VÝROČNÍ ZPRÁVA

O ČINNOSTI

NÁRODNÍHO BEZPEČNOSTNÍHO ÚŘADU

ZA ROK

2011

Praha 2012

1. Úvod

Stejně jako v předcházejících letech byla i v roce 2011 činnost Národního bezpečnostního úřadu (dále jen „Úřad“), 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“), 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,
- přípravné legislativní, organizační a provozně-technické činnosti v souvislosti s nově převzatou gescí za oblast kybernetické bezpečnosti.

2. Činnost Úřadu

2.1. Legislativní a právní činnost Úřadu

2.1.1. Vnější legislativní činnost

Zákon byl v roce 2011 celkem třikrát novelizován, a to zákonem č. 255/2011 Sb., zákonem č. 420/2011 Sb. a zákonem č. 458/2011 Sb.

- Zákon č. 255/2011 Sb., kterým se mění zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů, a zákon č. 634/2004 Sb., o správních poplatcích, ve znění pozdějších předpisů, je novelou (dále jen „velká novela“), která s účinností od 1. ledna 2012 provádí zejména změny na úseku ochrany utajovaných informací, odstraňuje administrativní zátěž účastníků bezpečnostního řízení

i Úřadu, zavádí zpoplatnění žádosti podnikatele o vydání osvědčení podnikatele, zkracuje lhůty bezpečnostního řízení, a reaguje na změny v oblasti elektronizace veřejné správy.

- Zákon č. 420/2011 Sb., o změně některých zákonů v souvislosti s přijetím zákona o trestní odpovědnosti právnických osob a řízení proti nim, s účinností od 1. ledna 2012, stanoví nové povinnosti podnikatelům při podání žádosti o vydání osvědčení podnikatele a stanoví také nové bezpečnostní riziko, jehož výskyt u podnikatele Úřad v rámci bezpečnostního řízení ověřuje.

- Zákon č. 458/2011 Sb., o změně zákonů související se zřízením jednoho inkasního místa a dalších změnách daňových a pojistných zákonů, provádí s účinností od 1. ledna 2015 dílčí změny při posuzování ekonomické stability podnikatele.

V souvislosti s přijetím velké novely zákona Úřad připravil aktualizaci prováděcích předpisů. Celkem Úřad vydal 3 zcela nové vyhlášky:

- vyhláška č. 363/2011 Sb., o personální bezpečnosti a o bezpečnostní způsobilosti,

- vyhláška č. 405/2011 Sb., o průmyslové bezpečnosti,

- vyhláška č. 432/2011 Sb., o zajištění kryptografické ochrany utajovaných informací,

a 4 další vyhlášky, kterými byla provedena výrazná novelizace stávajících vyhlášek:

- vyhláška č. 433/2011 Sb., kterou se mění vyhláška č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací, ve znění vyhlášky č. 55/2008 Sb.,

- vyhláška č. 434/2011 Sb., kterou se mění vyhláška č. 525/2005 Sb., o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací,

- vyhláška č. 453/2011 Sb., kterou se mění vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor,

- vyhláška č. 454/2011 Sb., kterou se mění vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008 Sb.

S účinností od 1. ledna 2012 je tak komplexně právně zajištěna činnost Úřadu, jak plyne z velké novely zákona.

Úřad dále, na základě 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, zpracovává věcný záměr zákona o kybernetické bezpečnosti tak, aby byl do konce března 2012 předložen vládě. Na základě téhož usnesení vlády má Úřad povinnost předložit do konce července 2013 samotný návrh zákona o kybernetické bezpečnosti.

2.1.2. Vnitřní legislativní činnost

V průběhu roku 2011 bylo vydáno celkem 24 nových interních aktů řízení ředitele Úřadu. V souvislosti se zefektivněním řídících procesů a činnosti Úřadu po přijetí velké novely zákona a s převzetím gesce za oblast kybernetické bezpečnosti včetně zřízení Národního centra kybernetické bezpečnosti došlo k novelizaci organizačního řádu. Ostatní nově vydané interní akty řízení byly vydány z důvodu změn v právním řádu a s ohledem na snahu o zvýšení produktivity Úřadu.

2.1.3. Právní činnost

V roce 2011 bylo pro porušení povinností stanovených zákonem ukončeno celkem 70 správních řízení, z toho v 60 případech s fyzickými osobami a v 10 případech s právnickými osobami. Ve 3 případech bylo správní řízení zastaveno a v 67 případech byla uložena sankce (převážně peněžitá pokuta). V 5 dalších případech správní řízení dosud nebylo ukončeno. Celková výše uložených pokut dosáhla částky 666.500 Kč.

Správní řízení v roce 2011

	Fyzická osoba	Právnická osoba	Celkem
Ukončená správní řízení	60	10	**70**
Počet uložených sankcí	58	9	**67**
Zastavená správní řízení	2	1	**3**
Dosud neukončená správní řízení	2	3	**5**

V oblasti právní činnosti bylo v roce 2011 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 uplatňuje nárok na náhradu této škody 10 žadatelů. 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 2011

V roce 2011 byly vyvíjeny následující aktivity v rámci sjednávání mezinárodních smluv:

- **Smlouva mezi vládou České republiky a Radou ministrů Albánské republiky o výměně a vzájemné ochraně utajovaných informací**

  Smlouva byla v ČR ratifikována, čeká se na splnění vnitrostátních podmínek pro vstup smlouvy v platnost na albánské straně.

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

  Smlouva vstoupila v platnost 1. července 2011 a byla publikována ve Sbírce mezinárodních smluv.

- **Smlouva mezi vládou České republiky a vládou Ázerbájdžánské republiky o výměně a vzájemné ochraně utajovaných informací**

  Parlament ČR vyslovil souhlas s ratifikací.

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

  V roce 2011 pokračovalo expertní jednání o smlouvě.

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

  Smlouva vstoupila v platnost 1. července 2011 a byla publikována ve Sbírce mezinárodních smluv.

- **Smlouva mezi vládou České republiky a vládou Černé Hory o výměně a vzájemné ochraně utajovaných informací**

  Smlouva vstoupila v platnost 1. června 2011 a byla publikována ve Sbírce mezinárodních smluv.

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

  Smlouva vstoupila v platnost 1. července 2011 a byla publikována ve Sbírce mezinárodních smluv.

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

  Parlament ČR vyslovil souhlas s ratifikací.

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

  Smlouva byla v ČR ratifikována, čeká se na splnění vnitrostátních podmínek pro vstup smlouvy v platnost na lucemburské straně.

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

  Expertní jednání o smlouvě bylo ukončeno. Dosud probíhá vnitrostátní schvalovací procedura v Nizozemsku.

- **Smlouva mezi vládou České republiky a vládou Rumunska o vzájemné ochraně vyměněných utajovaných informací**

  Smlouva vstoupila v platnost 1. června 2011 a byla publikována ve Sbírce mezinárodních smluv.

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

  V roce 2011 pokračovalo expertní jednání o smlouvě.

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

  Smlouva byla v ČR ratifikována, čeká se na splnění vnitrostátních podmínek pro vstup smlouvy v platnost na švýcarské straně.

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

  V roce 2011 pokračovalo expertní jednání o smlouvě.

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

  Smlouva byla podepsána v Bruselu dne 12. října 2011 ředitelem Národního bezpečnostního úřadu Ing. Dušanem Navrátilem a ředitelem Národního bezpečnostního úřadu Estonska Märtem Kraftem.

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

  V roce 2011 pokračovalo expertní jednání o smlouvě.

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

  V roce 2011 pokračovalo expertní jednání o smlouvě.

- **Bezpečnostní smlouva mezi vládou České republiky a vládou Řecké republiky o vzájemné ochraně vyměněných utajovaných informací**

  Smlouva byla v ČR ratifikována, nyní se čeká na oznámení řecké strany o splnění podmínek pro její vstup v platnost.

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

  Parlament ČR vyslovil souhlas s ratifikací.

2.2.1.2. Výhled na rok 2012

V roce 2012 Úřad předpokládá dokončení expertních jednání s Belgií, Tureckem, USA, Austrálií a Brazílií a dále zahájení jednání se Spojenými arabskými emiráty, Alžírskem, Irákem a Egyptem.

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 orgánů EU:

Orgány NATO

NATO
Bezpečnostní výbor (Security Committee-AC/35 – od roku 1998)
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)
Pracovní skupina AC35 pro přípravu instrukcí k uplatňování bezpečnostní politiky (Security Committee in Security Policy Format)
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
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

EU
Pracovní skupiny Implementation Tempest Task Force (ITTF) a Technical Tempest Task Force (TTTF) – Pracovní skupiny pro oblasti problematiky TEMPEST

Orgány NATO:

- **Bezpečnostní výbor** (Security Committee) 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** (WG/1 on Information Assurance) 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, 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.

- **Pracovní skupina AC35 pro přípravu instrukcí k uplatňování bezpečnostní politiky** (Security Committee in Security Policy Format) je odpovědná za přípravu, revidování a vytváření bezpečnostních politik NATO. Skupina doporučuje směrnice, nařízení a příručky prováděcích předpisů NATO v jednotlivých oblastech bezpečnosti.

- **Pracovní skupina IICWG** (International Interoperability Control Working Group) 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** (Council Security Committee 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** (Commission Security Policy Advisory Group) je orgánem, jehož hlavní úlohou je poskytovat Komisi poradní stanoviska ve věcech bezpečnostní politiky.

- **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** – 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)** – 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.

Pokud jde o Srbsko, v lednu 2011 proběhl seminář v oblasti bezpečnosti informačních technologií pro pracovníky srbského Národního bezpečnostního úřadu. V březnu 2011 proběhl expertní seminář v oblasti personální bezpečnosti, administrativní bezpečnosti a bezpečnosti informačních technologií pro pracovníky Kosovské zpravodajské služby. Pro kolegy z chorvatského Národního bezpečnostního úřadu pak Úřad uspořádal pracovní jednání, které se soustředilo na personální a průmyslovou bezpečnost a dále na opravné prostředky.

V červnu 2011 uspořádal Úřad konferenci pro zástupce národních bezpečnostních úřadů členských států Visegrádské skupiny (V4), Slovinska, NATO a EU. Hlavním tématem jednání byla ochrana utajovaných informací v zemích V4, opravné prostředky a kybernetická bezpečnost.

2.2.4. Ostatní mezinárodní aktivity Úřadu

Vzhledem k tomu, že Úřad získal nové pravomoci v oblasti kybernetické bezpečnosti, se pracovníci Úřadu aktivně účastnili konferencí a workshopů na toto téma. Úřad také zahájil jednání s NATO Cyber Defence Management Authority o memorandu o porozumění v oblasti kybernetické bezpečnosti.

V souvislosti s přesunem sídla Galileo Supervisory Authority (GSA) do ČR Úřad aktivně participoval na řešení bezpečnostních aspektů tohoto přesunu včetně negociace koordinačního ujednání s GSA o bezpečnosti.

2.3. Personální bezpečnost

Oblast personální bezpečnosti zahrnuje provádění bezpečnostního řízení u fyzických osob, provádění úkonů za účelem prověření, zda fyzická osoba, která je držitelem osvědčení fyzické osoby, i nadále splňuje podmínky pro jeho vydání, vydávání osvědčení fyzické osoby, vydávání rozhodnutí o nevydání osvědčení fyzické osoby a rozhodnutí o zrušení platnosti osvědčení fyzické osoby, vydávání osvědčení pro cizí moc, potvrzujících cizí moci vydání osvědčení fyzické osoby, a úkony s tím spojené, zakládání, vedení, doplňování, evidenci a vyřazování bezpečnostních svazků a vedení evidence fyzických osob, které jsou držiteli osvědčení fyzické osoby. Zahrnuje rovněž součinnost s orgány státu, právnickými osobami a dalšími subjekty, které disponují informacemi důležitými pro bezpečnostní řízení. Uvedené činnosti zajišťovaly v roce 2011 v Úřadu 4 samostatné organizační

celky začleněné do sekce bezpečnostního řízení (viz organizační strukturu v kapitole 3.4.).

Vzhledem ke zcela zásadní modifikaci legislativního rámce provádění bezpečnostního řízení a celé oblasti personální bezpečnosti, ke které došlo v rámci přijetí velké novely zákona a vydání nové vyhlášky č. 363/2011 Sb. s účinností od 1. ledna 2012, věnoval se Úřad ve druhé polovině roku 2011 také přípravě změn systému jejich zajištění a provádění a tyto změny realizoval tak, aby je mohl aplikovat ihned od 1. ledna 2012, aniž by došlo k ohrožení výkonu státní správy v oblasti personální bezpečnosti.

V roce 2011 byla, stejně jako v předchozích letech, věnována pozornost nejen průběžnému zlepšování již zavedených postupů, ale i vytváření nových efektivních procesů v rámci bezpečnostního řízení včetně metodického působení. V důsledku této činnosti Úřad realizoval požadavky na provádění bezpečnostních řízení v naprosté většině případů v kratších lhůtách, než jsou zákonem stanoveny. Pouze v jednotlivých případech bylo nezbytné, aby ředitel Úřadu, na základě informace od orgánu státu, právnické osoby nebo podnikající fyzické osoby, podle § 118 zákona tyto lhůty prodloužil.

Na základě zkušeností s uplatňováním postupů v bezpečnostním řízení, počínaje přijetím žádosti o vydání osvědčení fyzické osoby až po závěrečné rozhodnutí ve věci, byla dále upřesňována Metodika bezpečnostního řízení z roku 2008, a to zejména s ohledem na velkou novelu zákona. Úřad pro zaměstnance podílející se na provádění bezpečnostního řízení zorganizoval tematická školení ke specifickým otázkám, kterých se bezpečnostní řízení týká. Ke konci roku pak byli všichni zaměstnanci důkladně proškoleni v souvislosti s novelizací právní úpravy.

Součinnost, kterou v rámci bezpečnostního řízení poskytují Úřadu zpravodajské služby, Policie ČR a další spolupracující orgány státu a právnické osoby, byla i v roce 2011 na velmi dobré úrovni. V souladu s usnesením vlády ČR č. 1381 ze dne 12. prosince 2007 byla vzájemná spolupráce dále upravována. V průběhu roku byla uzavřena 1 realizační dohoda a 2 dodatky k již dříve uzavřeným dohodám. Jednalo se o Dohodu o poskytování informací s Generální inspekcí bezpečnostních sborů ze dne 28. prosince 2011, Dodatek č. 3 k Realizační dohodě ze dne 28. ledna 2008 o poskytování informací mezi Úřadem a Ministerstvem vnitra a Policií české republiky ze dne 22. prosince 2011 a Dodatek č. 3 k Realizační dohodě ze dne 25. ledna 2008 upravující poskytování údajů mezi Úřadem a společností LLCB, z. s. p. o. ze dne 17. října 2011. Koncem roku byly zahájeny činnosti na přípravě dodatků k dalším realizačním dohodám, a to v souvislosti se změnami, které přináší zákon č. 255/2011 Sb. (jedná se především o dohody, které upravují spolupráci se zpravodajskými službami).

Jako efektivní pro urychlení bezpečnostního řízení se také projevila komunikace pomocí datových schránek s účastníkem řízení a s ostatními spolupracujícími subjekty z veřejné i privátní sféry, se kterými nemá Úřad zavedenu komunikaci kryptovaně zabezpečenou elektronickou formou. V této souvislosti lze zejména zmínit komunikaci s bankami.

Další oblastí činnosti byla spolupráce Úřadu s úřady cizí moci, které mají v působnosti ochranu utajovaných informací, při provádění vlastních bezpečnostních řízení (vyžadování informací). Úřad u partnerských úřadů vyžádal informace k 141 osobě a na základě jejich žádostí prováděl šetření k 26 osobám, které byly v daném státě prověřovány pro přístup k utajovaným informacím.

Oproti roku 2010 došlo v loňském roce ke snížení počtu podaných žádostí o vydání osvědčení fyzické osoby. Úřad přijal celkem 2.538 žádostí.

V roce 2011 bylo ve 46 případech bylo rozhodnuto o nevydání osvědčení a ve 308 případech bylo bezpečnostní řízení zastaveno. V roce 2011 bylo rovněž přijato 84 žádostí o ověření splnění podmínek přístupu fyzické osoby k utajované informaci stupně utajení Vyhrazené.

Velkou část objemu činnosti Úřadu v oblasti personální bezpečnosti (4.824 případů) v roce 2011 činilo provádění prověřování, zda fyzická osoba, která je držitelem osvědčení fyzické osoby, i nadále splňuje podmínky pro jeho vydání. Toto prověřování bylo standardně prováděno 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 nebo je Úřad získal přímo svou vlastní činností (např. z průběžného monitoringu tzv. otevřených zdrojů). V 249 případech toto prověřování vyústilo v zahájení řízení o zrušení platnosti osvědčení fyzické osoby, které bylo v 96 případech ukončeno vydáním rozhodnutí o zrušení platnosti osvědčení fyzické osoby (tyto údaje nejsou promítnuty v kapitole 2.3.1. Statistické přehledy).

2.3.1. Statistické přehledy

Přijaté žádosti a ukončená bezpečnostní řízení v roce 2011

	Důvěrné	Tajné	Přísně tajné	Celkem
Přijaté žádosti	1.208	1.174	156	**2.538**
Osvědčení vydáno	1.620	2.028	263	**3.911**
Osvědčení nevydáno	18	27	1	**46**
Řízení zastaveno	93	136	79	**308**

Přijaté žádosti o vydání osvědčení fyzické osoby v letech 2008 až 2011

Vydaná osvědčení fyzické osoby v letech 2008 až 2011

Přijaté žádosti o ověření splnění podmínek pro přístup fyzické osoby k utajované informaci stupně utajení Vyhrazené v letech 2008 až 2011, včetně ověření podmínek podle § 9 odst. 2 zákona

Ukončená bezpečnostní řízení v roce 2011

Ukončená bezpečnostní řízení v letech 2008 až 2011

Vydaná osvědčení fyzické osoby pro cizí moc v roce 2011

COSMIC TOP SECRET	332
COSMIC TOP SECRET ATOMAL	44
NATO SECRET	1.594
NATO SECRET ATOMAL	7
NATO CONFIDENTIAL	554
WEU FOCAL TOP SECRET	26
WEU SECRET	16
WEU CONFIDENTIAL	24
CELKEM	**2.597**

Vydaná osvědčení fyzické osoby pro cizí moc v letech 2008 až 2011

2.3.2. Analýza důvodů nevydání nebo zrušení platnosti osvědčení fyzické osoby

Převládajícím důvodem pro nevydání nebo zrušení platnosti osvědčení fyzické osoby bylo, jako v roce minulém, 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 zahrnuje poměrně velký rozsah faktických důvodů, které byly při jeho shledání Úřadem odvislé zejména od skutečností vyplývajících např. z trestního či přestupkového řízení, a dále širokého spektra případů porušování právních předpisů a interních normativních aktů nebo jejich obcházení, kdy převážnou motivací zde bylo získání majetkového či jiného prospěchu. K nesplnění bezpečnostní spolehlivosti fyzické osoby náležely především případy, kdy se účastníci řízení (žadatelé či držitelé osvědčení) se svým přístupem k plnění svých závazkových vztahů ocitli v neudržitelné finanční, potažmo majetkové situaci, kterou řešili přistupováním k novým závazkům již s vědomím předchozí nesplácet, což může mít až fatální dopad na jejich schopnost, resp. ochotu utajovat informace, jako možné protislužby nebo nabídky, ve vazbě na případné zlepšení jejich stávajících majetkových poměrů. Tyto případy většinou doprovázela rovněž neochota účastníků řízení takové finanční problémy Úřadu vůbec uvést, potažmo objasnit. Za určitých okolností byly tyto skutečnosti klasifikovány také jako bezpečnostní riziko podle § 14 odst. 3 písm. i) zákona – zřejmě nepřiměřené finanční nebo majetkové poměry vzhledem k řádně přiznaným příjmům fyzické osoby, zejména v případech, kdy má účastník řízení majetek, jehož nabytí není schopen prokázat, popřípadě takové závazky, jejichž účel není schopen zdůvodnit.

Ostatní rizika uvedená v § 14 odst. 2 a 3 zákona byla konstatována pouze u jednotlivých případů.

Dalším stále vzrůstajícím důvodem nevydání či zrušení platnosti osvědčení fyzické osoby bylo nesplnění podmínky bezúhonnosti podle § 6 odst. 2 písm. c) zákona. Také v roce 2011 výrazně vzrostl počet případů, kdy fyzická osoba nesplňovala podmínku bezúhonnosti (nebo ji přestala splňovat v době platnosti osvědčení fyzické osoby) z důvodu pravomocného odsouzení za spáchání úmyslného trestného činu v souvislosti s jízdou motorovým vozidlem pod vlivem návykové látky.

2.3.3. Personální projekt

V souladu s § 72 zákona již pošesté předložila ministerstva a další ústřední správní úřady své personální projekty. Obecně lze konstatovat, že se tak jako v minulém roce při jejich zpracování pozitivně projevila snaha vyhovět účelu zákona a metodická činnost Úřadu zaměřená na tuto oblast.

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 práce, neboť jiný důvod přístupu k utajované informaci nelze akceptovat.

V roce 2011 bylo vyjádření Úřadu k personálním projektům předloženo do připomínkového řízení dotčeným ministerstvům a orgánům státní správy. Největší počet žádostí na rok 2012 je plánován rezortem Ministerstva obrany, a to v celkovém počtu 3.200 žádostí. Většinu 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 14. prosince 2011 a vydala usnesení č. 926, 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 2011 Úřad také vedl, ve smyslu části čtvrté zákona, bezpečnostní řízení k žádostem o vydání dokladu o bezpečnostní způsobilosti fyzických osob (dále jen „doklad“). Naprostou většinu podaných žádostí 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, a to v oblasti zadávání veřejných zakázek. Dnem 12. září 2011 totiž nabyl účinnosti zákon č. 258/2011 Sb., kterým se mění zákon č. 137/2006 Sb., o veřejných zakázkách, ve znění pozdějších předpisů, který v § 157a nově stanovil za citlivou činnost podle zákona činnost při zadávání veřejné zakázky veřejným zadavatelem podle § 2 odst. 2 písm. a) a b) zákona č. 137/2006 Sb., jejíž předpokládaná hodnota přesáhne 300 mil. Kč.

Významnou částí náplně činnosti Úřadu v oblasti bezpečnostní způsobilosti je rovněž průběžné ověřování splnění podmínek pro vydání dokladu u jeho držitelů.

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.

Postupy zaměstnanců Úřadu a úkony v rámci bezpečnostního řízení prováděného na základě žádosti o vydání dokladu, prověřování splnění podmínek pro vydání dokladu u jeho držitelů, bezpečnostní řízení o zrušení platnosti dokladu a úkony s tím spojené, jsou metodicky usměrňovány Metodikou bezpečnostního řízení uvedenou v kapitole 2.3.

Z důvodu zabezpečení řádného výkonu státní správy v oblasti bezpečnostní způsobilosti po 31. prosinci 2011 v souvislosti se zásadní novelou zákona a vydáním vyhlášky č. 363/2011 Sb. byly také v této oblasti ve druhé polovině roku 2011 připravovány změny systému zajištění a provádění činností, které oblast bezpečnostní způsobilosti zahrnuje. Úřad připravil realizaci těchto změn tak, aby je ihned od 1. ledna 2012 bylo možné aplikovat.

V roce 2011 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, jako je tomu např. v souvislosti s nově vzniklou citlivou činností v oblasti veřejných zakázek.

2.4.1. Statistické přehledy

Přehled přijatých žádostí a ukončených bezpečnostních řízení v roce 2011

Citlivá činnost podle	Přijaté žádosti	Doklad vydán	Doklad nevydán	Řízení zastaveno	Zrušení platnosti dokladu
§ 8 zákona č. 38/1994 Sb.[1]	71	79	0	6	1
§ 2a zákona č. 18/1997 Sb.[2]	50	155	0	0	1
§ 5 zákona č. 310/2006 Sb.[3]	11	10	0	0	0
§ 25c odst. 10 zákona č. 61/1988 Sb.[4]	2	3	0	0	0
§ 157a zákona č. 137/2006 Sb.[5]	2	0	0	0	0
Ostatní	16	8	0	15	3
Celkem	**152**	**255**	**0**	**21**	**5**

2.5. Průmyslová bezpečnost

V oblasti průmyslové bezpečnosti Úřad zabezpečoval provádění bezpečnostního řízení o žádostech podnikatelů, vydávání osvědčení podnikatele, vydávání osvědčení podnikatele pro cizí moc, potvrzující cizí moci vydání osvědčení podnikatele, vydávání rozhodnutí o nevydání osvědčení podnikatele, vydávání rozhodnutí o zrušení platnosti osvědčení podnikatele a úkony s těmito činnostmi spojené.

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

---

[1] § 8 zákona 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.
[2] 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.
[3] 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.
[4] Zákon č. 61/1988 Sb., o hornické činnosti, výbušninách a o státní báňské správě, ve znění pozdějších předpisů.
[5] Zákon č. 137/2006 Sb., o veřejných zakázkách, ve znění pozdějších předpisů.

Přijetím velké novely zákona a vydáním nové vyhlášky č. 405/2011 Sb. došlo k zásadní modifikaci legislativního rámce provádění bezpečnostního řízení, s účinností od 1. ledna 2012. Proto se zejména ve druhém pololetí 2011 Úřad také organizačně připravoval na zavedení obsahu nové právní úpravy do praktických činností v oblasti průmyslové bezpečnosti tak, aby ji ihned od 1. ledna 2012 mohl aplikovat, aniž by došlo k ohrožení výkonu státní správy v oblasti průmyslové bezpečnosti.

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 kapitolu 2.3.).

2.5.1. Bezpečnostní řízení o žádosti podnikatele

V průběhu roku 2011 bylo Úřadem přijato 136 žádostí podnikatelů o vydání osvědčení podnikatele. Z tohoto počtu bylo k 31. prosinci 2011 rozhodnuto o 66 žádostech, u zbylých 70 žádostí k tomuto datu bezpečnostní řízení o žádosti podnikatele probíhala. Výrazným faktorem ovlivňujícím počty podaných žádostí je dynamika podnikatelského prostředí (vznik nových obchodních společností a přeměny obchodních společností – podnikatelů, kteří přejímají realizace zakázek obsahujících utajované informace po společnostech, jež tímto způsobem trh uvolnily).

Počet podaných žádostí včetně stupně požadovaného osvědčení podnikatele především ve druhé polovině roku 2011 ovlivnilo předpokládané nabytí účinnosti velké novely zákona k 1. lednu 2012. Velká novela zákona výrazným způsobem upravuje přístup podnikatelů k utajovaným informacím stupně utajení Vyhrazené. Podle nové právní úpravy již přístup podnikatele pouze k utajované informaci stupně utajení Vyhrazené nebude podmíněn držením osvědčení podnikatele. Tato skutečnost se promítla i do přijatých žádostí, a to zásadním snížením počtu podaných nových žádostí podnikatelů na stupeň utajení Vyhrazené a naopak navýšením počtu žádostí o vydání osvědčení podnikatele pro přístup k vyšším stupňům utajení, a to právě o podnikatele, kteří byli držiteli osvědčení podnikatele na stupeň utajení Vyhrazené.

Stejně jako v předchozím období se do počtu podaných žádostí promítaly důsledky celosvětové ekonomické recese.

Úřad v roce 2011 vydal celkem 191 osvědčení podnikatele. Tento počet zahrnuje osvědčení vydaná na základě provedeného bezpečnostního řízení o žádosti podnikatele o vydání osvědčení podnikatele podle § 96 zákona i osvědčení vydaná postupem podle § 56 odst. 4 zákona.

2.5.2. Statistické přehledy

Přijaté žádosti o vydání osvědčení podnikatele v roce 2011

Vyhrazené	Důvěrné	Tajné	Přísně tajné	Celkem
31	76	28	1	**136**

Stav zpracování žádostí o vydání osvědčení podnikatele přijatých v roce 2011

Osvědčení vydáno	Osvědčení nevydáno	Řízení zastaveno	Probíhalo k 31.12.2011	Celkem
55	1	10	70	**136**

Vydaná osvědčení podnikatele v roce 2011

Vyhrazené	Důvěrné	Tajné	Přísně tajné	Celkem
76	89	26	0	**191**

Řízení o zrušení platnosti osvědčení podnikatele v roce 2011

Celkem zahájeno	Platnost zrušena	Řízení zastaveno	Probíhalo k 31.12.2011
52	27	13	12

Přijaté žádosti o vydání osvědčení podnikatele v letech 2008 až 2011

2.5.3. Analýza důvodů nevydání osvědčení podnikatele

V roce 2011 rozhodl Úřad v 1 bezpečnostním řízení o žádosti podnikatele o nevydání osvědčení podnikatele. Důvodem nevydání osvědčení bylo nesplnění podmínky podle § 16 odst. 1 písm. b) zákona.

Za totéž období Úřad rozhodl ve 34 případech o zrušení platnosti osvědčení podnikatele. Důvody a počty zrušených osvědčení podnikatele lze charakterizovat následovně:

- nesplnění podmínky podle § 16 odst. 1 písm. a) zákona – 3 případy,
- nesplnění podmínky podle § 16 odst. 1 písm. b) zákona – 3 případy,
- nesplnění podmínky podle § 16 odst. 1 písm. c) zákona – 3 případy,
- nesplnění podmínky podle § 16 odst. 1 písm. d) zákona – 20 případů,
- kombinace nesplnění více podmínek současně – 5 případů.

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 zjišťuje způsobilost zabezpečených oblastí a objektů k ochraně před únikem utajovaných informací kompromitujícím vyzařováním. Do této oblasti činnosti patří také certifikace stínicích komor.

Úřad odpovídá za rozvoj kryptologie a základní i aplikovaný výzkum v oblasti kryptografie, kryptoanalýzy, bezpečnosti informačních systémů a kompromitujícího vyzařování.

V roce 2011 Úřad zpracoval a vydal v rámci dalšího rozvoje bezpečnostních standardů nový bezpečnostní standard NBÚ - 1/2011, Podmínky provozu kryptografických prostředků TCE 621 IP, TCE 621/B, TCE 621/C a TCE 671, verze 1.0, novou verzi 2.0. bezpečnostního standardu NBÚ - 2/2007, Instalace zařízení z hlediska kompromitujícího elektromagnetického vyzařování, a nový bezpečnostní standard NBÚ - 2/2011, Obranné prohlídky, Kontrola zabezpečených oblastí z hlediska úniku informací prostřednictvím kompromitujícího vyzařování.

Zpracován byl rovněž bezpečnostní standard upravující oblast bezpečného vymazávání informací z počítačových médií, který bude vydán na začátku roku 2012, a byly zahájeny práce na několika dalších bezpečnostních standardech. Bezpečnostní standardy jsou poskytovány v souladu s jejich stupněm utajení a s uplatněním zásady „need-to-know.

Průběžně byly zpracovávány metodické materiály zabývající se dílčími problémy zabezpečení informačních systémů, nastavením bezpečnostních charakteristik nejčastěji používaných operačních systémů a aktuálními problémy zástavby kryptografických prostředků do mobilních systémů pro zahraniční mise Armády ČR. Metodické materiály jsou zveřejňovány nebo poskytovány žadatelům o certifikaci podle skutečné potřeby.

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 2011 dalších 118 žádostí, včetně žádostí o opakovanou certifikaci, a to jak ze státní správy, tak ze soukromé sféry. Bylo vydáno 122 certifikátů informačních systémů, z toho 73 na žádost podanou v roce 2011. Z celkového počtu certifikátů vydaných v roce 2011 se jednalo pouze ve 33 případech o první certifikaci informačního systému, z toho 12 ze státní správy. V 15 případech provozovatel informačního systému s certifikátem platným do roku 2011

nepožádal již o opakovanou certifikaci a platnost certifikátu automaticky skončila. Celkem v 11 případech byl proces certifikace ukončen bez vydání certifikátu, a to vesměs z vůle žadatele o certifikaci, pro nesplnění podmínek pro získání osvědčení podnikatele nebo skončením platnosti osvědčení podnikatele během certifikačního řízení.

Certifikace informačních systémů v roce 2011

Přijaté žádosti	Ukončeno bez vydání certifikátu nebo uplynutím doby platnosti certifikátu		Vydané certifikáty	
	státní správa	podnikatelé	státní správa	podnikatelé
118	5	21	60	62

Přijaté žádosti o certifikaci informačního systému v letech 2006 až 2011

Vydané certifikáty informačních systémů v letech 2006 až 2011

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 2011 přibylo pouze 10 žádostí o certifikaci nově budovaného informačního systému ze státní správy (podobně jako v roce 2010) a 22 žádostí ze soukromého sektoru. To svědčí o trendu pozorovaném již v loňském roce, kdy informační systémy pro zpracování utajovaných informací jsou již většinou provozovány po více než jedno období platnosti certifikátu informačního systému. V rámci opakovaných certifikací již provozovaných informačních systémů byly 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 rostla, a to způsobem nesnižujícím úroveň jejich zabezpečení.

V roce 2011, kromě opakované certifikace menších informačních systémů v několika ministerstvech a úřadech, ve 12 krajských nebo městských úřadech či ve 2 případech v Parlamentu ČR, proběhla opakovaná certifikace řady významných informačních systémů státní správy, např. 8 informačních systémů Ministerstva obrany, 2 informačních systémů Ministerstva vnitra (včetně Vega-T), informačních systémů 2 policejních útvarů s celorepublikovou působností, 2 rozsáhlých informačních systémů Ministerstva zahraničních věcí a několika klíčových informačních systémů všech 3 zpravodajských služeb ČR.

V roce 2011 Úřad zajistil pro Ministerstvo obrany a zpravodajské služby národní akreditaci lokalit 3 systémů NATO, nutnou pro schválení jejich dalšího připojení ke klasifikovaným sítím NATO po realizovaných změnách (ICC, BICES a TUMBA3), pro Ministerstvo vnitra národní akreditaci lokality informačního systému BdL po jejím přemístění (součinnost zemí EU) a pro Ministerstvo zahraničních věcí pokračování národní akreditace součinnostního systému EU Extranet-R. Zároveň byla příslušným orgánům NATO a 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.

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.

2.6.1.2. Certifikace kryptografických prostředků

V roce 2011 bylo Úřadu podáno celkem 7 žádostí o certifikaci kryptografického prostředku. V řízeních k certifikaci kryptografického prostředku bylo vydáno celkem 8 certifikátů, 1 řízení bylo ukončeno bez vydání certifikátu. Přitom významný podíl pracovní kapacity pracoviště certifikace kryptografických prostředků byl zaměřen na certifikaci kryptografických prostředků vyvíjených ČR. Stav řízení je shrnut v následující tabulce.

Certifikace kryptografických prostředků v roce 2011

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
7	0	10	0	1	3	6	7	7

Přijaté žádosti o certifikaci kryptografického prostředku v letech 2006 až 2011

Vydané certifikáty kryptografických prostředků v letech 2006 až 2011

Úřad provedl opakovanou certifikaci kryptografických prostředků TCE 621/B, TCE 621/C, KRYDAT E1VX, SPIDER a SECTEL. Nově byly certifikovány kryptografické prostředky PCS1 a RF1302S (radiostanice). Nebyla vyžadována opakovaná certifikace kryptografického prostředku ECHINOPS. Zastavena byla certifikace kryptografického prostředku RF20S.

V návaznosti na nové poznatky k provozu byly upraveny, formou doplňku, certifikační zprávy kryptografických prostředků HCryptW, KRYDEC XP_04 a kryptografické prostředky třídy TCE 621.

Úřad vydal schválení pro aplikaci využívající kryptografický prostředek třídy HCrypt a pro provedené speciální zástavby kryptografického prostředku ELCRODAT 4-2 a kryptografické prostředky třídy TCE 621 do mobilních armádních systémů.

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 národní, EU a NATO v hlasové formě. Početně významné zastoupení mají kryptografické prostředky pro ochranu utajovaných informací v prostředí IP sítí, nadále však zůstávají zachovány 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 RF1302S, eCustodian, TCE 621 IP, TCE 621/B, TCE 621/C a TCE 121 KPE.

2.6.1.3. Certifikace kryptografických pracovišť

Většina žádostí o certifikaci kryptografických pracovišť spadá do kategorie opakovaných žádostí. 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 2011

	Přijaté žádosti	Rozpracováno	Certifikováno	Zamítnuto
Státní správa	4	0	4	0
Podnikatelé	0	0	0	0
Celkem	**4**	**0**	**4**	**0**

Přijaté žádosti o certifikaci kryptografického pracoviště v letech 2006 až 2011

Vydané certifikáty kryptografických pracovišť v letech 2006 až 2011

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 22 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 oblastí v 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 2011 bylo v Úřadu vygenerováno celkem 82.705 kryptografických klíčů a hesel uložených na 7.188 nosičích různých typů a dalších 119 kusů jiného kryptografického materiálu (procesory, paměti, kryptografická dokumentace, instalační a šifrovací SW).

Úřad vzal do evidence a provedl distribuci celkem 1.442 ks nového kryptografického a CCI materiálu a dále zajistil servis a opravy na území ČR u 63 ks kryptografických prostředků a mimo ČR u 22 ks kryptografických prostředků.

Pro přehled nosičů klíčového materiálu kryptografického prostředku KRYDEC byly vytvořeny technické podmínky k evidenci těchto nosičů pomocí čárového kódu. Ve spolupráci s Ministerstvem obrany byly smluvně nastaveny postupy pro bezpečnou likvidaci kryptografických prostředků pro celou státní správu.

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 2011 TEMPEST měření podle standardů NATO řady SDIP, EU řady IASG 04 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 2011 hodnoceno více než 50 zařízení. Z toho bylo prováděno TEMPEST měření více než 10 ks zařízení STEP, EUROTEMPEST a Siltec, a to jako samostatného zařízení nebo v kombinaci s kryptografickým prostředkem KRYDEC. 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 2011 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 2011, je uveden v následující tabulce:

Měřená zařízení a objekty v roce 2011

Typ měření[6]	Počet
Zónové měření	20 objektů + vojenské kontejnery
Kryptografické prostředky	1 typ
PC sestavy	3 typy – třída 0; přes 10 typů – třída 1 a 2
Audio technika	2 typy zařízení
Obranné prohlídky	4 objekty
Mobilní systémy	2 systémy

2.6.2.3. Schvalování projektů bezpečnosti komunikačních systémů

V roce 2011 byl opakovaně schválen projekt bezpečnosti 1 komunikačního systému provozovaného Ministerstvem obrany. Naopak byla ukončena činnost 2 komunikačních systémů (v Ministerstvu obrany a Ministerstvu vnitra) v souvislosti s ukončením platnosti certifikátu příslušného již zastaralého kryptografického prostředku. Nové žádosti o schválení projektu bezpečnosti komunikačního systému nebyly v roce 2011 podány.

Na podporu efektivního plnění úkolů státní správy Úřad v roce 2011 nadále zajišťoval správu komunikačního systému MODUS využívajícího certifikovaných kryptografických prostředků SECTRA Tiger XS (přídavný kryptografický modul

[6] 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 vnitra.

k mobilnímu telefonu), umožňujících mobilní telefonii pro utajované informace do stupně utajení Tajné. Úřad provozuje středisko pro řízení vzniklé komunikační sítě určené pro vrcholové představitele státu a rovněž pro řízení rezortních sítí konfigurovaných podle vlastního návrhu rezortu.

Komunikační systém vládního utajovaného spojení založený na použití kryptografických prostředků Sectel 9600 Toro je v současné době 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, pokračuje připojování dalších lokalit určených nařízením vlády. Kontrol se účastní i pracovníci Úřadu.

2.6.2.4. Školení pracovníků kryptografické ochrany a zkoušky odborné způsobilosti

Úřad v roce 2011 organizačně zajistil a provedl, v souladu se zákonem, celkem 10 školení skupin pracovníků kryptografické ochrany a po zkoušce odborné způsobilosti vydal 103 osvědčení o zvláštní odborné způsobilosti pracovníka kryptografické ochrany. Kromě toho probíhají další školení na Ministerstvu vnitra, Ministerstvu obrany a Ministerstvu zahraničních věcí na základě smluv uzavřených mezi Úřadem a uvedenými ministerstvy. Úřad v roce 2011 schvaloval aktualizaci osnov a obsahu některých kurzů.

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

Větší část problémů při zabezpečování zákonem stanovených činností Úřadu v oblasti kryptografické ochrany a certifikace informačních systémů nakládajících s utajovanými informacemi uvedených ve zprávě o činnosti Úřadu za rok 2010 se v roce 2011 podařilo vyřešit.

- Vzhledem k tomu, že v roce 2011 byla schválena velká novela zákona, je již používání označení určitého typu kryptografického materiálu jako „kontrolovaná kryptografická položka“ (CCI) zavedeno do právního řádu ČR, a je tedy možné dopracovat prozatímní bezpečnostní standard do konečné podoby. Podobně již v české legislativě nechybí pojem „taktická informace“ umožňující využívat pro ochranu určitého typu utajovaných informací (zejména informací krátkodobého významu) levnější kryptografické prostředky.

- V roce 2011 se opětovně podařilo kvalitně obsadit všechna přidělená pracovní místa pro činnosti Úřadu uložené mu zákonem v oblasti bezpečnosti informačních systémů a kryptografické ochrany.

- Ke dni účinnosti velké novely zákona a nové vyhlášky č. 432/2011 Sb., o zajištění kryptografické ochrany utajovaných informací, se nepodařilo zpracovat všechny požadované bezpečnostní standardy (např. pro taktickou informaci.

- Národní certifikace některých kryptografických prostředků, vyvinutých a certifikovaných v některé 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, potřebných pro provedení certifikace Úřadem.

- Z hlediska zajištění praktické ochrany utajovaných informací v informačních nebo komunikačních systémech a zajištění kryptografické ochrany byl v celé státní správě i v roce 2011 problémem nedostatek odborníků v oboru informačních technologií, splňujících podmínky pro přístup k utajované informaci stupně utajení Důvěrné, Tajné nebo Přísně tajné. Důsledkem je, že stejné osoby zastávají funkce ve správě a bezpečnostní správě několika informačních nebo komunikačních systémů nebo více funkcí v určitém informačním systému. Pozitivním momentem je, že již byl naplňován požadavek NATO a EU, aby v klíčových rolích ve správě informačních systémů nakládajících s utajovanými informacemi NATO a EU působily osoby prověřené pro přístup k utajovaným informacím o stupeň vyšším, nežli je stupeň utajení v daném systému zpracovávaných utajovaných informací.

2.7. Administrativní a fyzická bezpečnost, ústřední registr

2.7.1. Administrativní bezpečnost

Na základě žádostí podnikatelů o vydání osvědčení podnikatele bylo z hlediska administrativní bezpečnosti posuzováno vytvoření podmínek pro označování, evidenci, zapůjčování, ukládání, přepravu, další manipulaci a vyřazování utajované informace v souladu se zákonem a příslušným prováděcím právním předpisem.

Posouzené bezpečnostní dokumentace a realizované dohlídky v roce 2011

Bezpečnostní dokumentace	Realizované dohlídky
30	22

Bezpečnostní dokumentace posouzené v letech 2006 až 2011

V průběhu roku 2011 Úřad požádaly 2 subjekty, které přechodně přestaly splňovat zákonné podmínky pro přístup k utajované informaci, o dočasné uložení utajovaných dokumentů. Důvodem byl zánik platnosti osvědčení podnikatele a změna dislokace zabezpečené oblasti.

2.7.1.1. Problémové oblasti administrativní bezpečnosti

- vedení administrativních pomůcek určených pro evidenci utajovaných dokumentů,
- manipulace s utajovanými dokumenty stupně utajení Vyhrazené.

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 realizoval:

- činnosti spojené s členstvím v certifikační radě TrezorTestu (účast na výrobních auditech u 6 firem v rámci ČR, účast na certifikačních radách a účast při provádění zkoušek na mechanických zábranných systémech dle příslušných norem);
- účast v technické normalizační komisi (TNK124) pro EZS a EPS při zavádění evropských norem a aktualizaci stávajících norem;
- provádění metodické pomoci v rámci certifikace technických prostředků, dále v souvislosti se zástavbou technických prostředků v objektech a zabezpečených oblastech a spolupráce se subjekty při tvorbě návrhů opatření fyzické bezpečnosti v těchto prostorách.

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 2011 přijal celkem 170 žádostí o certifikaci pro 485 technických prostředků. V rámci posuzovaní a vyhodnocování podkladů pro certifikaci bylo u 36 % žádostí vyžádáno jejich doplnění a upřesnění. V 31 případech byl certifikační proces ukončen bez vydání certifikátu, a to především z důvodu podání žádosti o certifikaci výrobku, který certifikaci nepodléhá.

Úřad vydal celkem 444 certifikátů technických prostředků. Rozdíl mezi počtem podaných žádostí a počtem vydaných certifikátů je způsoben slučováním více technických prostředků obdobných vlastností na jeden certifikát. K 1. lednu 2012 zbývalo posoudit ještě 12 žádostí o certifikaci pro 29 technických prostředků, které byly Úřadu zaslány v prosinci 2011. Počty vydaných certifikátů technických prostředků podle jednotlivých skupin definovaných zákonem jsou uvedeny v následující tabulce.

Vydané certifikáty technických prostředků v roce 2011

Technické prostředky	Vydané certifikáty
Mechanické zábranné prostředky[7]	122
Elektrická zámková zařízení, systémy pro kontrolu vstupů[8]	13
Zařízení elektrické zabezpečovací signalizace a tísňové systémy[9]	204
Speciální televizní systémy[10]	35
Zařízení elektrické požární signalizace[11]	5
Zařízení sloužící k vyhledávání nebezpečných látek nebo předmětů[12]	6
Zařízení fyzického ničení nosičů informací[13]	56
Zařízení proti pasivnímu a aktivnímu odposlechu utajované informace[14]	0
Celkem	**441**

[7] § 30 odst. 1 písm. a) zákona.
[8] § 30 odst. 1 písm. b) zákona.
[9] § 30 odst. 1 písm. c) a e) zákona.
[10] § 30 odst. 1 písm. d) zákona.
[11] § 30 odst. 1 písm. f) zákona.
[12] § 30 odst. 1 písm. g) zákona.
[13] § 30 odst. 1 písm. h) zákona.
[14] § 30 odst. 1 písm. i) zákona.

Certifikáty technických prostředků v roce 2011

Certifikace technických prostředků v letech 2006 až 2011

Kromě certifikátů uvedených v tabulce a grafech byly v roce 2011 dále, na základě podaných žádostí, vydány 3 certifikáty pro jednotlivé technické prostředky – uživatelské certifikáty. Tyto žádosti podávají uživatelé, kteří si zajistí vlastní posudek na konkrétní technický prostředek nasazený pro ochranu utajovaných informací. Vývoj počtu vydaných uživatelských certifikátů technických prostředků v období účinnosti zákona zobrazuje následující graf.

Uživatelské certifikáty technických prostředků v letech 2006 až 2011

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. V rámci certifikačního postupu Úřadu byl aktualizován zkušební postup na odolnost cylindrických vložek proti SG metodě.

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 2011 přijato celkem 71 žádostí o stanovisko k bezpečnostní dokumentaci podnikatele z hlediska zajištění ochrany utajovaných informací fyzickou bezpečností. Při posuzování dokumentací byla v 54 % případů provedena konzultace s podnikatelem v Úřadu nebo přímo v sídle podnikatele. Bylo posouzeno 65 bezpečnostních dokumentací podnikatele a bylo provedeno 35 tzv. dohlídek, při kterých byla v sídle podnikatele ověřena jeho schopnost zabezpečit ochranu utajovaných informací z hlediska fyzické bezpečnosti. K 1. lednu 2012 zbývá posoudit 6 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 2011

	Vyhrazené	Důvěrné	Tajné	Přísně tajné	Celkem
Přijaté žádosti	19	39	13	0	**71**
Posouzené dokumentace	19	35	11	0	**65**

2.7.2.3. Problémové oblasti fyzické bezpečnosti

Certifikace technických prostředků:

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

Posuzování projektů fyzické bezpečnosti:

- struktura předkládaných projektů fyzické bezpečnosti nesplňující požadavky příslušných právních předpisů a z toho plynoucí chyby při skutečné realizaci zabezpečení objektů a zabezpečených oblastí.

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

- nedostatky ve zpracování projektů fyzické bezpečnosti,
- nedostatky při instalaci mechanických zábranných prostředků (neukotvení úschovných objektů, zaměňování způsobu otevírání dveří u zabezpečených oblastí, nezabezpečení průlezných otvorů),

- nedostatky při instalaci poplachových zabezpečovacích a tísňových systémů (chybné umístění jednotlivých prvků, nefunkčnost systémů kontroly vstupu).

2.7.3. Ústřední registr

Prostřednictvím ústředního registru je realizováno poskytování utajovaných informací v rámci mezinárodní spolupráce. V roce 2011 vykonával ústřední registr evidenci a ukládání těchto utajovaných informací. Zejména se jednalo o utajované informace NATO. V průběhu roku došlo, vzhledem k celkové mezinárodní situaci, k výraznému navýšení počtu evidovaných dokumentů stupně utajení Tajné. U vybraných dokumentů ústřední registr prováděl jejich distribuci podřízeným registrům utajovaných informací, zřízeným v rámci ústředních orgánů státní správy a právnických osob.

Utajované dokumenty NATO evidované v ústředním registru

NATO	2007	2008	2009	2010	2011	Celkem
Neutajované	138	163	299	212	235	**1.047**
Vyhrazené	49	1.921	6.058	4.869	4.092	**16.989**
Důvěrné	720	1.102	1.440	1.026	1.433	**5.721**
Tajné	514	655	719	2.858	5.774	**10.520**
Přísně tajné	0	0	1	0	0	**1**
Celkem	**1.421**	**3.841**	**8.517**	**8.965**	**11.534**	**34.278**

Utajované dokumenty NATO evidované v ústředním registru

Kromě výše uvedených utajovaných dokumentů NATO jsou v ústředním registru evidovány utajované dokumenty EU (pouze pro potřebu Úřadu) a utajované dokumenty ostatních smluvních stran.

V rámci kontrolní činnosti ústředního registru bylo, podle § 79 odst. 6 zákona, provedeno 23 kontrol podřízených registrů utajovaných informací včetně ATOMAL registrů. V rámci metodického řízení byla v roce 2011 provedena školení vedoucích

podřízených registrů a ATOMAL registrů, která byla zaměřena na bezpečnost utajovaných informací cizí moci.

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

Ústřední registr rovněž ověřoval splnění podmínek nezbytných pro zřízení registru utajovaných informací u subjektů, které podaly žádost o zřízení registru utajovaných informací cizí moci. Ke konci roku 2011 bylo zřízeno celkem 43 registrů utajovaných informací.

Jako každý rok byly provedeny inventury utajovaných dokumentů v ústředním registru i v jemu podřízených registrech v ČR. Na jejich základě byla zaslána zpráva o provedené kontrole Bezpečnostnímu úřadu NATO.

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. Opravné prostředky

2.8.1. Bezpečnostní řízení

V roce 2011 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 fyzické osoby nebo osvědčení podnikatele,
- rozhodnutí o zrušení platnosti osvědčení 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.

2.8.1.1. Statistické přehledy

2.8.1.1.1. Rozklady

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

Rok	Dosud nerozhodnuto	Vyhověno	Zamítnuto	Zastaveno	Celkem
2010	0	13	34	1	**48**
2011	5	6	22	3	**36**

Rozklady proti rozhodnutím Úřadu v oblasti bezpečnostního řízení v letech 2006 až 2011

* 5 podání z roku 2011 dosud nebylo rozhodnuto

Řízení o rozkladu v roce 2011

Řízení o rozkladu v letech 2006 – 2011

2.8.1.1.2. Žaloby správní

Žaloby proti rozhodnutím ředitele Úřadu o rozkladu (2006 – 2011)
(rozhoduje Městský soud v Praze)

Celkem	Dosud nerozhodnuto	Řízení zastaveno	Vyhověno	Zamítnuto	Odmítnuto
69	22	9	9	28	1

2.8.1.1.3. Kasační stížnosti

Kasační stížnosti proti rozhodnutím Městského soudu v Praze o zamítnutí žaloby (2006 – 2011)
(rozhoduje Nejvyšší správní soud v Brně)

Celkem	Dosud nerozhodnuto	Řízení zastaveno	Vyhověno	Zamítnuto	Odmítnuto
14	0	0	3	9	2

Kasační stížnosti Úřadu proti rozhodnutím Městského soudu v Praze o vyhovění žalobě (2006 – 2011) *(rozhoduje Nejvyšší správní soud v Brně)*

Celkem	Dosud nerozhodnuto	Řízení zastaveno	Vyhověno	Zamítnuto	Odmítnuto
2	0	0	2	0	0

2.8.1.2. Hodnocení rozhodovací praxe Úřadu

Jak vyplývá z výše uvedených údajů, v současné době je rozhodnuto ve 47 případech o žalobách proti rozhodnutí ředitele Úřadu o rozkladu, přičemž pouze 9 žalob shledal Městský soud v Praze důvodnými. „Úspěšnost“ Úřadu tedy činí cca 81 %.

2.8.2. Správní řízení o pokutě

V roce 2011 rozhodoval ředitel Úřadu rovněž o opravných prostředcích – rozkladech – uplatněných ze strany fyzických a právnických osob ve správním řízení pro porušení povinností v oblasti ochrany utajovaných informací.

O podaných rozkladech rozhodoval ředitel Úřadu dle příslušných ustanovení zákona č. 500/2004 Sb., správní řád, a to vždy na základě návrhu rozkladové komise ustavené v souladu s § 152 odst. 2 správního řádu.

Stejně jako v bezpečnostním řízení, i ve správním řízení o pokutě je možno rozhodnutí ředitele o rozkladu napadnout správní žalobou, o níž rozhoduje Městský soud v Praze. Proti rozhodnutí Městského soudu v Praze je možno dále podat kasační stížnost, o níž rozhoduje Nejvyšší správní soud.

Konkrétně se v roce 2011 jednalo o 2 rozklady. V obou případech byl rozklad zamítnut, přičemž účastníci řízení proti rozhodnutí ředitele Úřadu doposud nepodali

žalobu k Městskému soudu v Praze. Žaloba proti rozhodnutí ředitele Úřadu o rozkladu podaná k Městskému soudu v Praze v roce 2010, dosud nebyla rozhodnuta.

2.8.3. Řízení dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím

V roce 2011 ředitel Úřadu nerozhodoval o žádných opravných prostředcích – rozkladech – uplatněných v řízení dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, proti rozhodnutí Úřadu o odmítnutí žádosti o poskytnutí informace.

2.9. Výzkumná a vývojová činnost Úřadu

2.9.1. Cíle a organizace výzkumu a vývoje

Základním cílem v oblasti výzkumu a vývoje je další rozvoj bezpečnostních technologií pro ochranu utajovaných informací v komunikačních a informačních systémech. V důsledku rychlého rozvoje informačních technologií se stále zvyšuje náročnost výzkumu a vývoje v oblasti bezpečnosti informačních technologií. Z hlediska dostupných lidských zdrojů je nezbytné využívat pro řešení vývojových a výzkumných úkolů i externí odborná pracoviště a jednotlivé odborníky, čímž jsou částečně uvolňovány omezené vlastní kapacity Úřadu pro ty výzkumně-vývojové práce, které nemohou být (např. z důvodu utajení) řešeny mimo Úřad.

Výzkum a vývoj byl proto prováděn na odborných pracovištích Úřadu a široce také na základě smluv o dílo financovaných z rozpočtu Úřadu. Byly dokončeny 3 projekty zahájené v roce 2010. V roce 2011 bylo postupně zahájeno 13 nových projektů, z nichž část navazuje na vývoj realizovaný v minulých letech a vyžaduje k řešení subjekty splňující podmínky pro přístup k utajované informaci. Řešení několika vysoce specializovaných projektů se ujala odborná pracoviště ČVUT v Praze.

Využívání finančních prostředků se soustředilo na výzkumné aktivity sloužící k uspokojení reálných potřeb bezpečnostní praxe, a to v oblasti kryptografické ochrany, ochrany proti úniku utajovaných informací kompromitujícím vyzařováním a počítačové bezpečnosti. Tyto potřeby zjišťuje Úřad při své certifikační a konzultační činnosti, při jednáních se zástupci orgánů státní správy, při výkonu státního dozoru i vyhodnocením speciálních dotazníků z oblasti kryptografické ochrany předkládaných klíčovým rezortům státní správy.

V roce 2011 Úřad aktualizoval svou koncepci dalšího rozvoje výzkumu a vývoje v oblasti kryptografické ochrany. Záměrem je její další vývoj v roce 2012 ve spolupráci zejména s těmi rezorty státní správy, pro které je kryptografická ochrana utajovaných informací nezbytná.

2.9.2. Přehled projektů realizovaných formou smlouvy o dílo

V roce 2011 probíhalo řešení projektů ve dvou hlavních oblastech – oblasti kryptografické ochrany utajovaných informací a oblasti ochrany utajovaných informací před jejich únikem kompromitujícím vyzařováním.

Oblast kryptografické ochrany zahrnovala

- vývoj prototypu osobního kryptografického prostředku ve formě malého externího šifrovacího zařízení, připojovaného k PC přes rozhraní USB a umožňujícího šifrování datového archivu v interní Flash paměti a OFF-line šifrování souborů nebo adresářů uložených na PC,

- vývoj prototypu mobilního telefonu pro síť GSM s národními kryptografickými funkcemi, umožňujícího šifrování hovorů a SMS, šifrování archivu na interní Flash paměti a OFF-line šifrování souborů nebo adresářů na PC připojeném přes USB rozhraní,

- vývoj rozhraní PCI-express pro národní kryptografické prostředky PCS1 a LanPCS a realizace jejich portace pro OS MS Windows 7,

- další rozvoj graficky orientovaného SW nástroje CipherCAD pro vizualizaci, návrh a analýzu kryptografických algoritmů a protokolů k podpoře analytické a certifikační činnosti Úřadu,

- studii realizovatelnosti implementace evropských šifrovacích algoritmů rodiny VEGAS do stávajících nebo uvažovaných národních kryptografických prostředků pro ochranu utajovaných informací,

- studii možnosti využití technologií VoIP a speciální microSD karty pro šifrování citlivých hovorů v komerčních mobilních telefonech s vybraným operačním systémem.

Oblast kompromitujícího vyzařování zahrnovala

- kompletní vývoj automatizovaného systému pro měření útlumu stíněných prostorů, umožňujícího měřit magnetickou i elektrickou složku elektromagnetického pole a vložený útlum vestavěných filtrů v požadovaném frekvenčním rozsahu a v souladu s ČSN EN 50 147-1,

- analýzu antén pro zónové měření dosud používaných v Úřadu a posouzení jejich možností pro použití v rozšířeném kmitočtovém pásmu 1 GHz – 3 GHz, posouzení vlivu rozdílného vertikálního umístění přijímacích a vysílacích antén a specifikaci případných úprav antén,

- vývoj a realizaci antén pro zónová měření na základě provedené analýzy, zlepšení vlastností směrové přijímací a všesměrové vysílací antény umožňující jejich použití pro zónové měření v kmitočtovém pásmu 10 MHz až 3 GHz,

- vývoj nových modulů pro měřící systém MENEA (zpracování laboratorních měření kompromitujícího vyzařování), zahrnující i přechod k operačnímu systému Windows 7 v 64 bitové verzi,

- zlepšení parametrů měřící komory Úřadu pro měření kompromitujícího vyzařování z elektronických zařízení, v níž se provádí naprostá většina měření pro potřeby ochrany utajovaných informací v ČR, rozšířením v kmitočtovém pásmu 1 GHz – 10 GHz,

- analýzu soupravy pro měření magnetické složky elektromagnetického pole, zahrnující hodnocení vlivu jejích jednotlivých částí na přesnost měření útlumu stínicích komor, včetně sestavení matematických modelů pro popis jednotlivých částí a systému jako celku,

- rozbor současných přenosových systémů s rozprostřeným spektrem a detekce zařízení vysílajících signály tímto způsobem a možností eliminace úniku informací; vývoj měřícího mobilního systému pro měření a hodnocení modulačních produktů na nosných kmitočtech vysílačů a současně i generátoru audio modulačních signálů pro testování systémů používajících vysílače; vývoj mobilního měřícího systému pro rychlé skenování frekvenčního spektra.

2.9.3. Vlastní výzkum a vývoj v Úřadu

Vlastní výzkum a vývoj byl v roce 2011 prováděn na 3 odborných pracovištích Úřadu – kryptologickém, TEMPEST a certifikačním. Rámcem pro výzkum a vývoj byl výzkumný záměr „Výzkum speciálních bezpečnostních technologií k ochraně utajovaných informací na rok 2011“.

Kryptologický výzkum a vývoj se zaměřil zejména do oblasti analýzy, verifikace, testování a implementace národních i některých zahraničních kryptografických algoritmů včetně jejich stavebních prvků.

Řešena byla oblast národní inicializace a finalizace nových kryptografických prostředků vyvíjených v rámci externí spolupráce a vlastní vývoj SW kryptografických aplikací používaných v bezpečnostní praxi.

Průběžně byla prováděna podpora životního cyklu kryptografických prostředků, zejména pak rozvoj a údržba vyvinutých, nasazených a certifikovaných kryptografických prostředků aktuálně využívaných.

Byla vytvořena řada modelových pracovišť pro implementaci, verifikaci a testování kryptografického SW i HW.

Dále bylo rozvíjeno a zefektivňováno technologické vybavení vývojových, překladových, testovacích a měřících laboratoří v souladu s aktuálními potřebami jednotlivých řešených vývojových projektů.

Na pracovišti TEMPEST byly provedeny dílčí výzkumné činnosti zaměřené na metodiku zónového měření, metodiku měření útlumových vlastností UPS a filtrů,

na metodiku měření kompromitujících signálů u speciálních komponentů IS (scanner, projektor) a na problematiku přijímačů pro radiomonitoring. Pokračovalo budování mobilního systému pro TEMPEST měření.

V souladu s výzkumným záměrem a na základě analýz mezinárodních standardů pro bezpečné mazání paměťových médií, které byly provedeny v roce 2010, byl zpracován bezpečnostní standard pro opětovné užití, snížení a zrušení stupně utajení nosičů utajovaných informací. Dále byly zpracovány požadavky na hodnocení produktů pro bezpečné odstranění dat z paměťových médií. Tyto požadavky byly předány potencionálním dodavatelům produktů. V současné době probíhá příprava podkladů pro následné hodnocení vybraných produktů. Hodnocení předložených produktů bude prováděno v následujícím období.

V oblasti testování a hodnocení nástrojů k provádění analýzy rizik bylo prováděno testování produktů RISKAN ver. 2,0, GSTOOL ver. 4.5 a EAR / PILAR, Testování uvedených nástrojů bude probíhat i v následujícím roce. Po jeho ukončení bude zpracováno doporučení k používání uvedených nástrojů při provádění analýzy rizik v informačních systémech podléhajících certifikaci Úřadem a pro provádění analýzy rizik v oblasti kybernetické bezpečnosti.

V roce 2011 bylo v laboratořích National Security Agency (NSA) a National Institute of Standards and Technology (NIST) ukončeno hodnocení operačních systémů Microsoft Windows 7 a Microsoft Windows 2008 R2. Hodnocení bylo provedeno v souladu se standardem Common Kriteria for IT Security Evaluation (Version 3.1 R3) pro úroveň EAL 4+. V návaznosti na toto hodnocení bylo na certifikačním pracovišti Úřadu zpracováno doporučení pro bezpečné nastavení operačního systému Microsoft Windows 7, které zahrnuje národní specifika a je v souladu s národní právní úpravou v oblasti ochrany utajovaných informací. Doporučení obsahuje bezpečnostní nastavení pro samostatné pracovní stanice a pro pracovní stanice zapojené do lokálních počítačových sítí. Doporučení je již poskytováno na vyžádání žadatelům o certifikaci informačních systémů, kteří své systémy provozují s výše jmenovanými operačními systémy.

2.10. 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, podnikatelé 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. zajištění 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.

2.10.1. Kontroly provedené v roce 2011

Na základě požadavku na zvýšení celkového počtu uskutečněných kontrol při současném snížení počtu zaměstnanců, kteří jednotlivé kontroly provádějí, bylo na konci roku 2010 rozhodnuto o změně systému výkonu státního dozoru. Bylo omezeno provádění velkých jednorázových komplexních kontrol subjektů s rozsáhlou organizační strukturou (Ministerstvo obrany, Armáda ČR, Ministerstvo vnitra, Policie ČR, Celní správa ČR aj.) a nadále jsou prováděny samostatné kontroly u jednotlivých organizačních součástí těchto subjektů. Zvýšen byl rovněž podíl tzv. tematických kontrol, kdy je kontrolována pouze určitá dílčí oblast, a nově byl zaveden typ tzv. nárazových kontrol, při kterých jsou kontrolovány rovněž pouze některé oblasti, a navíc je většinou kontrola provedena namátkově v kratším časovém úseku za účasti minimálního počtu zaměstnanců Úřadu.

S cílem urychlit postup při kontrolní činnosti dále vedení Úřadu rozhodlo o sestavení formulářů stanovujících jednotné kontrolní postupy pro jednotlivé kontrolované oblasti a typy kontrol. Na základě těchto formulářů pak byla změněna i forma písemných výstupů z kontrolních akcí – protokolů o kontrole, které byly doposud zpracovávány formou slovního popisu kontrolovaných skutečností a jednotlivých kontrolních zjištění. Sjednocení a formalizace kontrolních postupů a omezení rozsahu zjišťovaných skutečností umožnilo ve většině případů výrazně zkrátit dobu potřebnou k provedení kontroly, neboť postup již prakticky nemusel být přizpůsobován různým typům kontrolovaných subjektů a konkrétnímu stavu kontrolované oblasti.

V roce 2011 provedl Úřad celkem 129 kontrol ochrany utajovaných informací, z toho 52 v orgánech státu a jejich složkách a 77 u podnikatelů. Oproti předchozímu roku byl počet provedených kontrol navýšen téměř čtyřikrát. Kromě komplexních, tematických a tzv. nárazových kontrol byly provedeny rovněž 2 kontroly následné, zaměřené na ověření odstranění nedostatků zjištěných při předchozích kontrolách. Souhrnné počty jednotlivých kontrol jsou uvedeny v následující tabulce.

Kontroly provedené v roce 2011

Kontroly	Komplexní	Tematické	Nárazové	Následné	Celkem
Orgány státu	9	22	19	2	**52**
Podnikatelé	14	30	33	0	**77**
Celkem	**23**	**52**	**52**	**2**	**129**

Kontroly byly prováděny na základě průběžně doplňovaných plánů kontrol na jednotlivá pololetí roku 2011. Většina kontrol byla do plánu zařazena z vlastního podnětu Úřadu, především u subjektů, u kterých dosud kontrola provedena nebyla nebo na základě periodicity. V průběhu roku byly na základě získaných poznatků nebo na základě vnějších podnětů do plánu kontrol průběžně zařazovány mimořádné tematické kontroly zaměřené na ověření dodržování konkrétních povinností orgánů státu, podnikatelů a jejich zaměstnanců. Přehled jednotlivých kontrolních akcí uskutečněných v roce 2011 je uveden v následujících tabulkách.

Kontroly v orgánech státu a jejich součástech v roce 2011

Kontrolovaná osoba	Kontrolovaná osoba
Český báňský úřad	Ministerstvo průmyslu a obchodu
Český statistický úřad	Ministerstvo školství, mládeže a tělovýchovy
Český úřad zeměměřický a katastrální	Ministerstvo zahraničních věcí
Energetický regulační úřad	Ministerstvo zahraničních věcí – zastupitelský úřad ČR v Ammánu
HZS Olomouckého kraje	
HZS Plzeňského kraje	Ministerstvo zahraničních věcí – zastupitelský úřad ČR v Berlíně
HZS Středočeského kraje	
Kancelář prezidenta republiky	Ministerstvo zahraničních věcí – zastupitelský úřad ČR v Damašku
Krajské státní zastupitelství v Praze	
Krajský soud v Hradci Králové (2x)	Ministerstvo zahraničních věcí – zastupitelský úřad ČR v Kyjevě
Krajský soud v Ostravě	
Krajský soud v Praze	Ministerstvo zahraničních věcí – zastupitelský úřad ČR v Moskvě
Městské státní zastupitelství v Praze	
Městský soud v Brně	Ministerstvo zahraničních věcí – zastupitelský úřad ČR v Rize
Ministerstvo financí	
Ministerstvo kultury	Ministerstvo zahraničních věcí – zastupitelský úřad ČR v Tallinnu
Ministerstvo obrany – 153. ženijní prapor Olomouc	
Ministerstvo obrany – 21. základna taktického letectva Čáslav	Ministerstvo zahraničních věcí – zastupitelský úřad ČR ve Varšavě
Ministerstvo obrany – 22. základna letectva Náměšť nad Oslavou	Ministerstvo zahraničních věcí – zastupitelský úřad ČR ve Vilniusu
Ministerstvo obrany – 24. základna dopravního letectva Praha – Kbely	Ministerstvo zdravotnictví
	Obvodní soud pro Prahu 2
Ministerstvo obrany – 43. výsadkový mechanizovaný prapor Chrudim	Obvodní soud pro Prahu 5
	Okresní soud Brno-venkov
Ministerstvo obrany – centrální registr	Okresní soud v Břeclavi
Ministerstvo obrany – Generální štáb Armády ČR (Kancelář náčelníka GŠ + GŠ)	Okresní soud v Ostravě
	Stálá delegace ČR při NATO v Bruselu
Ministerstvo obrany – Krajské vojenské velitelství hlavní město Praha	Úřad pro ochranu hospodářské soutěže
	Úřad vlády ČR – registr
Ministerstvo obrany – Krajské vojenské velitelství Plzeň	Vězeňská služba ČR – GŘ VS, Vazební věznice Praha – Ruzyně a Praha – Pankrác
Ministerstvo obrany – Posádkové velitelství Praha	Vojenská kancelář prezidenta republiky
Ministerstvo pro místní rozvoj	Vrchní soud v Praze

Kontroly u podnikatelů v roce 2011

Kontrolovaná osoba	Kontrolovaná osoba
AERO TRADE, a. s.	Letiště Praha, a. s.
AERO Vodochody a. s.	Luwex, akciová společnost
AG COM, a. s.	MARHOLD a. s.
AGA – Letiště, s. r. o.	MEDTEC-VOP s. r. o.
ANECT a. s.	METROPROJEKT Praha a. s.
Arch.Design, s. r. o.	Metrostav a. s.
Atos IT Solutions and Services, s. r. o.	MICROSOFT s. r. o.
CAMBRIDGE COMPANY, s. r. o.	MobilKom, a. s.
CESA, a. s., Pardubice	Netprosys, s. r. o.
COFELY FM s. r. o. (2x)	NSN CS, s. r. o.
ČD Cargo, a. s.	OMNIPOL a. s.
České aerolinie a. s.	PositronLabs s. r. o.
ČEZ, a. s.	Pozemní stavby Zlín, a. s.
ČEZ ICT Services, a. s.	Pražská vodohospodářská společnost a. s.
DELINFO, spol. s r. o. (2x)	Princip a. s.
DELTA ARMY, s. r. o.	Rapos, s. r. o.
Domeček – odpady s. r. o.	Sellier & Bellot, a. s.
ELSO PHILIPS SERVICE, spol. s r. o.	SENSE Progress, a. s.
FASS, s. r. o.	Simac Technik ČR, a. s.
FORTE a. s.	SKILL s. r. o.
H Q H SYSTEM spol. s r. o.	Správa železniční dopravní cesty, stát. organizace
HELIKA, a. s.	S-projekt plus, a. s.
HEWLETT-PACKARD s. r. o.	STAEG, spol. s. r. o.
HICON, spol. s r. o.	STÁTNÍ TISKÁRNA CENIN, státní podnik (2x)
HOCHTIEF CZ a. s.	STAVITELSTVÍ ŘEHOŘ, s. r. o.
IBM Česká republika, spol. s r. o.	STEP, spol. s r. o.
IMOS Brno a. s.	Svoboda a syn, s. r. o.
INDRA Czech Republic s. r. o.	T-Mobile Czech Republic a. s.
INTAR a. s.	Trade FIDES, a. s.
INTV, spol. s r. o.	T-SOFT a. s.
JOHNSON CONTROLS INTERNATIONAL, s. r. o.	TTC TELEKOMUNIKACE, s. r. o.
KOMIX s. r. o.	Ústav jaderného výzkumu Řež, a. s.
Konek Tel, a. s.	VAE CONTROLS, s. r. o.
KONSTRUKTIVA KONSIT a. s.	VCES a. s.
LEC s. r. o.	Vegacom a. s.

Kontrolovaná osoba	Kontrolovaná osoba
VOKD, a. s.	Z.L.D. s. r. o.
XEOS spol. s r. o.	ZVI 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 2011

Kontroly 2011 – dle důvodu

Kontroly 2011 – dle typu

2.10.2. Výsledky kontrol

Nedostatky zjištěné při kontrolách vyplývaly z porušení nebo nedodržení jednotlivých ustanovení zákona a dalších právních předpisů a byly uváděny jako kontrolní zjištění v protokolech o jednotlivých kontrolách. Z celkového počtu 129 kontrol provedených v roce 2011 nebyly nedostatky zjištěny v 62 případech (48 %) (v roce 2010 nebyly nedostatky zjištěny pouze v 6 případech ze 33, což činilo 18 %). Ve 33 případech (25 %) byly podány podněty k zahájení správního řízení pro podezření ze spáchání přestupku nebo správního deliktu (v roce 2010 14 případů – 42 %).

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 2011 byly zjištěny zejména následující typy nedostatků:

Obecné nedostatky

- nezřízení nebo neobsazení funkce bezpečnostního ředitele nebo neoznámení jmenování bezpečnostního ředitele do funkce;
- nesplnění některé z podmínek pro výkon funkce bezpečnostního ředitele;
- nezrušení stupně utajení utajované informace po pominutí důvodu jejího utajení;
- neplnění povinnosti kontrolovat dodržování povinností stanovených zákonem;
- chybějící dokumenty obsahující utajované informace;
- vnitřním předpisem stanovený postup pro zajištění ochrany utajovaných informací, který byl v rozporu s právní úpravou ochrany utajovaných informací.

Personální bezpečnost

- přístup k utajované informaci zjištěný u fyzické osoby, která nesplňovala všechny zákonem stanovené podmínky pro tento přístup;
- 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;
- neproškolení fyzické osoby, která měla přístup k utajované informaci;
- neplnění dalších zákonem stanovených povinností (nevyhotovení písemného záznamu o zániku platnosti oznámení o splnění podmínek pro přístup k utajované informaci stupně utajení Vyhrazené, nevyhotovení písemného vyrozumění fyzické osoby o zániku platnosti tohoto oznámení);
- formální nedostatky vyhotovených písemných dokladů (nesprávné nebo chybějící datum).

Administrativní bezpečnost

- nezaevidování utajovaných informací (dokumentů);
- nezaznamenání pohybu utajovaného dokumentu ve stanovených administrativních pomůckách nebo nesprávné údaje, 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);

- používání administrativních pomůcek, které nesplňovaly požadavky stanovené právním předpisem na jejich obsah a úpravu (autentizace, evidence v neodpovídajících pomůckách, nesplnění podmínek stanovených pro použití elektronické evidence);

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

- nevedení evidence administrativních pomůcek a nedostatky v jejím vedení (chybné údaje, duplicitní evidenční označení, neúplné záznamy);

- neplnění dalších povinností stanovených v oblasti administrativní bezpečnosti právními předpisy (např. při předávání nebo přepravě utajovaných dokumentů, při odesílání utajovaných dokumentů v nelistinné podobě).

Fyzická bezpečnost

- nezpracování projektu fyzické bezpečnosti pro objekt a zabezpečené oblasti, ve kterých se ukládají utajované informace;

- nezajištění fyzické ostrahy u zabezpečené oblasti;

- nedostatky v realizaci opatření fyzické bezpečnosti (nefunkčnost použitých technických prostředků, nestanovení režimových opatření);

- absence požadovaných technických prostředků pro zajištění objektů a zabezpečených oblastí (EZS);

- nedostatečná úroveň opatření fyzické bezpečnosti (nesplnění stanovených minimálních požadavků pro příslušnou kategorii zabezpečené oblasti);

- nesplnění dalších povinností stanovených v oblasti fyzické bezpečnosti právními předpisy (neprovádění průběžného hodnocení rizik, neověřování, zda použitá opatření odpovídají projektu fyzické bezpečnosti a právním předpisům, neprovádění funkčních zkoušek technických prostředků a zápisů o jejich provedení).

Bezpečnost informačních a komunikačních systémů

- nakládání s utajovanými informacemi v informačním systému, který nebyl certifikován Úřadem;

- neprovádění aktualizace dokumentace informačního systému; neplnění povinností při provozu informačního systému (audit, antivirová ochrana,

kontroly, zápisy do provozní dokumentace informačního systému, evidence médií, nesoulad dokumentace se skutečným stavem).

Kryptografická ochrana

- nedostatečné zabezpečení kryptografického prostředku proti neoprávněné manipulaci;
- absence osvědčení odborné způsobilosti pracovníka kryptografické ochrany;
- manipulace s kryptografickým materiálem osobou neoprávněnou k této manipulaci;
- nedostatky ve vedení evidence kryptografických písemností.

V rámci výkonu státního dozoru Úřad rovněž získává poznatky, které pomáhají vyhodnotit efektivitu právní úpravy a konkrétních řešení jednotlivých oblastí ochrany utajovaných informací, 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 novelizace právní úpravy ochrany utajovaných informací. 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 zjišťované při výkonu státního dozoru.

2.11. Metodická činnost Úřadu

Metodickou činnost vůči orgánům státu a jejich organizačním složkám a vůči podnikatelům vykonával Úřad v roce 2011 především v rámci odborné činnosti jednotlivých organizačních celků poskytováním konzultací, zodpovídáním telefonických, písemných nebo elektronickou formou položených dotazů a rovněž při výkonu státního dozoru a provádění tzv. dohlídek v průběhu bezpečnostního řízení u podnikatelů.

Tato činnost výrazně zintenzivnila ve druhé polovině roku v souvislosti s blížícím se termínem nabytí účinnosti velké novely zákona a prováděcích předpisů k zákonu (zcela nové vyhlášky nebo zásadní novely stávajících vyhlášek) a vyvrcholila provedením seminářů pro oblasti personální bezpečnosti, bezpečnostní způsobilosti a průmyslové bezpečnosti.

Předmětem metodické činnosti je zejména oblast bezpečnostního řízení, hlášení změn, procesu certifikace, zpracovávání bezpečnostní dokumentace, projektu fyzické bezpečnosti, a konkrétních postupů při praktické aplikaci právních předpisů v oblasti administrativní a fyzické bezpečnosti.

Nejčastěji kladené dotazy a odpovědi stejně jako vydávané metodické pokyny a návody Úřad uveřejňuje na svých internetových stránkách (viz kapitolu 2.12.2.).

2.11.1. Metodická činnost v oblasti bezpečnostního řízení

Metodická činnost Úřadu v oblasti bezpečnostního řízení je nezbytným, trvalým a kontinuálním procesem, který probíhal i v průběhu celého roku 2011. Členění této činnosti korespondovalo s jednotlivými fázemi bezpečnostního řízení.

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

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

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 podnikatelům – 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.

Těžiště metodické činnosti v hodnoceném roce bylo orientováno zejména do prvních tří oblastí.

V souvislosti s konzultační a metodickou činností Úřadu v této oblasti nelze opomenout uspořádání bezplatných seminářů pro bezpečnostní ředitele státní správy a samosprávy a pro podnikatele v závěru roku 2011. Semináře byly zaměřeny na poskytnutí informací ke změnám, které v oblasti personální a průmyslové bezpečnosti a v oblasti bezpečnostní způsobilosti přinesla velká novela zákona a nové vyhlášky o personální bezpečnosti a bezpečnostní způsobilosti a o průmyslové bezpečnosti. Semináře se uskutečnily ve dnech 1., 6., 7., a 8. prosince 2011 a zúčastnili se jich zástupci 97 podnikatelů a 64 orgánů státní správy a samosprávy.

2.11.2. Metodická činnost v oblasti administrativní bezpečnosti

V oblasti administrativní bezpečnosti poskytuje Úřad metodickou pomoc při řešení systému opatření při tvorbě, příjmu, evidenci, zpracování, odesílání, přepravě, přenášení,

ukládání, a jiném nakládání s utajovanými dokumenty v konkrétních podmínkách podnikatele nebo orgánu státu. V roce 2011 byla metodická pomoc poskytnuta celkem 26 subjektům.

2.11.3. Metodická činnost v oblasti fyzické bezpečnosti

V oblasti fyzické bezpečnosti provádí Úřad metodickou pomoc v rámci certifikace technických prostředků (např. posuzování vhodnosti certifikace u stávajících nebo zabudovaných mechanických zábranných prostředků, návrh kombinace dveří s uzamykacím systémem s ohledem na požadované bodové hodnocení atd.).

Dále je průběžně na vyžádání prováděna metodická pomoc týkající se instalace technických prostředků a návrhu opatření fyzické bezpečnosti u podnikatelů nebo orgánu státu (např. Skanska CZ a. s., RETIA, a. s., LOM PRAHA s. p., Poslanecká sněmovna Parlamentu ČR, Senát Parlamentu ČR, Generální finanční ředitelství Ministerstva financí ČR, Kancelář prezidenta republiky, Generální inspekce bezpečnostních sborů aj.). Rozsáhlá metodická podpora byla realizována pro budovu GSA HQ Prague (Galileo). Ve spolupráci s Ministerstvem financí byl proveden návrh opatření fyzické bezpečnosti, stanoven rozsah předpokládaných instalovaných technických prostředků a poskytnuta konzultace na zadávací dokumentaci pro výběrové řízení pro dodavatele stavebních úprav a technologie do budovy GSA HQ Prague.

2.12. Věstník Úřadu a internetové stránky Úřadu

2.12.1. Věstník Úřadu

Úřad vydává, v souladu se zákonem, Věstník Úřadu jako periodickou tiskovinu, která vychází dvakrát ročně, v případě potřeby i vícekrát. V roce 2011 byla vydána 2 pravidelná čísla.

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

Ve Věstníku Úřadu jsou dále zveřejňovány informace z oblasti personální, administrativní, průmyslové a fyzické bezpečnosti, bezpečnosti informačních a komunikačních systémů, kryptografické ochrany utajovaných informací a bezpečnostní způsobilosti. Dále jsou zveřejňovány metodické pokyny vydávané Úřadem, různé pokyny, návody a instrukce, žádosti a další 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 na adrese Úřadu nebo v obchodním oddělení Tiskárny Ministerstva vnitra.

Obsah Věstníku Úřadu je rovněž zveřejňován na internetových stránkách Úřadu.

2.12.2. Internetové stránky Úřadu

Internetové stránky Úřadu (www.nbu.cz) jsou v provozu od roku 1999. Jsou na nich pravidelně zveřejňovány veškeré informace, které se týkají činnosti Úřadu a jeho hlavních úkolů. Členěny jsou na odborné a všeobecné informace, včetně aktualit, tiskových zpráv a elektronické podatelny. Všechny údaje jsou průběžně aktualizovány.

Obsahem svých internetových stránek se Úřad snaží především reagovat na nejčastěji kladené dotazy tak, aby jejich uživatelé nalezli vše, co potřebují vědět o problematice utajovaných informací, bezpečnostní způsobilosti i o Úřadu samotném. V roce 2011 byly podle očekávání nejvíce vyhledávanými informace týkající se bezpečnostního řízení.

Na internetových stránkách Úřadu je zveřejňován přehled všech platných právních předpisů upravujících oblast ochrany utajovaných informací a bezpečnostní způsobilosti, průběžně aktualizovaný o jejich novelizace. Internetové stránky také obsahují informace o ztrátě nebo ukončení platnosti certifikátů, o falešných certifikátech apod. Zveřejňovány jsou rovněž aktuální metodické pokyny a zpřístupněny jsou i elektronické verze dotazníků a žádostí. Internetové stránky vždy obsahují poslední číslo Věstníku Úřadu. Nově na ně byl umístěn také odkaz na protikorupční linku 199.

Internetové stránky 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 2011 vykázaly internetové stránky více než 150.000 přístupů, což je více než 12.500 návštěv za měsíc.

2.13. Poskytování informací podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím

V roce 2011 byly Úřadu podány 2 žádosti o informace podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů. Těmto žádostem bylo vyhověno a požadované informace byly žadatelům poskytnuty. Nebylo tedy vydáno žádné rozhodnutí o odmítnutí žádosti.

V roce 2011 nebyla poskytnuta žádná výhradní licence ani nebyla podána žádná stížnost podle § 16a zákona č. 106/1999 Sb.

2.14. Inspekce ředitele Úřadu

Inspekce ředitele Úřadu v průběhu roku 2011 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 2011 inspekce ředitele Úřadu řešila jedinou stížnost, která byla vyhodnocena jako nedůvodná.

3. Bezpečnostní, ekonomické a personální zabezpečení Úřadu

3.1. Ochrana utajovaných informací v Úřadu

Ochranu utajovaných informací v Úřadu zajišťoval odbor bezpečnostní, v jehož čele stojí bezpečnostní ředitel Úřadu, který je také předsedou krizového štábu Úřadu.

3.1.1. Ochrana objektu Úřadu

V roce 2011 byl nainstalován nový systém kontroly vstupu do budovy B Úřadu. V souvislosti s budováním pracoviště Národního centra kybernetické bezpečnosti v Brně byly prováděny přípravné práce v oblasti zajištění fyzické bezpečnosti.

3.1.2. Vnitřní kontrola

Vnitřní kontrola byla, v souladu s Plánem kontrol na rok 2011, zaměřena na dodržování zásad při ochraně utajovaných informací ze strany zaměstnanců Úřadu. Kontrolní činnost byla prováděna v provozní i mimoprovozní době a byla průběžně vykonávána na všech pracovištích Úřadu.

Kontrolní činnost byla zaměřena zejména na:

- zabezpečení pracovišť při krátkodobé i dlouhodobé nepřítomnosti zaměstnance,

- klíčové hospodářství,
- zabezpečení výpočetní techniky,
- zabezpečení úschovných objektů a uzamykatelných schránek,
- dodržování pravidel administrativní bezpečnosti,
- manipulaci a uložení evidovaných razítek Úřadu,
- neoprávněné vnášení nebezpečných předmětů či alkoholických nápojů.

Odbor bezpečnostní provedl 1 plánovanou a 5 namátkových kontrol, během nichž nebyly zjištěny žádné závažné nedostatky.

3.1.3. Bezpečnostní řízení prováděná k zaměstnancům Úřadu

Na základě bezpečnostního řízení realizovaného odborem bezpečnostním bylo v roce 2011 vydáno 41 osvědčení fyzické osoby, 10 osvědčení fyzické osoby pro cizí moc a 1 oznámení o splnění podmínek pro přístup k utajované informaci stupně utajení Vyhrazené.

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 utajované archiválie a v rámci činnosti specializovaného archivu o neutajované archiválie. Archiv dohlíží na výkon spisové služby a pravidelně provádí výběr archiválií ve skartačním řízení. Archiválie jsou vedeny v základní evidenci Národního archivního dědictví. V roce 2011 bylo provedeno 9 archivních prohlídek. Celkový rozsah archiválií v roce 2011 je v bezpečnostním archivu 9,45 běžných metrů, ve specializovaném archivu 6,84 běžných metrů. V roce 2011 Archiv navštívil bezpečnostní archiv 1 interní badatel a specializovaný archiv 2 interní badatelé.

3.3. Ekonomické zabezpečení Úřadu

Úřad byl zřízen zákonem č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů, dne 1. listopadu 1998, kdy se po ekonomické stránce vyčlenil ze struktur Ministerstva vnitra. Jako ústřední správní úřad pro oblast ochrany utajovaných informací a bezpečnostní způsobilosti plní úkoly stanovené zákonem

a je financován v plné výši ze státního rozpočtu v rámci samostatné kapitoly státního rozpočtu „308“.

Příjmy přímo související se správní činností Úřadu byly pro rok 2011 rozpočtovány ve výši 300 tis. Kč. Jejich plnění bylo navýšeno nahodilými příjmy, se kterými rozpočet nepočítá, a celkem činily 1.124 tis. Kč, z čehož největší podíl tvořily pokuty uložené Úřadem v celkové výši 667 tis. Kč. Samostatným příjmem Úřadu ve výši 1.989 tis. Kč jsou finanční prostředky ze Strukturálních fondů EU, Integrovaný operační program záměr č. 204 ze Seznamu záměrů strategických projektů pro čerpání prostředků ze Strukturálních fondů EU v rámci Smart Administration. Jedná se o projekt „Zavedení elektronického systému spisové služby a Document Management Systemu v Národním bezpečnostním úřadě v návaznosti na zavedení datových schránek“, který je připravován v souladu se zákonem č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů. Tento projekt byl dvouletý, jeho první etapa byla ukončena v roce 2010 a v roce 2011 byla realizována etapa druhá (viz přílohu).

Schválené rozpočtové výdaje na rok 2011 byly upraveny čtyřmi rozpočtovými opatřeními Ministerstva financí z 244.671 tis. Kč na 245.000 tis. Kč. K posílení rozpočtu došlo 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. Na základě tohoto usnesení vlády vzniklo Národní centrum kybernetické bezpečnosti, situované v Brně, jako součást Úřadu.

Rozpočet roku 2011 byl dále posílen o nespotřebované výdaje roku 2010 ve výši 739,67 tis. Kč. Znamená to, že rozpočet Úřadu byl o tyto prostředky přečerpán na 100,02 %. Rozpočet za rok 2011 byl čerpán ve výši 245.047 tis. Kč. Největší objem běžných výdajů tvořily, jako každým rokem, mzdové výdaje a zákonem dané odvody, ty byly vyčerpány na 99,80 %. Běžné výdaje, zejména platby v oblasti energií, nezbytných služeb a nákupů k zajištění činnosti Úřadu činily po rozpočtových změnách 54.835 tis. Kč (posíleny byly o nespotřebované výdaje roku 2010) a byly čerpány na úrovni 100,57 %, Kapitálové výdaje upraveného rozpočtu ve výši 26.502 tis. Kč v oblasti pořízení hmotného a nehmotného majetku byly vyčerpány na 99,99 %.

V roce 2011 byl Úřad organizátorem třídenního setkání vrcholných představitelů bezpečnostních úřadů států tzv. Visegradské čtyřky, jejichž hostitelem v předchozích letech byla Slovenská republika a Polská republika. Jednalo se o 3. ročník setkání, kterého se zúčastnili představitelé NOS NATO a další zahraniční hosté. Vzhledem k omezeným zdrojům byla koncepce vysoce úsporná, celé jednání bylo ryze pracovní a nezbytné společenské aktivity byly omezeny na minimum. Celkové náklady na toto setkání činily 239 tis. Kč.

Výzkum a vývoj byl v plném rozsahu financován z prostředků kapitoly „308“, tj. bez dotací výzkumu a vývoje státního rozpočtu, ve výši 14.783 tis. Kč. Vyčerpáno bylo 99,98 %, tj. 14.780 tis. Kč. V rámci uzavřených smluvních závazků s externími řešiteli bylo na účelové výzkumné projekty vyčerpáno 12.107 tis. Kč a v rámci institucionálních prostředků, které využívá Úřad pro potřeby vlastního výzkumu, bylo vyčerpáno 2.673 tis. Kč.

Nároky nespotřebovaných výdajů z rozpočtu roku 2011 ve výši 750 tis. Kč Úřad uplatní na pokrytí neplánovaných výdajů v roce 2012.

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 u všech účetních operací hlavní účetní a u vybraných finančních operací průřezově i správcem rozpočtu.

Každým rokem je rozpočet kapitoly „308“ snižován při stejném rozsahu činnosti. Úsporná opatření se proto zaměřují především na snížení kapitálových nákladů.

Celkové výdaje Úřadu v letech 2009 až 2011

	2009	2010	2011
Celkové výdaje (v tis. Kč)	289.158	259.792	245.047

3.4. Personální zabezpečení Úřadu

V začátku roku 2011 měl Úřad systemizovaných 275 pracovních míst.

Dne 19. října 2011 bylo přijato usnesení vlády ČR č. 781, kterým byl Úřad ustaven gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast. Od listopadu 2011 bylo převedeno jednoho pracovní místo z Ministerstva vnitra na Úřad a od roku 2012 dojde na základě uvedeného usnesení vlády k navýšení o dalších 8 funkčních míst.

K 31. prosinci 2011 bylo aktuálně obsazeno 263 pracovních míst, z toho bylo 130 mužů a 133 žen. Průměrný věk zaměstnanců byl 45 let a téměř 62 % 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 2011 pokračovalo jazykové vzdělávání, kterého se pravidelně účastní více než 60 zaměstnanců, dále probíhala i odborná školení 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 těch oblastech, které bezprostředně souvisejí s výkonem jejich odborných činností – 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 2011

Příloha – Projekt Systém elektronické spisové služby

INTEGROVANÝ OPERAČNÍ PROGRAM

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
ŠANCE PRO VÁŠ ROZVOJ

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

IDENTIFIKACE PROJEKTU

Název

Systém elektronické spisové služby

Výše dotace

Na realizaci projektu byla určena celková finanční částka ve výši: 4.680.000 Kč, z toho podíl ze státního rozpočtu činí výši 702.000 Kč a podíl z fondu Evropské unie činí výši 3.978.000 Kč.

Harmonogram a zahájení rutinního provozu

Realizace projektu byla plánována od 1. 6. 2010 do 31. 12. 2011 a zahájení rutinního provozu bylo realizováno od 2. 1. 2012.

SPECIFICKÉ CÍLE PROJEKTU A JEJICH NAPLNĚNÍ

Systém elektronické spisové služby musí respektovat veškeré právní předpisy a standardy:

- možnost pracovat s dokumenty v elektronické i analogové podobě,
- správa dokumentů – evidence a správa elektronických a analogových dokumentů,
- digitalizace dokumentů – převedení dokumentu v analogové podobě na dokument v elektronické podobě,
- workflow – řízené zpracování dokumentů,
- elektronická archivace – velkokapacitní úložiště pro ukládání a zpřístupnění elektronických objektů,
- modularita – poptávaný produkt musí být modulární, aby bylo možné postupně doplňovat jednotlivé funkční moduly,
- off-line práce se systémem – práce se spisy, evidence do sběrných archů – možnost synchronizace dat vybraného sběrného archu s databází systému ESS,
- fulltextové vyhledávání jako možné dodatečné rozšíření, indexace dokumentů (uživatelská, automatická) – možnost nastavení indexace nad vybranými kategoriemi dokumentů, možnost zadání požadavku na indexaci dle aktuálního požadavku nad vybranými dokumenty.

Úspěšnou realizací projektu byly naplněny cíle projektu a tím i definované indikátory:

- zvýšení výkonnosti Úřadu,
- zjednodušení činnosti veřejnosti vůči Úřadu,
- větší otevřenost Úřadu ve vztahu k jiným uživatelům,
- pomocí zavedených informačních technologií se optimalizovaly interní procesy.

Obsah

1. Úvod 3

2. Činnost Úřadu 3

2.1. Legislativní a právní činnost Úřadu 3

2.1.1. Vnější legislativní činnost 3

2.1.2. Vnitřní legislativní činnost 5

2.1.3. 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 2011 6

2.2.1.2. Výhled na rok 2012 8

2.2.2. Aktivity vyplývající z členství ČR v NATO a EU 9

2.2.3. Spolupráce s bezpečnostními úřady partnerských států 12

2.2.4. Ostatní mezinárodní aktivity Úřadu 13

2.3. Personální bezpečnost 13

2.3.1. Statistické přehledy 15

2.3.2. Analýza důvodů nevydání nebo zrušení platnosti osvědčení fyzické osoby 18

2.3.3. Personální projekt 19

2.4. Bezpečnostní způsobilost 19

2.4.1. Statistické přehledy 21

2.5. Průmyslová bezpečnost 21

2.5.1. Bezpečnostní řízení o žádosti podnikatele 22

2.5.2. Statistické přehledy 23

2.5.3. Analýza důvodů nevydání osvědčení podnikatele 24

2.6. Bezpečnost informačních a komunikačních systémů a kryptografická ochrana 24

2.6.1. Certifikační a akreditační činnost 25

2.6.1.1. Certifikace a akreditace informačních systémů 25

2.6.1.2. Certifikace kryptografických prostředků 27

2.6.1.3. Certifikace kryptografických pracovišť 29

2.6.1.4. Certifikace stínicích komor 30

2.6.2. Další odborná činnost 30

2.6.2.1. Výroba kryptografického materiálu 30

2.6.2.2. Měření kompromitujícího vyzařování (TEMPEST) 31

2.6.2.2.1. TEMPEST měření elektronických zařízení 31

2.6.2.2.2. Zónové měření, instalační záznamy, obranné prohlídky 32

2.6.2.2.3. Přehled provedených měření 32

2.6.2.3. Schvalování projektů bezpečnosti komunikačních systémů 32

2.6.2.4. Školení pracovníků kryptografické ochrany a zkoušky odborné způsobilosti 33

2.6.3. Problémové oblasti bezpečnosti informačních a komunikačních systémů a kryptografické ochrany 33

2.7. Administrativní a fyzická bezpečnost, ústřední registr 34

2.7.1. Administrativní bezpečnost 34

2.7.1.1. Problémové oblasti administrativní bezpečnosti 35

2.7.2. Fyzická bezpečnost 35

2.7.2.1. Certifikace technických prostředků 36

2.7.2.2. Posuzování bezpečnostní dokumentace podnikatele z hlediska fyzické bezpečnosti 38

2.7.2.3. Problémové oblasti fyzické bezpečnosti 38

2.7.3. Ústřední registr 39

2.8. Opravné prostředky 40

2.8.1. Bezpečnostní řízení 40

2.8.1.1. Statistické přehledy 41

2.8.1.1.1. Rozklady 41

2.8.1.1.2. Žaloby správní 42

2.8.1.1.3. Kasační stížnosti 42

2.8.1.2. Hodnocení rozhodovací praxe Úřadu 42

2.8.2. Správní řízení o pokutě 42

2.8.3. Řízení dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím 43

2.9. Výzkumná a vývojová činnost Úřadu 43

2.9.1. Cíle a organizace výzkumu a vývoje 43

2.9.2. Přehled projektů realizovaných formou smlouvy o dílo 44

2.9.3. Vlastní výzkum a vývoj v Úřadu 45

2.10. Státní dozor 46

2.10.1. Kontroly provedené v roce 2011 47

2.10.2. Výsledky kontrol 50

2.11. Metodická činnost Úřadu 53

2.11.1. Metodická činnost v oblasti bezpečnostního řízení 54

2.11.2. Metodická činnost v oblasti administrativní bezpečnosti 54

2.11.3. Metodická činnost v oblasti fyzické bezpečnosti 55

2.12. Věstník Úřadu a internetové stránky Úřadu 55

2.12.1. Věstník Úřadu 55

2.12.2. Internetové stránky Úřadu 56

2.13. Poskytování informací podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím 56

2.14. Inspekce ředitele Úřadu 57

3. Bezpečnostní, ekonomické a personální zabezpečení Úřadu 57

3.1. Ochrana utajovaných informací v Úřadu 57

3.1.1. Ochrana objektu Úřadu 57

3.1.2. Vnitřní kontrola 57

3.1.3. Bezpečnostní řízení prováděná k zaměstnancům Úřadu 58

3.2. Archiv Národního bezpečnostního úřadu 58

3.3. Ekonomické zabezpečení Úřadu 58

3.4. Personální zabezpečení Úřadu 60

Příloha – Projekt Systém elektronické spisové služby 63