 1. ledna 2012, odstranil administrativní zátěž a zjednodušil postup pro ty podnikatelské subjekty, které ke své činnosti nezbytně potřebují mít přístup k utajovaným informacím pouze stupně utajení Vyhrazené.

Stejně jako v minulých letech byla nedílná část metodické činnosti zaměřena do oblastí poskytování prvotních informací a metodických doporučení před podáním žádosti, poskytování pomoci, konzultací a metodických doporučení při odstraňování nedostatků žádosti a zejména do oblasti metodického vedení osob, které jsou již držiteli osvědčení, a dále poskytování informací a metodické pomoci pro podnikatelské subjekty, které měly v úmyslu učinit prohlášení.

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. 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 2013 byla vydána dvě pravidelná čísla.

Obsahem Věstníku Úřadu je 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 rovněž zveřejňován na internetových stránkách Úřadu.

2.13.2. Internetové stránky Úřadu

Na internetových stránkách Úřadu (www.nbu.cz) jsou zveřejňovány veškeré informace, které se týkají činnosti Úřadu a jeho hlavních úkolů. Jsou zde uvedeny odborné i všeobecné informace, včetně aktualit, tiskových zpráv 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 2013 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, byly zřízeny nové stránky www.govcert.cz, na kterých uživatelé naleznou aktuality z této oblasti, informace o činnosti Rady pro kybernetickou bezpečnost, informační servis atd.

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.

Internetové stránky Úřadu byly vybrány Národní knihovnou ČR jako kvalitní zdroj, který by měl být uchován do budoucna, jejich záznam je součástí bibliografie a katalogu Národní knihovny ČR. Stránky jsou opatřeny logem Webarchiv.

V roce 2013 vykázaly internetové stránky téměř 200.000 přístupů, což je více než 16.000 návštěv za měsíc.

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

V roce 2013 bylo Úřadu podáno 11 žádostí o informace podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů.

Všem žádostem bylo v plném rozsahu vyhověno a požadované informace byly žadatelům poskytnuty.

V roce 2013 nebyla poskytnuta žádná výhradní licence ani nebyla podána žádná stížnost podle § 16a zákona č. 106/1999 Sb.

2.15. INSPEKCE ŘEDITELE ÚŘADU

Inspekce ředitele Úřadu v průběhu roku 2013 prováděla, v rámci plnění dlouhodobých úkolů, činnosti související s výkonem interní kontroly určených oblastí působnosti Úřadu.

V oblasti boje proti korupci plnila úkoly vyplývající z příslušných usnesení vlády ČR a podílela se na činnosti Mezirezortní koordinační skupiny pro boj s korupcí při Úřadu vlády ČR.

V roce 2013 inspekce ředitele Úřadu řešila 3 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

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

V roce 2013 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.

Kontroly byly vykonávány jednorázově i průběžně. V roce 2013 nebylo zjištěno závažné porušení ochrany utajovaných informací zaměstnanci Úřadu. Rovněž ustanovení provozního řádu byla v roce 2013 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 zaměstnanců Úřadu a u uchazečů o zaměstnání v 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 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 2013 bylo evidováno 95 žádostí o vydání osvědčení fyzické osoby, na jejichž základě bylo vydáno 48 osvědčení fyzické osoby. V 1 případě nebylo žádosti vyhověno (oznámení o nevydání osvědčení). Ve zbývajících případech nebyla bezpečnostní řízení k 31. prosinci 2013 ukončena.

Vydaná osvědčení fyzické osoby v rámci Úřadu v roce 2013

Důvěrné	7
Tajné	41
Přísně tajné	11
Celkem	**59**

Důvody zastavení bezpečnostního řízení v rámci Úřadu v roce 2013

Nedání souhlasu účastníka řízení podle § 107 odst. 5 zákona	1
Odpadnutí důvodu řízení	1
Oznámení odpovědné osoby podle § 67 odst. 1 písm. g) zákona	4
Celkem	**6**

Důvody zániku platnosti osvědčení fyzické osoby v rámci Úřadu v roce 2013

Doručení nového osvědčení	33
Vrácení osvědčení	4
Změna některého z údajů uvedených v osvědčení	5
Celkem	**42**

Vydaná osvědčení fyzické osoby pro cizí moc v rámci Úřadu v roce 2013

COSMIC TOP SECRET ATOMAL	4
COSMIC TOP SECRET	5
NATO SECRET	12
Celkem	**21**

V roce 2013 bylo dále vydáno 8 oznámení o splnění podmínek pro přístup k utajované informaci stupně utajení Vyhrazené.

Odbor bezpečnostní zajišťuje rovněž evidenční ochranu zaměstnanců Úřadu v případě jejich ohrožení v souvislosti s výkonem povolání. V roce 2013 byla, v souvislosti se změnou organizační struktury Úřadu, provedena aktualizace seznamu chráněných osob.

3.1.3. Fyzická bezpečnost v rámci Úřadu

V roce 2013 bylo v oblasti fyzické bezpečnosti realizováno výběrové řízení na rekonstrukci elektrické požární signalizace pro objekty areálu Úřadu v Praze v ulici Na Popelce. S vítězným uchazečem byla podepsána smlouva o dílo, s předpokladem plnění zasahujícím zejména do roku 2014. S ohledem na změny v požadavcích na příslušné kategorie zabezpečených oblastí byly realizovány úpravy dotčených bezpečnostních technologií v souladu s vyhláškou č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů.

V rámci budování NCKB jsou, na základě veřejné zakázky „Zabezpečení objektu Mučednická č. p. 1125, Brno“ vypsané v roce 2012, instalovány 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. Předpokládané dokončení díla je v prvním čtvrtletí roku 2014. Instalací výše uvedených bezpečnostních technologií bude zajištěna vysoká úroveň fyzické bezpečnosti objektu. Zaměstnanci Úřadu se podíleli na návrhu uvedených technologií a působí jako technický dozor při jejich realizaci.

Pro potřeby Ochranné služby Policie ČR, která zajišťuje stálou ostrahu objektu, bylo v roce 2013 vybaveno pracoviště (recepce) technikou pro kontrolu zavazadel a návštěv.

V průběhu roku 2013 bylo zahájeno zpracovávání projektu fyzické bezpečnosti pro objekt NCKB podle § 32 zákona a příprava dalších interních aktů řízení, které budou v této oblasti pro jeho provoz nezbytné.

3.1.4. Krizové řízení v rámci Úřadu

Odbor bezpečnostní zajišťuje připravenost Úřadu na řešení krizových situací v oboru své působnosti.

V roce 2013 se zástupci Úřadu účastnili jednání s příslušnými složkami Ministerstva vnitra, Ministerstva obrany a s Výborem pro civilní a nouzové plánování. Uvedeným subjektům byla poskytována nezbytná součinnost. V souvislosti s budováním NCKB proběhlo v roce 2013 jednání s Hasičským záchranným sborem Jihomoravského kraje zaměřené zejména na analýzu rizik objektu v ulici Mučednická v Brně.

3.1.5. Ostatní činnosti

Od roku 2013 jsou připravovány změny interních aktů řízení, týkajících se zajištění bezpečnosti a provozu Úřadu. Jedná se především o nový provozní řád a dále o směrnice upravující provoz a používání motorových vozidel Úřadu, resp. zřízení krizového štábu 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 2013 bylo provedeno 10 archivních prohlídek. Celkový rozsah archiválií je v bezpečnostním archivu 9,60 běžných metrů a ve specializovaném archivu 7,84 běžných metrů. V roce 2013 nenavštívil bezpečnostní archiv žádný badatel a specializovaný archiv navštívil 1 interní badatel.

V roce 2013 byla provedena generální inventura archiválií vedených v evidenci Národního archivního dědictví. Její ukončení bylo stanoveno na den 31. prosince 2013. V závěru bylo konstatováno, že nedošlo ke ztrátě ani neoprávněnému zničení žádné archiválie. Z výsledků generální inventury byl zpracován protokol popisující stav ke dni 31. prosince 2013, jenž byl dne 13. ledna 2014 zaslán odboru archivní správy a spisové služby Ministerstva vnitra.

3.3. EKONOMICKÉ ZABEZPEČENÍ ÚŘADU

Úřad je od 1. listopadu 1998 samostatnou kapitolou státního rozpočtu „308“ a jeho činnost byla v roce 2013 financována ze státního rozpočtu a z malé části i ze strukturálních fondů EU. Projekt byl zahájen v roce 2013 a bude ukončen v roce 2014.

Naplňování příjmů státního rozpočtu souvisí se správní činností Úřadu. Daňové příjmy, jejichž největší podíl tvořily správní poplatky, byly vybrány ve výši 310 tis. Kč. Nedaňové příjmy byly odvedeny za uložené pokuty ve výši 33 tis. Kč, za nahodilé příjmy, jako jsou přeplatky z předcházejících let a drobné příjmy ve výši 372,82 tis. Kč. Celkem Úřad odvedl do státního rozpočtu 715,82 tis. Kč.

Schválené rozpočtové výdaje na rok 2013 ve výši 299.897 tis. Kč byly upraveny rozpočtovými opatřeními Ministerstva financí na 322.257,41 tis. Kč.

K největšímu posílení rozpočtu, ve výši 15.820,80 tis. Kč, došlo v souvislosti s implementací veřejné regulované služby programu Galileo (PRS) v České republice, a to na základě usnesení vlády č. 71 ze dne 30. ledna 2013. Z celkového rozpočtu bylo 61.464 tis. Kč určeno na vybudování NCKB, situovaného v Brně, jako součásti Úřadu. NCKB je budováno v souvislosti s realizací usnesení vlády ČR č. 781 ze dne 19. října 2011, o ustavení Národního bezpečnostního úřadu gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast.

Rozpočet roku 2013 byl dále posílen o nespotřebované výdaje roku 2012 ve výši 39.939,42 tis. Kč. Důvodem nespotřebování těchto výdajů byl fakt, že v roce 2012 byly započaty stavební úpravy objektu určeného pro NCKB, na které byly převážně určeny. Rozpočet roku 2013 byl čerpán ve výši 295.754,73 tis. Kč. Největší objem běžných výdajů tvořily, jako každým rokem, mzdové výdaje a zákonem dané odvody, které byly vyčerpány na 97,92 %.

V roce 2013 byl zahájen projekt spolufinancovaný ze Strukturálních fondů EU „Napojení agendového informačního systému CEFEUS na ISZR“. Tento projekt byl schválen Ministerstvem vnitra jako Zprostředkujícím subjektem Integrovaného operačního programu pro období 2007-2013 (dále jen „IOP“) pro oblasti intervence 1.1 Rozvoj informační společnosti ve veřejné správě, na základě usnesení vlády č. 536 ze dne 14. května 2008 a Dohody o delegování úkolů Řídícího orgánu IOP na Ministerstvo vnitra jako Zprostředkující subjekt v rámci implementace IOP pro období 2007-2013 a dále vzhledem k rozhodnutí Komise č. K (207) 6835 ze dne 20. prosince 2007, kterým se přijímá IOP. Projekt byl schválen v oblasti podpory 1.1a Rozvoj informační společnosti ve veřejné správě, pod registračním číslem CZ.1.06./1.1.00/14.08497. Celkové náklady projektu činí 4.337,45 tis. Kč. V roce 2013 bylo čerpáno celkem 2.693,66 tis. Kč.

Běžné výdaje na provoz, zejména platby v oblasti energií, nezbytných služeb a nákupů k zajištění činnosti Úřadu a NCKB, činily po rozpočtových změnách 57.025,15 tis. Kč (posíleny byly o nespotřebované výdaje roku 2012) a byly čerpány na úrovni 85,63 %.

Kapitálové výdaje konečného rozpočtu ve výši 118.719,02 tis. Kč (byly posíleny o nespotřebované výdaje roku 2012) byly určeny zejména na financování vybudování NCKB, a to konkrétně ve výši 36.330,17 tis. Kč. V oblasti pořízení hmotného a nehmotného majetku byly vyčerpány ve výši 11.550,74 tis. Kč. Kapitálové výdaje ve výši 17.637,35 tis. Kč byly určeny 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 21.067,56 tis. Kč. Vyčerpáno bylo 18.528,45 tis. Kč. Z toho v rámci uzavřených smluvních závazků s externími řešiteli bylo na výzkumné projekty vyčerpáno 17.637,35 tis. Kč a v rámci vlastních výzkumných kapacit bylo vyčerpáno 891,10 tis. Kč.

Celkem činí nároky nespotřebovaných výdajů z rozpočtu roku 2013 částku 66.442,10 tis. Kč. Tyto finanční prostředky jsou určeny zejména na nákup IT technologií pro NCKB a PRS, na nákup speciálních přístrojů a technologií potřebných

pro řádné fungování těchto institucí, dále na zařízení budovy nábytkem. Dále jsou výdaje určeny na pokrytí smluvních závazků nerealizovaných v roce 2013.

Rozpočty jednotlivých let mají do roku 2012 klesající tendenci. Rokem 2012 (tento trend bude pokračovat i v roce 2014 a 2015) rozpočet a s tím související výdaje narůstají vlivem budování a následně pak provozováním NCKB a PRS v Brně. Největší skok je pak patrný v roce 2013, kdy byla dokončena rekonstrukce objektu v Brně, který je pro tato pracoviště vyčleněn.

Úřad i nadále financoval v roce 2013 vybudování NCKB na základě výše uvedeného usnesení vlády, na které byly finanční prostředky uvolněny pro rok 2013 ve výši 61.646 tis. Kč, tyto výdaje jsou vykazované a sledované zvlášť, včetně tabulkových počtů, mezd a zákonem daných odvodů, tj. mimo rozpočet na provoz Úřadu. Nemovitost, sídlo NCKB, byla v roce 2011 získána bezúplatně od Ministerstva obrany a koncem roku 2013 došlo k její kolaudaci, celkové náklady na stavební úpravy v roce 2013 činily 34.940,15 tis. Kč.

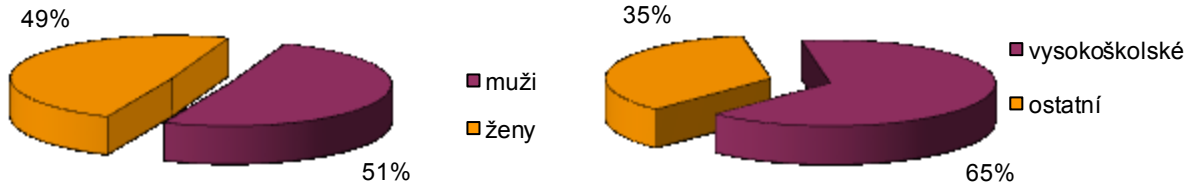
Veškeré výdaje finančních prostředků určených na financování činnosti Úřadu, tj. vyplývajících ze zákona, procházely, v souladu se zákonem o finanční kontrole, předběžnou a průběžnou finanční kontrolou. Následná kontrola byla prováděna jak příkazci operací, tak hlavní účetní a u vybraných finančních operací průřezově i správcem rozpočtu.

3.4. PERSONÁLNÍ ZABEZPEČENÍ ÚŘADU

Pro rok 2013 měl Úřad systemizovaných 296 pracovních míst, z tohoto počtu bylo 19 míst určeno pro NCKB, resp. problematiku kybernetické bezpečnosti, a 2 místa pro Národní centrum Public Regulated Services. V průběhu roku byla všechna pracovní místa v NCKB v Praze i v Brně, i místa v Národním centru PRS obsazena novými, převážně mladými odborníky. V této oblasti se rozvíjí spolupráce s vysokými školami a dalšími akademickými subjekty.

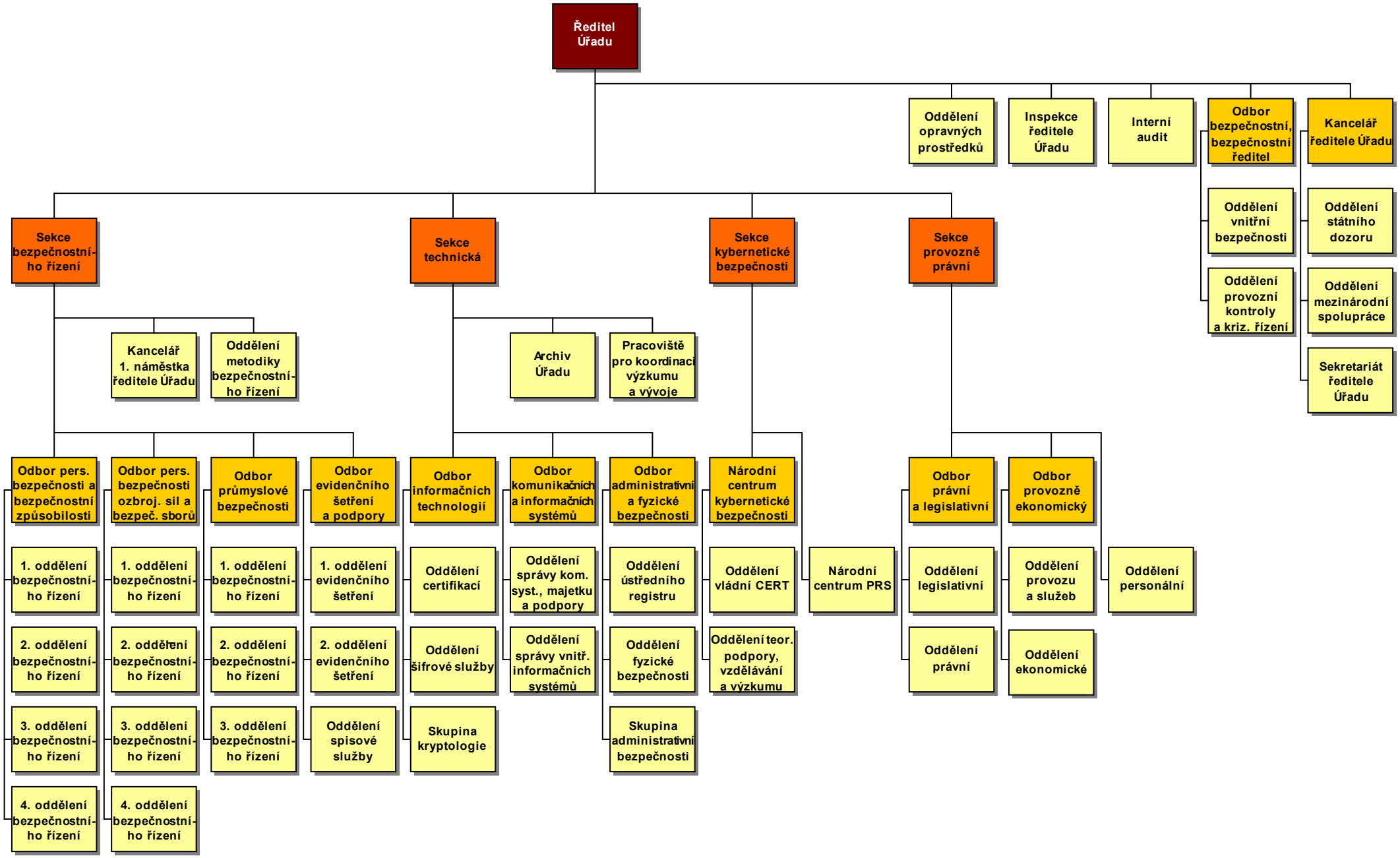
K 31. prosinci 2013 bylo aktuálně obsazeno 292 pracovních míst, z toho bylo 149 mužů a 143 žen. Průměrný věk zaměstnanců byl 49 let, více než 65 % zaměstnanců mělo vysokoškolské vzdělání. Úřad vyvíjí maximální úsilí, aby pracovní místa byla obsazena kvalifikovanými a schopnými zaměstnanci s odpovídající praxí, kteří zároveň splňují požadavky pro přístup k utajovaným informacím.

Struktura zaměstnanců Úřadu – muži/ženy a podle vzdělání

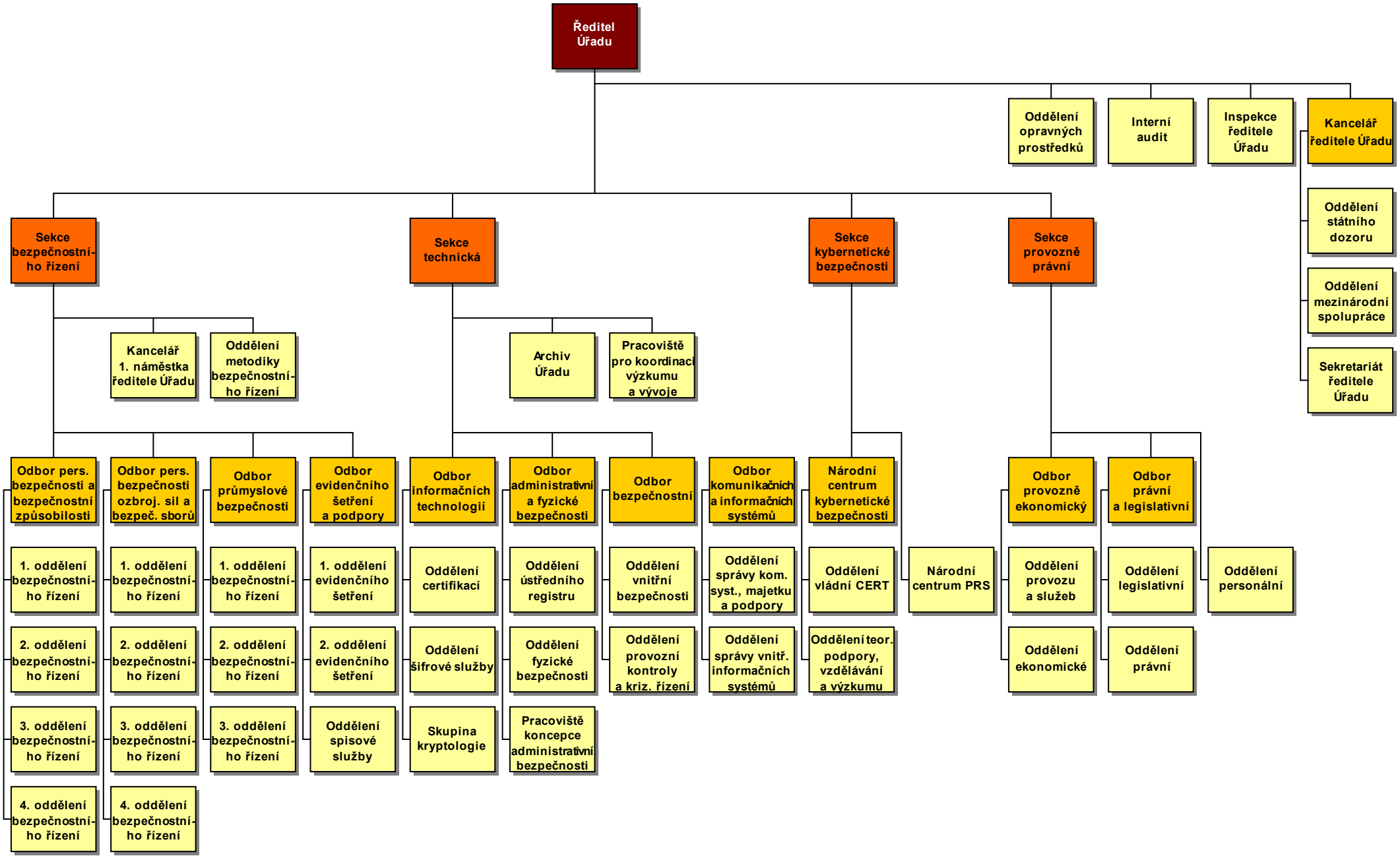


V Úřadu je průběžně realizován systém vzdělávání zaměstnanců. V roce 2013 pokračovalo jazykové vzdělávání, kterého se pravidelně účastní více než 60 zaměstnanců, dále probíhala odborná školení především v oblasti informačních technologií. Pozornost byla věnována zdokonalení komunikačních dovedností zaměstnanců, kteří přicházejí do kontaktu s veřejností, a pokračovalo rovněž manažerské vzdělávání vedoucích zaměstnanců zaměřené především na týmovou spolupráci. 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 k 1. 1. 2013



Organizační schéma Národního bezpečnostního úřadu k 31. 12. 2013



PŘÍLOHA – ČERPÁNÍ EVROPSKÝCH FONDŮ (TISKOVÁ ZPRÁVA)

INTEGROVANÝ OPERAČNÍ PROGRAM

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
ŠANCE PRO VÁŠ ROZVOJ

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

V Praze, 27. června 2013

Národní bezpečnostní úřad se zapojil do elektronizace a digitalizace veřejné správy

Elektronizace a digitalizace veřejné správy je dnes nezadržitelný proces. Těžko bychom, až na výjimky, hledali státní instituci, která není přístupná prostřednictvím počítačové sítě. Národní bezpečnostní úřad (NBÚ) se do tohoto procesu zapojuje kromě jiného s projekty, které jsou spolufinancovány ze strukturálních fondů Evropské unie.

V letošním roce začal NBÚ realizovat projekt Napojení agendového informačního sytému CEFEUS na Informační systém základních registrů. CEFEUS je informační systém, sloužící Národnímu bezpečnostnímu úřadu jako podpora pro bezpečnostní řízení u fyzických a právnických osob a podnikatelů.

Cílem je zlepšení služeb státní správy snížením administrativní zátěže podnikatelů a státní správy samotné, zrychlení některých procedur souvisejících s bezpečnostním řízením, a zejména využití získávání hodnot referenčních údajů garantovaným způsobem přímo z příslušných registrů namísto dokládání ze strany ekonomických subjektů či fyzických osob.

Řešení projektu předpokládá úpravy agendového informačního systému CEFEUS takovým způsobem, aby mohla být realizována bezpečná napojení na vnější rozhraní základních registrů.

Celková hodnota projektu je 4,4 milionu korun českých, ukončení jeho realizace je plánováno na první pololetí roku 2014.

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 4

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

2.1.4. Právní činnost 5

2.2. MEZINÁRODNÍ SPOLUPRÁCE ÚŘADU 6

2.2.1. Mezinárodní smlouvy 6

2.2.1.1. Hodnocení sjednávání smluv o ochraně utajovaných informací za rok 2013 7

2.2.1.2. Výhled na rok 2014 8

2.2.2. Aktivity vyplývající z členství ČR v NATO a EU 8

2.2.3. Spolupráce s bezpečnostními úřady partnerských států 12

2.2.4. Mezinárodní aktivity Úřadu v oblasti kybernetické bezpečnosti 13

2.3. PERSONÁLNÍ BEZPEČNOST 13

2.3.1. Bezpečnostní řízení o žádostech fyzických osob 14

2.3.2. Prověřování splňování podmínek po vydání osvědčení 15

2.3.3. Analýza důvodů nevydání nebo zrušení platnosti osvědčení fyzické osoby 15

2.3.4. Přehled ostatních důvodů zániku platnosti osvědčení fyzické osoby 16

2.3.5. Statistické přehledy 17

2.3.6. Personální projekt 19

2.4. BEZPEČNOSTNÍ ZPŮSOBILOST 20

2.4.1. Statistické přehledy 21

2.5. PRŮMYSLOVÁ BEZPEČNOST 22

2.5.1. Bezpečnostní řízení o žádostech podnikatelů 22

2.5.2. Prověřování splňování podmínek po vydání osvědčení 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 26
2.6.1. Certifikační a akreditační činnost 27
2.6.1.1. Certifikace a akreditace informačních systémů 27
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 33
2.6.2.1. Výroba kryptografického materiálu 33
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 34
2.6.2.2.3. Přehled provedených měření 34
2.6.2.3. Schvalování projektů bezpečnosti komunikačních systémů 35
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 36
2.7. ADMINISTRATIVNÍ A FYZICKÁ BEZPEČNOST, ÚSTŘEDNÍ REGISTR 36
2.7.1. Administrativní bezpečnost 36
2.7.2. Fyzická bezpečnost 37
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 41
2.8. KYBERNETICKÁ BEZPEČNOST 43
2.9. OPRAVNÉ PROSTŘEDKY 45

2.9.1. Bezpečnostní řízení 45

2.9.1.1. Statistické přehledy 46

2.9.1.1.1. Rozklady 46

2.9.1.1.2. Žaloby správní 46

2.9.1.1.3. Kasační stížnosti 46

2.9.1.2. Hodnocení rozhodovací praxe Úřadu 47

2.9.2. Správní řízení o pokutě 47

2.9.3. Řízení podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím 47

2.10. VÝZKUMNÁ A VÝVOJOVÁ ČINNOST ÚŘADU 47

2.10.1. Cíle a organizace výzkumu a vývoje 47

2.10.2. Projekty realizované v roce 2013 47

2.11. STÁTNÍ DOZOR 48

2.11.1. Kontroly provedené v roce 2013 48

2.11.2. Výsledky kontrol 51

2.12. METODICKÁ ČINNOST ÚŘADU 54

2.12.1. Metodická činnost v oblasti bezpečnostního řízení 55

2.13. VĚSTNÍK ÚŘADU A INTERNETOVÉ STRÁNKY ÚŘADU 56

2.13.1. Věstník Úřadu 56

2.13.2. Internetové stránky Úřadu 56

2.14. POSKYTOVÁNÍ INFORMACÍ PODLE ZÁKONA Č. 106/1999 SB., O SVOBODNÉM PŘÍSTUPU K INFORMACÍM 57

2.15. INSPEKCE ŘEDITELE ÚŘADU 58

3. BEZPEČNOSTNÍ, EKONOMICKÉ A PERSONÁLNÍ ZABEZPEČENÍ ÚŘADU 58

3.1. OCHRANA UTAJOVANÝCH INFORMACÍ A KRIZOVÉ ŘÍZENÍ V ÚŘADU 58

3.1.1. Vnitřní kontrola 58

3.1.2. Personální bezpečnost v rámci Úřadu 58

3.1.3. Fyzická bezpečnost v rámci Úřadu 60

3.1.4. Krizové řízení v rámci Úřadu 60

3.1.5. Ostatní činnosti 61

3.2. ARCHIV NÁRODNÍHO BEZPEČNOSTNÍHO ÚŘADU 61

3.3. EKONOMICKÉ ZABEZPEČENÍ ÚŘADU 61

3.4. PERSONÁLNÍ ZABEZPEČENÍ ÚŘADU 63

PŘÍLOHA – ČERPÁNÍ EVROPSKÝCH FONDŮ (TISKOVÁ ZPRÁVA) 67