
# Z P R Á V A

## O ČINNOSTI

## NÁRODNÍHO BEZPEČNOSTNÍHO ÚŘADU

## ZA ROK 2015

Praha 2016

# 1. ÚVOD

Činnost Národního bezpečnostního úřadu (dále jen „Úřad“) byla, v souladu s jeho působností a úkoly stanovenými především zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů (dále jen „zákon“), a dále zákonem č. 181/2014 Sb., o kybernetické bezpečnosti (dále jen „zákon o kybernetické bezpečnosti“), v roce 2015 zaměřena zejména na tyto hlavní oblasti:

- rozhodování o žádostech fyzických osob, žádostech podnikatelů a žádostech o doklad a provádění bezpečnostního řízení,
- certifikace technických prostředků, informačních systémů, kryptografických prostředků, kryptografických pracovišť a stínicích komor,
- spolupráce s bezpečnostními úřady členských zemí Organizace Severoatlantické smlouvy (NATO) a Evropské unie (EU) a zemí kandidujících na vstup do těchto organizací (vzájemné konzultace, příprava návrhů na sjednávání mezinárodních smluv) a podíl odborných pracovníků Úřadu na práci a jednání orgánů NATO a EU,
- aplikace právní úpravy ochrany utajovaných informací a bezpečnostní způsobilosti při plnění výše uvedených úkolů, výkon státního dozoru a poskytování metodické pomoci směřující k upevňování právního vědomí dotčených subjektů a ke sjednocování aplikační praxe v dané oblasti,
- legislativní, organizační a provozně-technické činnosti v souvislosti s gescí za oblast kybernetické bezpečnosti, implementace schválené Národní strategie kybernetické bezpečnosti na období let 2015 – 2020 a návazného Akčního plánu, určování prvků kritické informační infrastruktury a významných informačních systémů podle zákona o kybernetické bezpečnosti, technická asistence odborníků GovCERT.CZ subjektům spadajícím do jeho kompetence, cvičení s tematikou kybernetické bezpečnosti, spolupráce se zainteresovanými subjekty v ČR i v zahraničí, účast na konferencích, seminářích a přednáškách, poskytování informací veřejnosti atd.).

# 2. ČINNOST ÚŘADU

## 2.1. LEGISLATIVNÍ A PRÁVNÍ ČINNOST ÚŘADU

### 2.1.1. Vnější legislativní činnost

Zákon byl v roce 2015 jedenkrát novelizován, a to zákonem č. 204/2015 Sb., kterým se mění zákon č. 200/1990 Sb., o přestupcích, ve znění pozdějších předpisů, zákon č. 269/1994 Sb., o Rejstříku trestů, ve znění pozdějších předpisů, a některé další zákony. Novelizace umožní Úřadu v rámci bezpečnostního řízení vyžadovat opis nejen z evidence Rejstříku trestů, ale i z evidence přestupků, a to v elektronické podobě způsobem umožňujícím dálkový přístup. Uvedený zákon nabyl účinnosti dnem 1. října 2015.

Úřad v roce 2015 dále zpracoval novelu vyhlášky č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací, ve znění pozdějších předpisů. Vyhláška č. 275/2015 Sb., kterou se mění vyhláška č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací, ve znění pozdějších předpisů, v 76 novelizačních bodech řeší u utajovaných dokumentů v analogové podobě problémy zjištěné v rámci aplikační praxe a sjednocuje základní pojmy, výrazy a významy v oblasti utajované a neutajované spisové služby s cílem snížení administrativní zátěže původců utajovaných informací. Uvedená vyhláška nabyla účinnosti dnem 1. ledna 2016.

Právní úprava nakládání s utajovanými dokumenty v digitální podobě se intenzivně připravuje, neboť aplikační praxe si tuto právní úpravu vyžaduje. Tato nová právní úprava si však vyžádá i změnu zákona, neboť v současnosti se, podle § 23 odst. 3 zákona, zajištění ochrany utajovaných informací administrativní bezpečností nevztahuje na zpracování a přenos utajovaných informací v informačních systémech a kryptografických prostředcích.

Úřad se dále aktivně podílel na tvorbě návrhů zákonů, majících vazby na ochranu utajovaných informací a výkon citlivých činností, které byly připravovány ministerstvy nebo jinými ústředními správními úřady při přijímání nových zákonů nebo se změnami stávajících zákonů. Jednalo se zejména o přijetí nových zákonů, a to zákona o bezpečnostní činnosti a o změně souvisejících zákonů a atomového zákona. V této souvislosti, vzhledem k navýšení úkolů a prováděných bezpečnostních řízení, dosáhl Úřad i tomu odpovídající navýšení početních stavů Úřadu celkem o 12 pracovních míst včetně odpovídajících mzdových prostředků, zákonem daných odvodů, příslušenství, provozních výdajů a souvisejících jednorázových materiálových výdajů od 1. ledna 2016.

Úřad v rámci mezirezortního připomínkového řízení dále zpracoval stovky stanovisek k návrhům právních předpisů předkládaných ministerstvy nebo jinými ústředními správními úřady.

### 2.1.2. Legislativní činnost v rámci EU

Na evropské úrovni Úřad pokračoval v legislativním projednávání směrnice o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii (směrnice NIS), která byla Evropskou komisí představena dne 7. února 2013 v souvislosti se společným sdělením Evropské komise a vysoké představitelky EU pro zahraniční věci a bezpečnostní politiku o evropské strategii pro kybernetickou bezpečnost. Směrnice NIS byla velmi intenzivně projednávána během lotyšského i lucemburského předsednictví, přičemž během obou předsednictví proběhly celkem 4 neformální trialogy (2 za lotyšského a 2 za lucemburského předsednictví) a 7. prosince 2015 pak bylo na celkově již šestém neformálním trialogu dosaženo neformální dohody mezi unijními institucemi, čímž byla projednávání směrnice na technické úrovni uzavřena. Dne 18. prosince 2015 pak byla směrnice za Radu EU oficiálně odsouhlasena Výborem stálých zástupců (COREPER I).

Úřad již od počátku aktivně vysílal své experty na jednání na půdě Rady EU, která probíhala v rámci pracovní skupiny pro telekomunikace a informační společnost, kde aktivně prezentoval pozice ČR a zároveň vyjednával případnou spolupráci i s ostatními členskými státy. Rovněž prosazoval pozice ČR i v Evropském parlamentu. S ohledem na průřezovou povahu této regulace, která z velké míry dopadne i na podnikatelské prostředí ČR a rozvoj digitální agendy jako takové, konzultoval Úřad při vytváření národních pozic často s odborníky z jiných rezortů a ze soukromého sektoru, přičemž tyto konzultace byly zejména ze strany soukromého sektoru hodnoceny velmi kladně.

Prosazení pozic ČR hodnotí Úřad jako poměrně úspěšné. Podařilo se zejména vyjednat částečné zúžení působnosti směrnice v oblasti tzv. poskytovatelů digitálních služeb a zároveň se podařilo prosadit mírnější režim regulace pro tyto subjekty. Za další úspěch lze považovat prosazení

prodloužení lhůty pro dokončení identifikace operátorů základních služeb, kteří mají plnit požadavky stanovené směrnicí.

V souvislosti se směrnicí NIS se Úřad začal v průběhu roku 2015 taktéž na národní úrovni významně zapojovat i do aktivit v oblasti problematiky digitální agendy.

### 2.1.3. Vnitřní legislativní činnost

V průběhu roku 2015 bylo vydáno celkem 36 nových interních aktů řízení ředitele Úřadu. Konkrétně se jednalo o 7 směrnic a 29 pokynů, které byly vydány jako reakce na změny v právním řádu nebo z důvodu snahy o zefektivnění činnosti Úřadu a rovněž pro zajištění řízení o veřejných zakázkách, které jsou ve zvýšené míře zadávány. Ačkoliv bylo oproti roku 2014 vydáno o 6 interních aktů řízení méně, pokračuje trend vydávání vyššího počtu interních aktů řízení oproti předchozím letům, neboť si to vyžaduje aplikační praxe z důvodu zajištění nové působnosti Úřadu v oblasti kybernetické bezpečnosti. Z nejdůležitějších interních aktů řízení se jednalo zejména o organizační, platový a spisový řád, a v návaznosti na nabytí účinnosti zákona o státní službě, též o změnu pracovního řádu.

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

Úřad již čtvrtým rokem (od 1. ledna 2012) v rámci ochrany utajovaných informací zabezpečuje agendu, která se váže k zadávání veřejných zakázek veřejnými zadavateli, a podle § 138 odst. 1 písm. l) zákona se vyjadřuje k oznámení veřejných zadavatelů podle § 69 odst. 1 písm. r) zákona. Tato činnost spočívá v posuzování oznámení z hlediska ochrany utajovaných informací, učiněných veřejnými zadavateli, v nichž Úřadu oznamují skutečnost, že v rámci zadávacího řízení budou postupovat mimo režim zákona č. 137/2006 Sb., o veřejných zakázkách, ve znění pozdějších předpisů, z důvodu ochrany utajovaných informací, nebo že pro účast v zadávacím resp. koncesním řízení hodlají stanovit profesní kvalifikační předpoklad osvědčení podnikatele. Počet těchto oznámení od počátku této agendy osciluje kolem čísla 80.

V roce 2015 se Úřad vyjádřil k 75 podaným oznámením, tj. o 5 méně než v roce 2014.

Celkový objem finančních prostředků v rámci posuzovaných oznámení činil v roce 2015 cca 11,2 mld. Kč. Největší podíl na oznámeních mělo Ministerstvo obrany, a to 50 v celkové výši více než 10 mld. Kč, přičemž druhé Ministerstvo vnitra podalo 7 oznámení ve výši cca 116 mil. Kč.

V rámci posuzování podaných oznámení Úřad s veřejnými zadavateli ověřoval nezbytnou nutnost jimi zvoleného postupu z hlediska ochrany utajovaných informací, včetně vyžadování příslušných dokumentů obsahujících utajované informace, které mají být v rámci plnění předmětu veřejné zakázky poskytovány, a ověřování těchto skutečností se zaměstnanci jednotlivých oznamovatelů. Přehledy o zaslaných oznámeních a vyjádřeních Úřadu se, podle zákona, pravidelně zasílají k využití Úřadu pro ochranu hospodářské soutěže.

### 2.1.5. Právní činnost

V roce 2015 bylo pro porušení povinností stanovených zákonem ukončeno celkem 38 správních řízení, z toho ve 27 případech s fyzickými osobami a v 11 případech s právnickými osobami, a ve 37 případech byla uložena sankce (toliko peněžitá pokuta). Ve 2 dalších případech nebylo správní řízení dosud ukončeno. Celková výše uložených pokut dosáhla částky 261 500 Kč. Dále v celkem 7 případech nebyla řízení prozatím zahájena, neboť jsou Úřadem činěny patřičné kroky v rámci přípravného řízení.

V roce 2015 došlo k zastavení řízení pouze v jediném případě. Ve 22 dalších případech byla věc odložena nebo správní řízení nebylo zahájeno (ve 13 případech u fyzických osob, v 9 případech u právnických osob). Ve 24 případech byla věc z důvodu nepříslušnosti postoupena k projednání příslušnému služebnímu funkcionáři.

**Správní řízení v roce 2015**

| | Fyzická osoba | Právnická osoba | Celkem |
|---|---|---|---|
| **Ukončená správní řízení** | 27 | 11 | **38** |
| **Počet uložených sankcí** | 27 | 10 | **37** |
| **Zastavená správní řízení** | 0 | 1 | **1** |
| **Dosud neukončená správní řízení** | 2 | 0 | **2** |

V souladu se směrnicí ředitele Úřadu č. 5/2013, o zadávání veřejných zakázek v Národním bezpečnostním úřadu, ve znění pozdějších předpisů, odpovídá za závazný postup Úřadu v oblasti zadávání veřejných zakázek odbor právní a legislativní. Právní oddělení odboru právního a legislativního tak mj. odpovídá za stanovení správného postupu při zadávání veřejných zakázek a dohled nad dodržováním zásad zadávání veřejných zakázek podle zákona č. 137/2006 Sb., o veřejných zakázkách, ve znění pozdějších předpisů. Převážnou většinu veřejných zakázek zadávaných Úřadem v roce 2015 tvořily z hlediska objemu finančních prostředků veřejné zakázky malého rozsahu, které jsou zadávány prostřednictvím elektronického tržiště Gemin, kde jsou také údaje o všech těchto veřejných zakázkách zveřejněny. Odbor právní a legislativní se k zadání těchto veřejných zakázek vyjadřoval prostřednictvím schvalovacího nástroje v elektronickém tržišti, u zakázek malého rozsahu s plněním nad 500 000 Kč bez DPH vydává k zadání ještě zvláštní souhlas. V případě podlimitních a nadlimitních veřejných zakázek odbor právní a legislativní přímo vede zadávací řízení.

V oblasti právní činnosti bylo v roce 2015 dále uzavřeno cca 100 smluv nebo dodatků k již existujícím smlouvám s externími subjekty, jejichž předmětem je především zajištění činností a dodávek nezbytných pro plnění stanovených úkolů Úřadu.

Součást právní činnosti tvoří rovněž vyřizování nároků na náhradu škody způsobené nezákonným rozhodnutím nebo nesprávným úředním postupem, podle zákona č. 82/1998 Sb., o odpovědnosti státu za škodu způsobenou při výkonu veřejné moci rozhodnutím nebo nesprávným úředním postupem, ve znění pozdějších předpisů. V současnosti probíhá řízení ve věci uplatnění nároku na náhradu této škody se 3 žadateli. Dále je právním oddělením průběžně 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.

Odbor právní a legislativní dále vypracoval metodický návod postupu vydávání opatření obecné povahy podle části šesté zákona č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů, který byl příslušným organizačním celkem Úřadu aktivně využíván ve všech fázích určování prvků kritické informační infrastruktury na území České republiky v oblasti kybernetické bezpečnosti v odvětví „komunikační a informační systémy“. Odbor právní a legislativní rovněž poskytoval příslušnému organizačnímu celku Úřadu dodatečnou právní podporu a následnou kontrolu postupu podle citované části správního řádu.

## 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 2015*

V roce 2015 byly vyvíjeny následující aktivity v rámci sjednávání mezinárodních smluv:

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

  V roce 2015 pokračovalo expertní jednání o smlouvě.

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

  Vzhledem k tomu, že v Nizozemském království došlo ke změně zákona upravujícího ochranu utajovaných informací, bylo dohodnuto znovu provést expertní jednání. Nizozemská strana však nebyla připravena v roce 2015 toto zahájit.

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

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

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

  V roce 2015 si Úřad s tureckou stranou vyměnil texty smlouvy.

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

  Expertní jednání probíhají.

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

  Obě strany si vyměnily návrhy na sjednání smlouvy, expertní jednání se plánuje až na rok 2016.

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

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

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

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

*2.2.1.2. Výhled na rok 2016*

V roce 2016 Úřad předpokládá dokončení expertních jednání s Belgií, Nizozemskem, Tureckem, USA a Spojenými arabskými emiráty. Dále se očekává zahájení jednání s Maltou, Irákem a Spojeným královstvím.

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

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

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

Zástupci skupiny TEMPEST se zúčastnili několika mezinárodních setkání, kde prezentovali výsledky projektů vědecké a výzkumné činnosti Úřadu včetně reálných funkčních produktů vyvinutých ve spolupráci s českými výrobci. Současně bylo pracoviště TEMPEST navštíveno několika zahraničními delegacemi, přičemž hlavním bodem jejich zájmu byl nový unikátní měřící systém rovněž vyvinutý v rámci vědecké a výzkumné činnosti Úřadu.

### 2.2.3. Mezinárodní aktivity v oblasti kybernetické bezpečnosti

Rok 2015 byl ve znamení prohlubování spolupráce se strategickými partnery (Izrael, USA, Korejská republika) a dalšími zahraničními partnery (Itálie, Německo, Lucembursko, Rumunsko, Kanada, Estonsko). Tradičními partnery Úřadu jsou orgány a agentury Evropské unie (EU), Severoatlantické aliance (NATO) a dalších mezinárodních organizací. Další rozvoj zaznamenala Středoevropská platforma pro kybernetickou bezpečnost – Central European Cyber Security Platform (CECSP).

V rámci struktur EU pokračoval Úřad v jednáních o směrnici o bezpečnosti sítí a informací, představené Evropskou komisí v únoru 2013. Konečný návrh byl na úrovni COREPER členskými státy schválen 18. prosince 2015 (viz kap. 2.1.2.).

Práce pokračovala i ve skupině Přátel předsednictví pro kybernetické otázky (Friends of Presidency on Cyber Issues), kde jsou diskutována horizontální témata od kybernetické obrany po správu internetu a která sleduje implementaci Strategie kybernetické bezpečnosti Evropské unie, nebo s Evropskou obrannou agenturou, kde se angažuje zejména Ministerstvo obrany. Úřad je zastoupen i v Evropské agentuře pro bezpečnost sítí a informací (ENISA) prostřednictvím účasti na formálních a neformálních jednáních. Členy představenstva ENISA jsou, jako člen a alternát, 2 zástupci Úřadu, kteří se podílejí na schvalování programu, plánu prací a rozpočtu ENISA.

V rámci prohlubování a upevňování vztahů s NATO se Úřad jako gestor aktivně podílel na přípravě nového formátu memoranda o porozumění a spolupráci v oblasti kybernetické obrany. Dne 12. října 2015 jej podepsal ředitel úřadu Ing. Dušan Navrátil a náměstek generálního tajemníka NATO Sorin Ducaru. ČR se stala prvním členským státem NATO, který toto memorandum podepsal.

V rámci spolupráce mezi ČR a NATO Cooperative Cyber Defence Centre of Excellence v estonském Tallinnu, jehož posláním je přispívat k posilování kybernetické obrany a zlepšovat spolupráci a sdílení informací mezi účastnickými státy a NATO, v právní a politické divizi centra i nadále působil pracovník vyslaný Úřadem, který se autorsky podílel na několika publikacích centra, na jeho výzkumných projektech a organizaci cvičení a seminářů jím pořádaných. Tato spolupráce umožňuje ČR podílet se na výzkumných a vzdělávacích projektech CCDCOE a těžit z jejich výsledků.

Aktivity v rámci Středoevropské platformy pro kybernetickou bezpečnost (CECSP), jejímž je ČR zakládajícím členem, probíhaly pod maďarským předsednictvím. Uskutečnilo se 1 zasedání na politické a 1 na technické úrovni. Dále bylo uspořádáno 1 komunikační cvičení. V prosinci 2015 na technickém setkání platformy zástupci Úřadu představili partnerům některé své projekty, např. na tvorbu koordinačního centra pro české bezpečnostní týmy, webového portálu pro sdílení informací nebo ICS-SCADA laboratoře, sdíleli počet incidentů zpracovaných za měsíc a další české reálie. Informovali také o podobě a průběhu národního cvičení Cyber Czech 2015.

V rámci bilaterální spolupráce ČR navázala a prohloubila strategická partnerství s Izraelem, Spojenými státy americkými a Korejskou republikou.

Dne 26. února 2015 předseda vlády Bohuslav Sobotka podepsal během své návštěvy Koreje s korejskou prezidentkou Pak Kun-hje Společnou deklaraci o strategickém partnerství, která obsahuje i pasáž o spolupráci v oblasti kybernetické bezpečnosti.

Na základě společné deklarace podepsané během společného zasedání české a izraelské vlády v Jeruzalémě 25. listopadu 2014, navrhl ředitel partnerského úřadu Israeli National Cyber Bureau Dr. Eviatar Matania uspořádat seminář ke kybernetické bezpečnosti pro seniorní představitele státní správy ČR. Seminář se uskutečnil ve dnech 8. až 10. září 2015 v Tel Avivu za účasti 31 představitelů řady ministerstev, Parlamentu ČR, zpravodajských služeb, Policie ČR, Armády ČR a Nejvyššího státního zastupitelství na úrovni náměstků ministrů a ředitelů. Delegace byla vedena místopředsedou Poslanecké sněmovny Ing. Janem Bartoškem. Izraelské straně se podařilo shromáždit vynikající přednášející, a to jak z vládní, tak i soukromé sféry. Seminář postihl veškeré aspekty kybernetické bezpečnosti a účastníci semináře dostali hodnotné informace, které jim usnadní přijímat rozhodnutí tykající se této oblasti. Uvedený seminář posílil dobré vztahy mezi ČR a Státem Izrael.

Ve vztahu s USA se posilovala spolupráce zejména s Federal Bureau of Investigation a Department of Homeland Security. V oblasti právní úpravy zástupci Úřadu předávali zkušenosti zástupcům Kongresu a koordinátorovi Bílého domu pro otázky kybernetické bezpečnosti.

V rámci několika evropských projektů poskytoval Úřad v roce 2015 asistenci státům, které budují systém kybernetické bezpečnosti. Za tím účelem se uskutečnily workshopy o institucionálním, právním a technickém rámci kybernetické bezpečnosti pro Jordánsko, Srbsko a Bosnu a Hercegovinu. Zástupci Úřadu také v rámci instrumentu TAIEX Evropské komise prezentovali na žádost ukrajinské vlády v Kyjevě. V rámci projektu Enhancing Cyber Security zástupce Úřadu pravidelně přednáší vládním bezpečnostním týmům v Makedonii, Moldavsku a Kosovu. V roce 2015 proběhly 2 workshopy pro členy CERT/CSIRT týmů těchto zemí, první zaměřený na budování CERT/CSIRT týmu z hlediska technického a organizačního (působnost, typy útoků, nabízené služby, techniky shromažďování informací, personální náročnost), druhý na forenzní analýzu a table-top cvičení simulující útoky na součásti státní infrastruktury a phishingovou kampaň z interního pohledu CERT/CSIRT týmu.

Úřad je prostřednictvím vládního pracoviště GovCERT.CZ již druhým rokem akreditovaným členem evropského sdružení Trusted Introducer. Tato instituce, působící v rámci evropské organizace GÉANT (dříve TERENA), sdružuje bezpečnostní týmy vládní, národní, akademické a komerční sféry z celého světa. V rámci svého členství se GovCERT.CZ účastní pravidelných neveřejných setkání komunity, která slouží ke sdílení know-how, vyvíjených aplikací, zkušeností a informací o řešených incidentech.

Úřad se v roce 2015 účastnil řady mezinárodních cvičení. Jednalo se např. o:

- mezinárodní cvičení orgánů krizového řízení NATO Crisis Management Exercise,
- Locked Shields – největší mezinárodní technické cvičení kybernetické bezpečnosti,
- Cyber Coalition – alianční cvičení kybernetické bezpečnosti, kterého se účastnilo více než 700 odborníků na kybernetickou bezpečnost z členských a partnerských zemí NATO.

V roce 2015 Úřad uskutečnil první cvičení na klíč pro zahraničního partnera. Jednalo se o americké ministerstvo obrany a velitelství kybernetických sil USA (US CYBERCOM), na jehož žádost Úřad vyslal 2 experty a připravil modul do vzdělávacího programu budoucích členů velitelství

kybernetických sil a dalších složek. Událost měla kladný ohlas a představitelé Pentagonu projevili zájem o opakování i v roce 2016.

## 2.3. PERSONÁLNÍ BEZPEČNOST

V oblasti personální bezpečnosti Úřad v roce 2015, stejně tak jako v letech minulých, prováděl zejména bezpečnostní řízení o žádostech fyzických osob, vydával osvědčení fyzické osoby a osvědčení fyzické osoby pro cizí moc, potvrzující cizí moci vydání osvědčení fyzické osoby a vydával rozhodnutí o nevydání osvědčení fyzické osoby.

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

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

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

Součinnost, kterou v rámci bezpečnostního řízení poskytují Úřadu zpravodajské služby, Policie ČR a další spolupracující orgány státu a právnické osoby, byla v roce 2015 standardně 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 podepsána dohoda o postupu při poskytování informací mezi Národním bezpečnostním úřadem a Ministerstvem financí ČR ve věcech údajů souvisejících se správou daní a dále dodatek č. 1 ke smlouvě o získávání informací z evidencí Centrálního depozitáře cenných papírů, a.s. prostřednictvím Information Service Broker.

Další oblastí činnosti Úřadu byla spolupráce s úřady cizí moci, které mají v působnosti ochranu utajovaných informací, při provádění vlastních bezpečnostních řízení (vyžadování informací). Úřad u partnerských úřadů vyžádal informace ke 273 osobám a na základě jejich žádostí prováděl šetření k 56 osobám, které byly v daném státě prověřovány pro přístup k utajovaným informacím.

### 2.3.1. Bezpečnostní řízení o žádostech fyzických osob

Ze statistických údajů ohledně bezpečnostního řízení o žádostech fyzických osob, které jsou přehledně shrnuty v kapitole 2.3.5., vyplývá, že v loňském roce bylo přijato 6 236 žádostí o vydání osvědčení fyzické osoby, to je o 1 169 žádostí více než v předchozím roce. Z těchto údajů je zřejmé, že v roce 2015 došlo ke značnému nárůstu počtu přijatých žádostí oproti předchozímu roku, a to o více jak 23 %.

Největší podíl tvořily žádosti o vydání osvědčení fyzické osoby pro stupeň utajení Tajné (51 %) a pro stupeň utajení Důvěrné (46 %). Žádosti byly na rozdíl od předcházejících let podávány poměrně rovnoměrně v průběhu celého roku, přičemž nejvíce žádostí bylo podáno v měsíci červnu, a to v počtu 701 žádostí (viz graf Celkové počty přijatých žádostí v jednotlivých měsících roku 2015).

Celkem bylo v loňském roce rozhodnuto v 6 161 případech o vydání osvědčení fyzické osoby a v 16 případech o nevydání osvědčení. Ve 218 případech pak bylo bezpečnostní řízení zastaveno. Nejčastějším důvodem zastavení bezpečnostního řízení bylo zpětvzetí žádosti účastníkem řízení (93 případů). Významný podíl na zastavení bezpečnostního řízení měla také povinnost odpovědné osoby neprodleně oznámit Úřadu pominutí skutečností odůvodňujících nutnost přístupu fyzické osoby k utajovaným informacím (79 případů). Úřad tak mohl probíhající bezpečnostní řízení zastavit, neboť důvod řízení zanikl. Tím došlo ke snížení nákladů Úřadu a s ním spolupracujících orgánů a organizací, neboť nebylo nutné v těchto případech bezpečnostní řízení dokončovat. Současně tím byl posílen princip „need to know“, jehož hlavním smyslem je, aby k utajovaným informacím mohly mít přístup pouze osoby, které tyto informace k výkonu své pracovní nebo jiné obdobné činnosti nezbytně potřebují znát.

### 2.3.2. Prověřování splňování podmínek po vydání osvědčení fyzické osoby

Významný objem činnosti Úřadu v oblasti personální bezpečnosti souvisel s prověřováním, zda fyzická osoba, která je držitelem osvědčení fyzické osoby, i nadále splňuje podmínky pro jeho vydání. Prověřeno takto bylo celkem 3 292 držitelů osvědčení. Tato činnost byla standardně prováděna před vydáním osvědčení pro cizí moc a v případech, kdy Úřad obdržel od zpravodajských služeb, Ministerstva vnitra nebo Policie ČR informace, jejichž obsah nasvědčoval tomu, že držitel osvědčení fyzické osoby by mohl přestat splňovat podmínky pro jeho vydání, nebo tyto informace vyplynuly z nahlášených změn samotným držitelem osvědčení fyzické osoby, případně je Úřad získal přímo svou vlastní činností (např. z průběžného monitoringu tzv. otevřených zdrojů). Nezanedbatelnou část takto prověřených případů tvořilo rovněž periodické ověřování realizované po dobu platnosti příslušného osvědčení. Ve 126 případech toto prověřování vyústilo v zahájení řízení o zrušení platnosti osvědčení fyzické osoby, které bylo ve 40 případech ukončeno vydáním rozhodnutí o zrušení platnosti osvědčení fyzické osoby (viz kap. 2.3.5. Statistické přehledy).

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

Jak již bylo uvedeno v kapitolách 2.3.1. a 2.3.2., v minulém roce v 16 případech nebylo žadateli osvědčení vydáno a ve 40 případech bylo rozhodnuto o zrušení platnosti osvědčení.

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

Toto bezpečnostní riziko samo o sobě zahrnuje velký rozsah faktických důvodů. V roce 2015 měly tyto důvody opětovně příčinnou souvislost se skutečnostmi vyplývajícími z trestního či přestupkového řízení a dále ze širokého spektra porušování nebo obcházení právních předpisů, kdy převážnou motivací k takovémuto chování bylo nejen získání majetkového či jiného prospěchu, ale i posílení a utužení negativních interpersonálních vazeb (klientelismus), tedy bez zaznamenání okamžitého prospěchu v majetkové sféře dotčených osob.

Nejčastějším důvodem shledání uvedeného bezpečnostního rizika však opětovně byly případy neodpovědného až laxního přístupu žadatelů či držitelů osvědčení k jejich závazkovým vztahům, díky němuž se ocitli v neudržitelné finanční, potažmo majetkové situaci, kterou řešili přistupováním k novým závazkům již s vědomím předchozí nesplácet, což může mít zásadní dopad na jejich ochotu poskytnout utajovaným informacím dostatečnou ochranu, kdy nelze vyloučit opatření si „vedlejších příjmů“ na úhradu takovýchto závazků.

Ostatní rizika uvedená v § 14 odst. 2 a 3 zákona byla konstatována v roce 2015 ojediněle. Bezpečnostní riziko podle § 14 odst. 2 písm. b) zákona, tedy činnost spočívající v potlačování základních lidských práv a svobod však bylo ve srovnání s rokem 2014 opětovně v několika případech konstatováno v souvislosti s jednáním žadatelů o vydání osvědčení před rokem 1989. Kromě toho bylo zmíněné bezpečnostní riziko Úřadem rovněž identifikováno u účastníků řízení i v nedávné minulosti, např. ve formě pravicového extremismu. Také v roce 2015 byly zjištěny případy výskytu dalšího obligatorního bezpečnostního rizika – závažná nebo opakovaná činnost proti zájmům ČR, především pak zájmu na ochranu ekonomiky ČR, kdy Úřad při svém rozhodování vycházel jak ze zpráv příslušných zpravodajských služeb, tak orgánů činných v trestním řízení.

Dalším, byť ve srovnání s předešlými roky méně častým důvodem zrušení platnosti osvědčení fyzické osoby bylo i v roce 2015 nesplnění podmínky bezúhonnosti podle § 6 odst. 2 písm. c) zákona, přičemž stále převažuje řízení motorových vozidel pod vlivem návykových látek.

### 2.3.4. Přehled ostatních důvodů zániku platnosti osvědčení fyzické osoby

V uplynulém období zanikla platnost celkem 11 242 osvědčení, přičemž největší část případů představoval zánik uplynutím doby platnosti osvědčení v počtu 5 939 a doručením nového osvědčení fyzické osoby v celkovém počtu 4 072. Významným se v uplynulém hodnoceném období také jevil zánik platnosti osvědčení fyzické osoby projevem vůle držitele osvědčení, tzn., že držitel osvědčení vrátil, neboť už nadále nepotřeboval mít přístup k utajované informaci (884 případy).

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

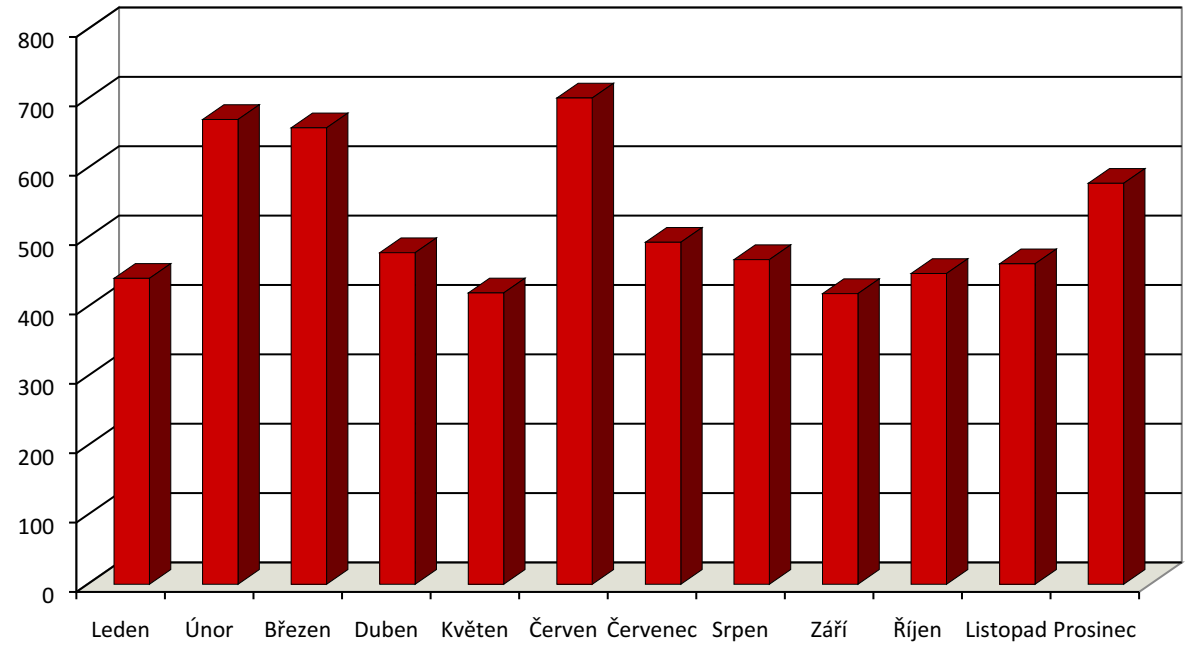
Počet případů zániku platnosti osvědčení fyzické osoby v roce 2015 podle jednotlivých důvodů je přehledně uveden v následující kapitole 2.3.5.

### 2.3.5. Statistické přehledy

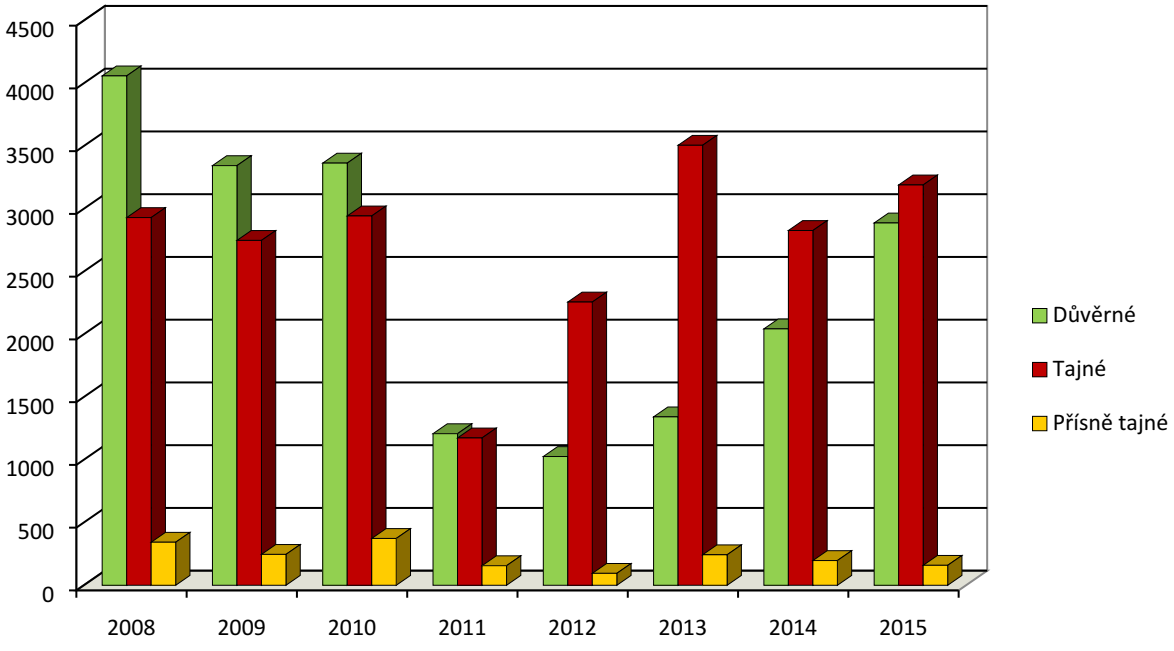
**Přijaté žádosti a ukončená bezpečnostní řízení v roce 2015**

| | Důvěrné | Tajné | Přísně tajné | Celkem |
|---|---|---|---|---|
| **Přijaté žádosti** | 2 887 | 3 190 | 159 | **6 236** |
| **Osvědčení vydáno** | 3 014 | 2 983 | 164 | **6 161** |
| **Osvědčení nevydáno** | 7 | 6 | 3 | **16** |
| **Řízení zastaveno** | 128 | 86 | 4 | **218** |

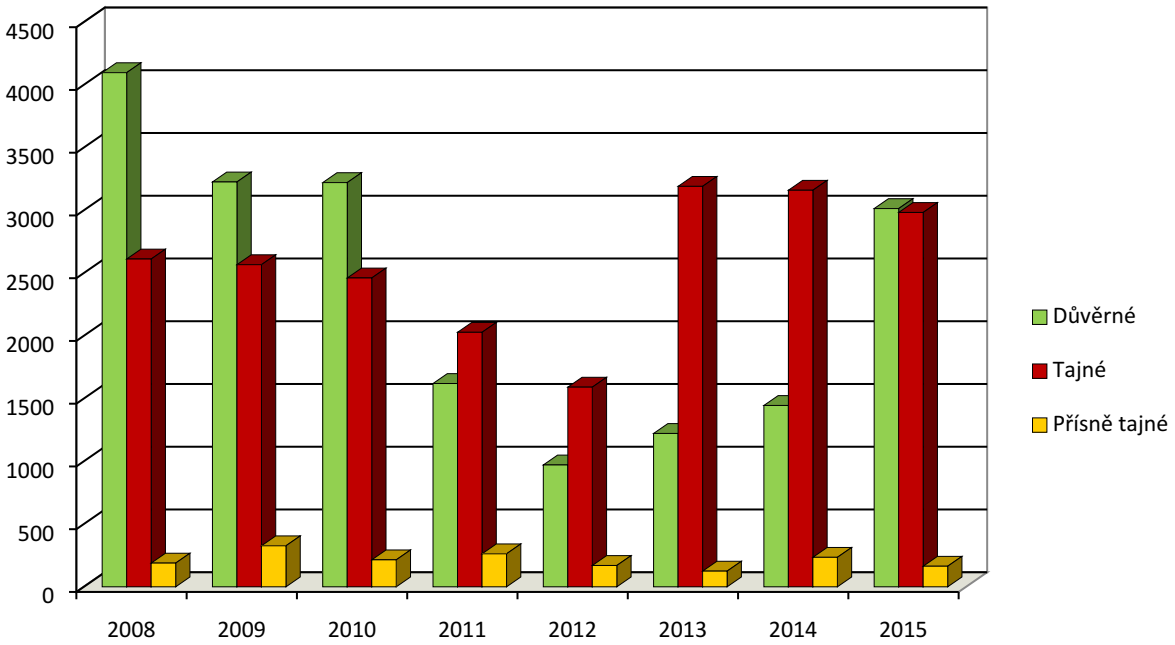
**Celkové počty přijatých žádostí v jednotlivých měsících roku 2015**



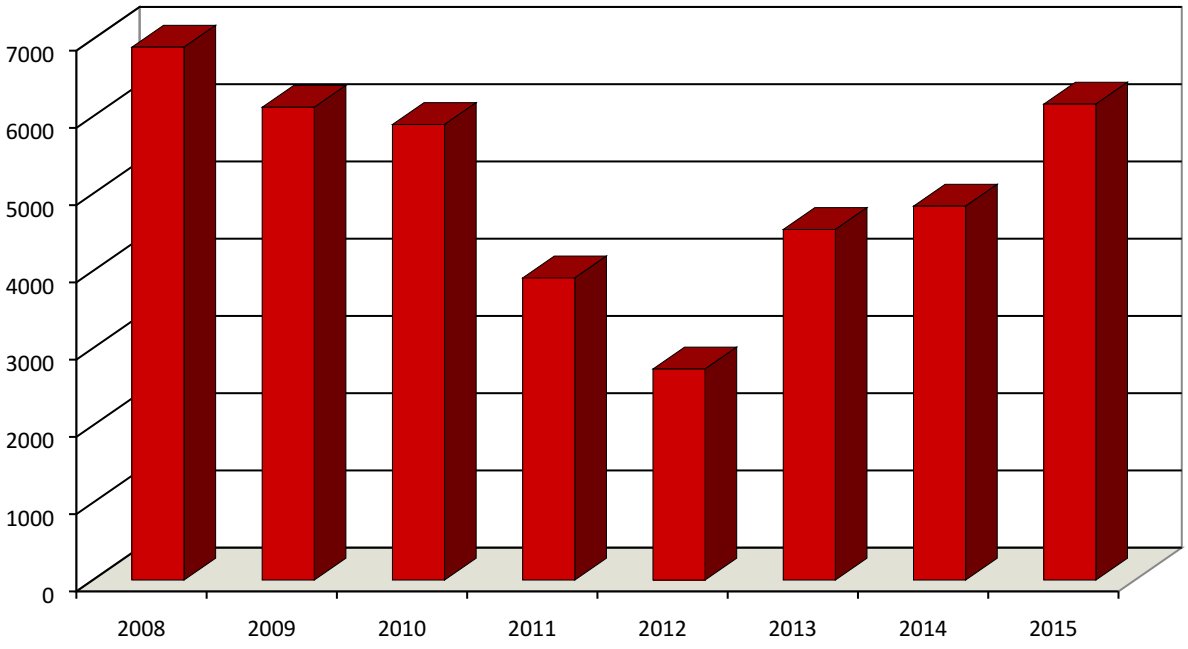

**Přijaté žádosti o vydání osvědčení fyzické osoby v letech 2008 až 2015**

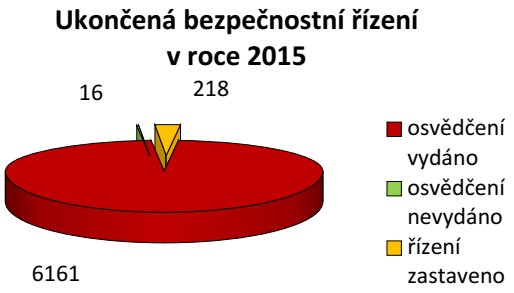


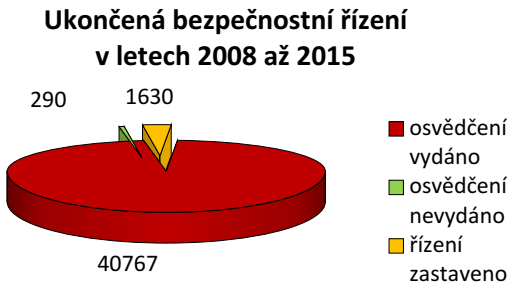
**Vydaná osvědčení fyzické osoby v letech 2008 až 2015**




**Vydaná osvědčení fyzické osoby v letech 2008 až 2015 celkem**



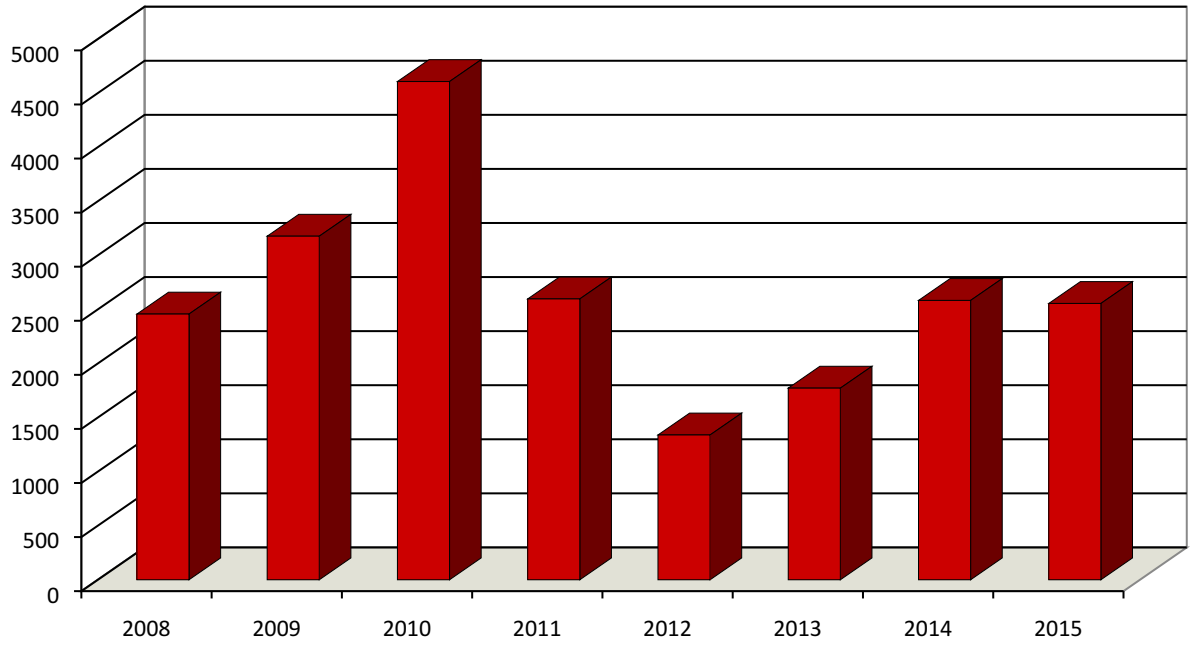


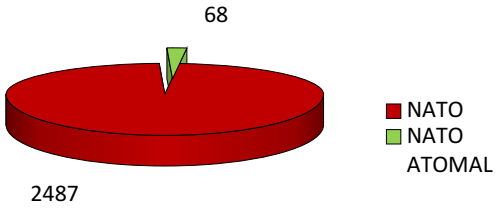

**Vydaná osvědčení fyzické osoby pro cizí moc v roce 2015**

| | |
|---|---|
| **COSMIC TOP SECRET** | 193 |
| **COSMIC TOP SECRET ATOMAL** | 53 |
| **NATO SECRET** | 2 040 |
| **NATO SECRET ATOMAL** | 15 |
| **NATO CONFIDENTIAL** | 254 |
| **Celkem** | **2 555** |

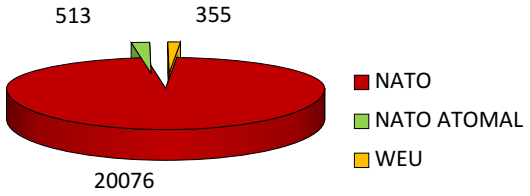
**Vydaná osvědčení fyzické osoby pro cizí moc v letech 2008 až 2015 celkem**



**Osvědčení pro cizí moc v roce 2015**




**Osvědčení pro cizí moc v letech 2008 až 2015[1)]**




**Zánik platnosti osvědčení fyzické osoby podle důvodu v roce 2015**

| | |
|---|---|
| **Uplynutí doby platnosti osvědčení** | 5 939 |
| **Zrušení platnosti osvědčení** | 40 |
| **Úmrtí držitele osvědčení** | 13 |
| **Ohlášení odcizení nebo ztráty osvědčení** | 36 |
| **Poškození osvědčení** | 12 |
| **Změna některého z údajů uvedených v osvědčení** | 221 |
| **Vrácení osvědčení** | 884 |
| **Doručení nového osvědčení** | 4 070 |
| **Vznik služebního nebo pracovního poměru u zpravodajské služby** | 27 |
| **Celkem** | **11 242** |

**Zastavení bezpečnostního řízení v roce 2015**

| | |
|---|---|
| **Nedání souhlasu podle § 107 zákona** | 4 |
| **Neodstranění nedostatků v žádosti ve stanovené lhůtě** | 35 |
| **Uvedení nepravdivé nebo neúplné výpovědi** | 5 |
| **Nesplnění podmínek – dosažení 18 let věku, svéprávnosti, bezúhonnosti** | 1 |
| **Úmrtí žadatele** | 1 |
| **Oznámení odpovědné osoby, že pominuly skutečnosti, kterými byla žádost odůvodněna** | 79 |
| **Zpětvzetí žádosti** | 93 |
| **Celkem** | **218** |

## 2.3.6. Personální projekt

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

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

schváleného v tomto usnesení a poskytovat řediteli Úřadu součinnost při zpracovávání vyjádření k personálním projektům a jejich ověřování. Předmětný materiál stanovuje jednotný obsah, formu a strukturu personálních projektů a upravuje i způsob jejich hodnocení Úřadem.

Účelem zpracování personálních projektů je získat celkový přehled o situaci na úseku personální bezpečnosti v oblasti ochrany utajovaných informací, zhodnotit stav z hlediska množství fyzických osob, které žádají o vydání osvědčení fyzické osoby, ve vztahu ke skutečným potřebám a četnosti výskytu utajovaných informací u ústředních orgánů státní správy a informovat o eventuálních nedostatcích a možných problémech vyskytujících se v personální bezpečnosti.

V roce 2015 bylo vyjádření Úřadu k personálním projektům předloženo do připomínkového řízení dotčeným ministerstvům a orgánům státní správy. Z připomínkových míst uplatnilo zásadní připomínky Ministerstvo obrany. Při vypořádání připomínek nedošlo k odstranění rozporu. Rozpor koncepční povahy se týkal počtu žádostí, které tento rezort předpokládal na rok 2016. Ministerstvo obrany trvalo na celkovém počtu 3 802 žádostí s předpokladem, že tento počet nebude ani v následujících letech nižší. Úřad nebyl schopen při své současné personální kapacitě tento počet žádostí akceptovat, protože by nemohl při celkovém počtu žádostí od všech oprávněných subjektů garantovat dostání všech svých zákonných povinností při realizaci bezpečnostního řízení. Materiál se tak předkládal pro jednání vlády ČR s rozporem. Navrhovaným řešením k odstranění rozporu bylo posílení personální kapacity Úřadu o minimálně 8 systemizovaných pracovních míst.

Dne 14. prosince 2015 vláda ČR materiál projednala a vydala usnesení č. 1034, kterým schválila předložené personální projekty a posílení personální kapacity Úřadu. 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 a do 30. června 2016 předložit vládě návrh na řešení požadavků dalšího navyšování počtu žádostí o vydání osvědčení fyzické osoby pro léta 2017 a následující ve vztahu k personální kapacitě Úřadu.

## 2.4. BEZPEČNOSTNÍ ZPŮSOBILOST

V roce 2015 Úřad vedl, ve smyslu části čtvrté zákona, bezpečnostní řízení k žádostem o vydání dokladu o bezpečnostní způsobilosti fyzických osob (dále jen „doklad“), vydával doklad, vydával rozhodnutí o nevydání dokladu, dále prověřoval, zda fyzické osoby, které již jsou držiteli dokladu, i nadále splňují podmínky pro jeho vydání, vydával rozhodnutí o zrušení platnosti dokladu a realizoval řadu dalších úkonů s tím spojených, např. zakládání, vedení, doplňování, evidenci a vyřazování bezpečnostních svazků, vedení evidence fyzických osob, které jsou držiteli dokladu atd.

Většinu podaných žádostí o vydání dokladu tvořily žádosti související s výkonem citlivé činnosti v oblasti atomového zákona a zahraničního obchodu s vojenským materiálem.

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

V roce 2015 Úřad participoval na připravované rozsáhlé novele atomového zákona, která mimo jiné klade i větší nároky na bezpečnostní způsobilost osob, které vstupují do vyhrazených prostor jaderných zařízení, a na návrhu zákona o bezpečnostní činnosti, který upravuje oblast soukromých bezpečnostních služeb a nově vymezuje citlivou činnost pro tyto služby.

### 2.4.1. Statistické přehledy

**Přehled přijatých žádostí a ukončených bezpečnostních řízení v roce 2015**

| Citlivá činnost podle | Přijaté žádosti | Doklad vydán | Doklad nevydán | Řízení zastaveno | Zrušení platnosti dokladu |
|---|---|---|---|---|---|
| **§ 8 zákona č. 38/1994 Sb.**[2)] | 121 | 125 | 4 | 10 | 0 |
| **§ 2a zákona č. 18/1997 Sb.**[3)] | 157 | 142 | 0 | 3 | 0 |
| **§ 6 zákona č. 229/2013 Sb.**[4)] | 0 | 1 | 0 | 57 | 0 |
| **§ 25c odst. 10 zákona č. 61/1988 Sb.**[5)] | 3 | 2 | 0 | 0 | 0 |
| **§ 157a zákona č. 137/2006 Sb.**[6)] | 5 | 7 | 0 | 2 | 0 |
| **§ 2a zákona č. 312/2006 Sb.**[7)] | 5 | 6 | 0 | 0 | 0 |
| **Ostatní** | 3 | 3 | 0 | 0 | 0 |
| **Celkem** | **294** | **286** | **4** | **72** | **0** |

## 2.5. PRŮMYSLOVÁ BEZPEČNOST

Mezi hlavní činnosti, které Úřad realizoval v oblasti průmyslové bezpečnosti v roce 2015, patří zejména provádění bezpečnostních řízení o žádostech podnikatelů o vydání osvědčení podnikatele, v jejichž závěru Úřad vydával osvědčení podnikatele nebo rozhodnutí o nevydání osvědčení podnikatele. Úřad dále přijímal žádosti podnikatelů o vydání osvědčení podnikatele pro cizí moc a při splnění zákonem stanovených podmínek vydával osvědčení podnikatele pro cizí moc, potvrzující cizí moci provedení bezpečnostního řízení u podnikatele a vydání osvědčení podnikatele.

Ve vztahu k podnikatelům, kteří jsou držiteli osvědčení podnikatele, se činnost Úřadu zaměřovala především na provádění úkonů k prověřování, zda i nadále splňují podmínky stanovené zákonem pro vydání osvědčení podnikatele, a to v souvislosti s hlášeními změn údajů uvedených v žádosti podnikatele oznamovaných jednotlivými držiteli osvědčení podnikatele, skutečnostmi získanými z vlastní činnosti Úřadu nebo informacemi poskytnutými Úřadu orgány státu či právnickými nebo fyzickými osobami. V návaznosti na zjištěné skutečnosti Úřad vedl řízení o zrušení platnosti

[2)] Zákon č. 38/1994 Sb., o zahraničním obchodu s vojenským materiálem a o doplnění zákona č. 455/1991 Sb., o živnostenském podnikání (živnostenský zákon), ve znění pozdějších předpisů, a zákona č. 140/1961 Sb., trestní zákon, ve znění pozdějších předpisů, ve znění pozdějších předpisů.
[3)] Zákon č. 18/1997 Sb., o mírovém využívání jaderné energie a ionizujícího záření (atomový zákon) a o změně a doplnění některých zákonů, ve znění pozdějších předpisů.
[4)] Zákon č. 229/2013 Sb., o nakládání s některými věcmi využitelnými k obranným a bezpečnostním účelům na území České republiky (zákon o nakládání s bezpečnostním materiálem), ve znění zákona č. 64/2014 Sb.
[5)] Zákon č. 61/1988 Sb., o hornické činnosti, výbušninách a o státní báňské správě, ve znění pozdějších předpisů.
[6)] Zákon č. 137/2006 Sb., o veřejných zakázkách, ve znění pozdějších předpisů.
[7)] Zákon č. 312/2006 Sb., o insolvenčních správcích, ve znění pozdějších předpisů.

osvědčení podnikatele a v případech, kdy podnikatel přestal splňovat podmínky pro vydání osvědčení podnikatele, vydával rozhodnutí o zrušení platnosti takových osvědčení.

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

V roce 2015 i nadále probíhala velmi dobrá a efektivní součinnost Policie ČR, zpravodajských služeb a dalších spolupracujících orgánů státu a právnických osob s Úřadem v rámci prováděných bezpečnostních řízení i v rámci prověřování a ověřování splňování podmínek pro vydání osvědčení podnikatele držiteli osvědčení.

### 2.5.1. Bezpečnostní řízení o žádostech podnikatelů

V průběhu roku 2015 bylo Úřadem přijato 81 žádostí podnikatelů o vydání osvědčení podnikatele. Z tohoto počtu bylo k 31. prosinci 2015 rozhodnuto o 52 žádostech, u zbylých 29 žádostí k tomuto datu bezpečnostní řízení o žádosti podnikatele probíhala.

Ve srovnání s rokem 2014 došlo k nepatrnému nárůstu počtu přijatých žádostí, a to celkem o 3 žádosti. Z hlediska struktury podaných žádostí byl rok 2014 charakterizován zvýšeným počtem žádostí podnikatelů o vydání osvědčení podnikatele podaných podle § 96 odst. 4 zákona, tj. podaných podnikateli, kteří i bezprostředně po uplynutí doby platnosti jeho dosavadního osvědčení mají mít přístup k utajovaným informacím. Počty zahájených bezpečnostních řízení jsou i nadále významně ovlivňovány změnou právních předpisů účinnou od 1. ledna 2012, zejména pak zrušením bezpečnostního řízení pro přístup podnikatele k utajované informaci stupně utajení Vyhrazené. Dalším výrazným faktorem, který se promítá do počtu podaných žádostí, jsou změny ve vývoji podnikatelského prostředí, které spočívají v transformacích obchodních společností formou různých typů přeměn nebo se projevují ve formě úpadků nebo zániků obchodních společností.

### 2.5.2. Prověřování splňování podmínek po vydání osvědčení podnikatele

V roce 2015 probíhalo standardním způsobem prověřování, zda držitelé osvědčení podnikatele nadále splňují zákonem stanovené podmínky pro jejich vydání.

Prověřování splňování podmínek je významným objemem činnosti Úřadu. Tato činnost je prováděna u všech držitelů osvědčení podnikatele. Z pohledu skladby ji lze rozdělit na standardní periodické prověřování, které je odvozeno od pravidelného ročního hlášení změn všemi držiteli osvědčení podnikatele (povinnost podle § 68 písm. d) zákona), dále na prověřování změn údajů oznamovaných podnikateli podle jiných ustanovení zákona (§ 68 písm. c) a f) zákona a § 69 odst. 1 písm. c) zákona), na případy, kdy Úřad obdržel od zpravodajských služeb, Ministerstva vnitra nebo Policie ČR informace, které se vztahovaly ke splňování podmínek pro vydání osvědčení podnikatele nebo jejichž obsah nasvědčoval tomu, že držitel osvědčení podnikatele by mohl přestat splňovat podmínky pro jeho vydání, případně takovéto informace Úřad získal přímo svou vlastní činností (např. z průběžného monitoringu tzv. otevřených zdrojů). Mimo uvedené druhy prověřování Úřad prováděl prověřování splňování podmínek pro vydání osvědčení podnikatele u žadatelů o vydání osvědčení pro cizí moc. Na podkladě skutečností zjištěných prověřováním bylo ve 14 případech zahájeno řízení o zrušení platnosti osvědčení podnikatele, které bylo ve 4 případech ukončeno vydáním rozhodnutí o zrušení platnosti osvědčení podnikatele (viz kap. 2.5.5. Statistické přehledy).

Prověřování splňování podmínek je současně jedním z podkladů pro výkon státního dozoru.

## 2.5.3. Analýza důvodů nevydání nebo zrušení platnosti osvědčení podnikatele

V roce 2015 rozhodl Úřad ve 2 bezpečnostních řízeních vedených o žádosti podnikatele o nevydání osvědčení podnikatele. Z hlediska struktury spočíval důvod nevydání v nesplnění podmínky podle § 16 odst. 1 písm. a) zákona.

Za totéž období Úřad rozhodl ve 4 případech o zrušení platnosti osvědčení podnikatele. Důvodem pro zrušení platnosti osvědčení bylo ve 2 případech nesplnění podmínky bezpečnostní spolehlivosti podle § 16 odst. 1 písm. b) zákona, v dalších 2 případech pak současné nesplnění podmínek podle § 16 odst. 1 písm. c) a d) zákona, tj. schopnost zabezpečit ochranu utajovaných informací, a nesplnění podmínky držení platného osvědčení fyzické osoby odpovědnou osobou podnikatele nejméně pro takový stupeň utajení, pro který žádá podnikatel o vydání osvědčení podnikatele.

## 2.5.4. Přehled ostatních důvodů zániku platnosti osvědčení podnikatele

V roce 2015 mezi důvody zániku platnosti osvědčení podnikatele převažoval zánik platnosti osvědčení podnikatele z důvodu doručení nového osvědčení podnikatele pro stejnou formu přístupu podnikatele k utajované informaci, celkem 52 případů. Druhým nejčastějším důvodem zániku platnosti osvědčení podnikatele pak byl zánik osvědčení podnikatele jeho vrácením držitelem, celkem 28 případů. Ve druhém uvedeném případu došlo oproti roku 2014 ke zvýšení počtu takto zaniklých platností osvědčení podnikatele, neboť v roce 2014 se jednalo o celkem 18 případů.

Počet případů zániku platnosti osvědčení podnikatele v roce 2015 podle jednotlivých důvodů je uveden v kapitole 2.5.5.

## 2.5.5. Statistické přehledy

**Přijaté žádosti o vydání osvědčení podnikatele v roce 2015**

| Důvěrné | Tajné | Přísně tajné | Celkem |
|---|---|---|---|
| 58 | 23 | 0 | **81** |

**Stav zpracování žádostí o vydání osvědčení podnikatele přijatých v roce 2015**

| Osvědčení vydáno | Osvědčení nevydáno | Řízení zastaveno | Probíhalo k 31. 12. 2015 | Celkem |
|---|---|---|---|---|
| 44 | 1 | 7 | 29 | **81** |

**Vydaná osvědčení podnikatele v roce 2015**

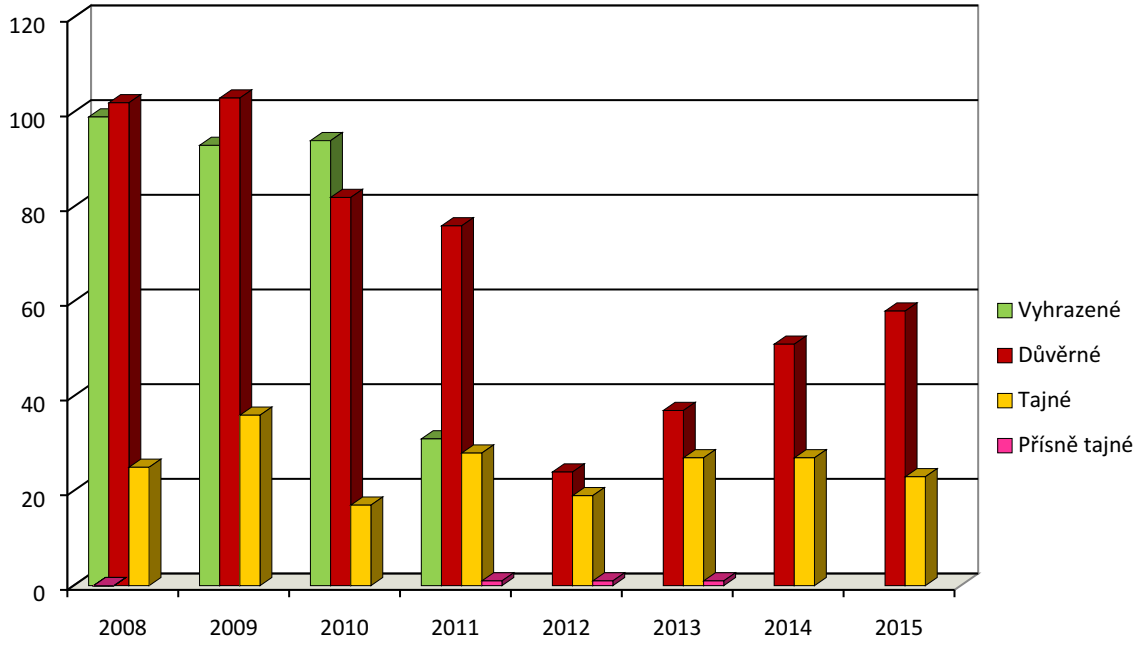
| Důvěrné | Tajné | Přísně tajné | Celkem |
|---|---|---|---|
| 74 | 37 | 0 | **111**[8)] |

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

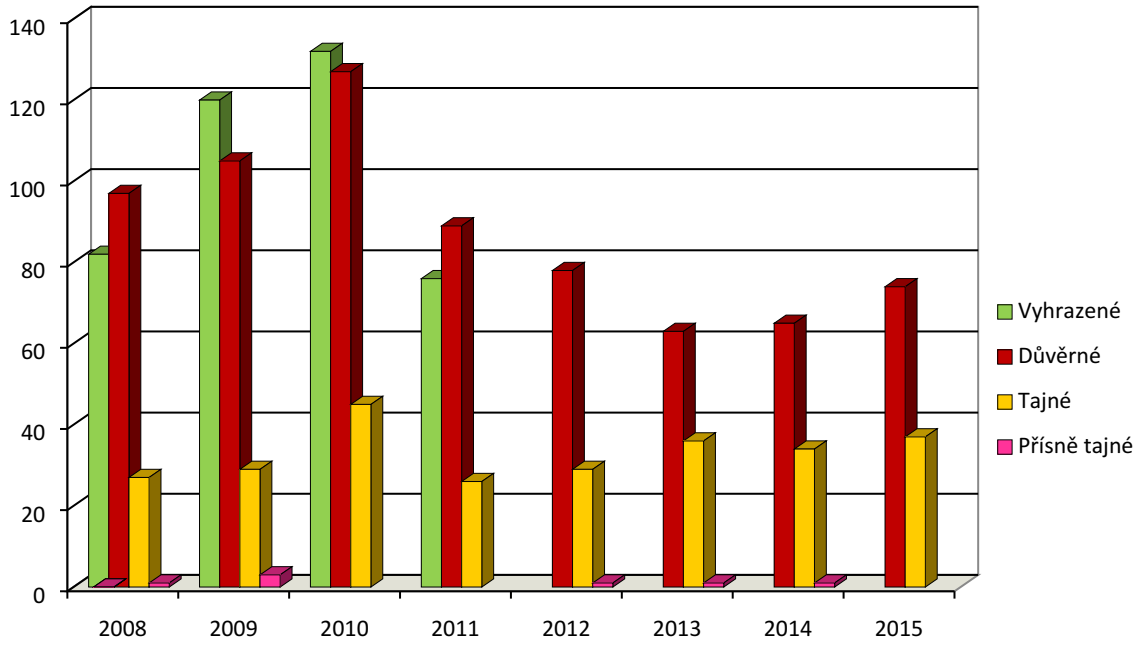
## Řízení o zrušení platnosti osvědčení podnikatele v roce 2015

| Zahájená řízení | Platnost zrušena | Řízení zastaveno | Probíhalo k 31. 12. 2015 |
|---|---|---|---|
| 14 | 4 | 11 | **15** |

### Přijaté žádosti o vydání osvědčení podnikatele v letech 2008 až 2015




### Vydaná osvědčení podnikatele v letech 2008 až 2015



**Zánik platnosti osvědčení podnikatele podle důvodu v roce 2015**

| | |
|---|---|
| **Uplynutí doby platnosti osvědčení** | 27 |
| **Zrušení platnosti osvědčení** | 4 |
| **Zrušení podnikatele** | 6 |
| **Ohlášení odcizení nebo ztráty osvědčení** | 0[9)] |
| **Poškození osvědčení** | 0[9)] |
| **Změna některého z údajů uvedených v osvědčení** | 1[9)] |
| **Vrácení osvědčení** | 28 |
| **Doručení nového osvědčení pro stejnou formu přístupu k UI** | 52 |
| **Doručení rozhodnutí o nevydání osvědčení pro stejnou formu přístupu k UI** | 0 |
| **Celkem** | **118** |

## 2.6. BEZPEČNOST INFORMAČNÍCH A KOMUNIKAČNÍCH SYSTÉMŮ A KRYPTOGRAFICKÁ OCHRANA

Úřad odpovídá za provádění certifikace informačních systémů a za schvalování projektů bezpečnosti komunikačních systémů nakládajících s utajovanými informacemi a v roli národní bezpečnostní akreditační autority dále za akreditaci lokalit informačních systémů NATO a EU rozmístěných na území ČR.

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

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

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

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

## 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 2015 dalších 124 žádostí, včetně žádostí o opakovanou certifikaci, a to 53 ze státní a 71 ze soukromé sféry. Ve 26 případech byla podána žádost o certifikaci nově budovaného informačního systému, pouze 9 takových žádostí pocházelo ze státní správy.

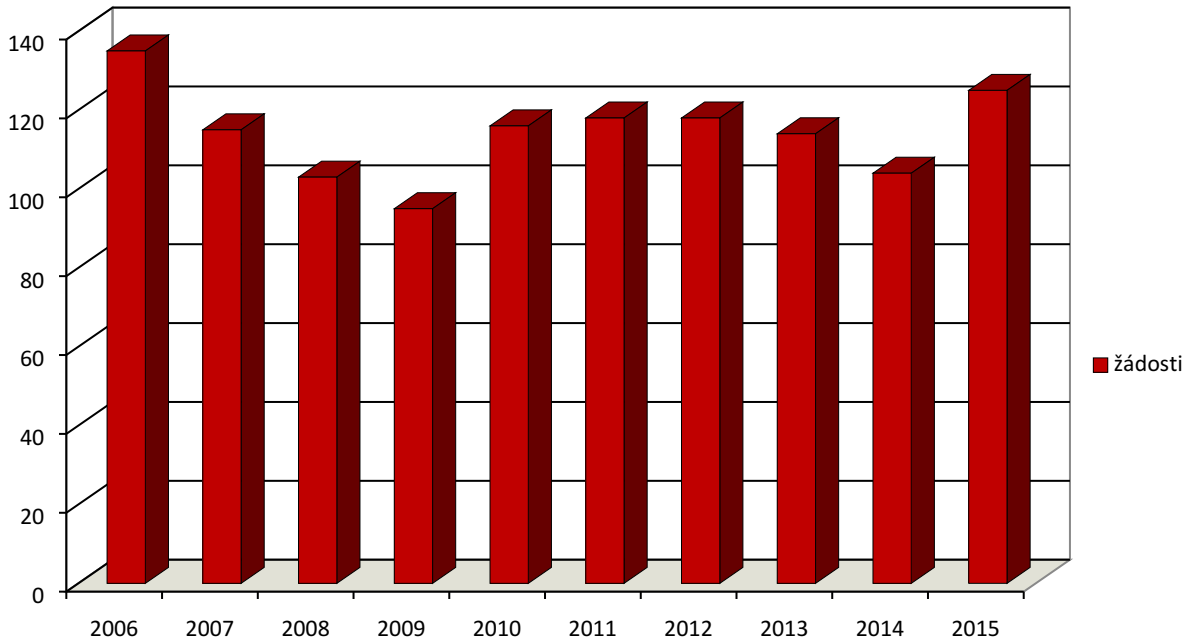
Bylo vydáno celkem 120 certifikátů informačních systémů, z toho 45 pro žadatele ze státní správy nebo samosprávy a 75 ze soukromé sféry. Celkem 69 certifikátů bylo vydáno na žádost podanou v roce 2015. Z celkového počtu certifikátů vydaných v roce 2015 se jednalo pouze v 27 případech o první certifikaci informačního systému, z toho 9 certifikátů bylo vydáno pro informační systémy státní správy.

V 17 případech provozovatel informačního systému s certifikátem platným do data spadajícího do roku 2015 nepožádal o opakovanou certifikaci a platnost certifikátu automaticky skončila.

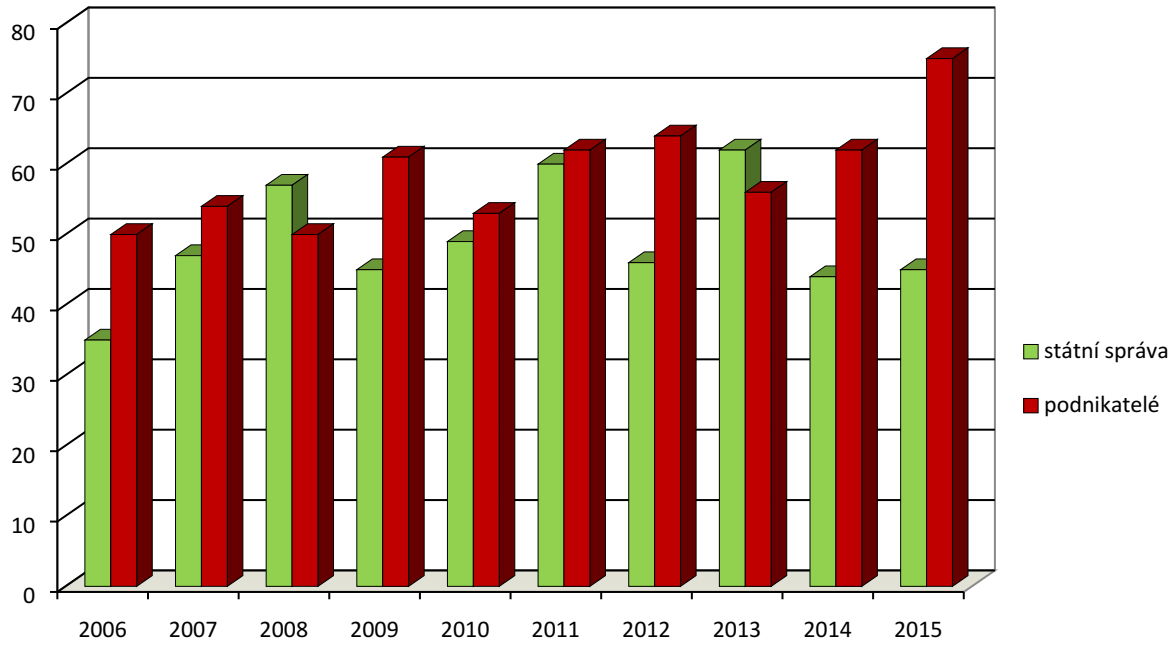
**Certifikace informačních systémů v roce 2015**

| Přijaté žádosti | Vydané certifikáty podle stupně utajení | | | | Vydané certifikáty | |
|---|---|---|---|---|---|---|
| | Vyhrazené | Důvěrné | Tajné | Přísně tajné | státní správa | podnikatelé |
| 124 | 19 % | 51 % | 26,4 % | 3,6 % | 45 | 75 |

**Přijaté žádosti o certifikaci informačního systému v letech 2006 až 2015**



**Vydané certifikáty informačních systémů v letech 2006 až 2015**




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

Lze konstatovat, že ačkoliv v roce 2015 přibylo pouze 9 žádostí o certifikaci nově budovaného informačního systému ze státní správy a 17 žádostí od podnikatelů, je většina informačních systémů pro zpracování utajovaných informací provozována po více než jedno období platnosti certifikátu informačního systému. Před uplynutím doby platnosti certifikátu, která je pro informační systémy nakládající s utajovanou informací stupně utajení Tajné a Přísně tajné nejvýše 2 roky, stupně utajení Důvěrné nejvýše 3 roky a stupně utajení Vyhrazené nejvýše 5 let, pak musí být certifikace pro další období opakována.

V rámci opakovaných certifikací již provozovaných informačních systémů jsou řešeny bezpečnostní problémy spjaté ze změnami použitých informačních technologií, rozšiřováním informačních systémů a s nasazováním prostředků kryptografické ochrany. Zejména ve státní správě technologická úroveň informačních systémů pro nakládání s utajovanými informacemi trvale roste, a to spolu s úrovní jejich zabezpečení. Výkyvy v počtu provedených certifikací souvisejí také s cykly, v nichž se provádí opakovaná certifikace.

V roce 2015, kromě certifikace menších informačních systémů v několika ministerstvech a úřadech (Ministerstvo průmyslu a obchodu, Ministerstvo zdravotnictví, Ministerstvo zemědělství, Ministerstvo pro místní rozvoj, Úřad vlády ČR, Nejvyšší kontrolní úřad, několik krajských a městských úřadů) a v České národní bance, proběhla opakovaná nebo nová certifikace významných a rozsáhlých informačních systémů Ministerstva vnitra a Policie ČR, Ministerstva obrany, Ministerstva zahraničních věcí, Úřadu pro zahraniční styky a informace a Vojenského zpravodajství.

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

V roce 2015 Úřad provedl pro rezort Ministerstva obrany národní akreditaci lokalit důležitých součinnostních systémů NATO a pro Ministerstvo zahraničních věcí a Ministerstvo vnitra národní akreditaci lokalit součinnostních systémů EU. Zároveň byla příslušným orgánům NATO nebo EU pro bezpečnostní akreditaci vydána požadovaná prohlášení o shodě s bezpečnostními požadavky kladenými na tyto součinnostní systémy, na jejichž základě mohou být národní lokality jejich účastníkem. Stálou pozornost vyžaduje i hodnocení a schvalování změn prováděných v uvedených systémech a jejich rozšiřování.

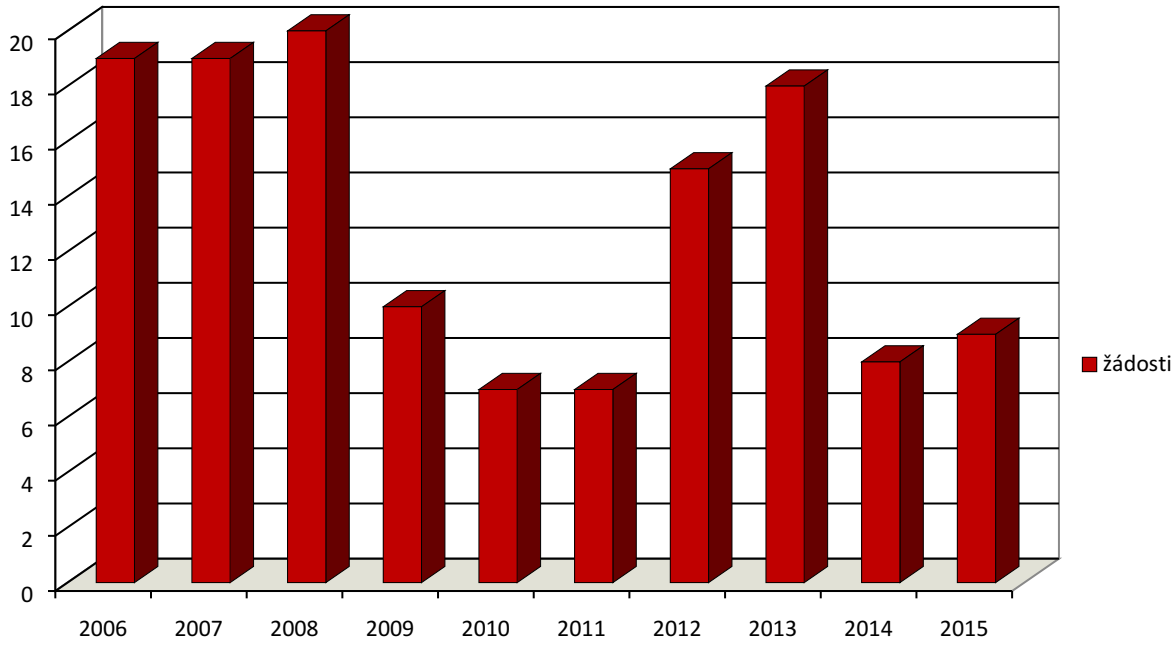
*2.6.1.2. Certifikace kryptografických prostředků*

V roce 2015 bylo Úřadu podáno celkem 9 žádostí o certifikaci kryptografického prostředku, z toho 1 na nový kryptografický prostředek. V řízeních k certifikaci kryptografického prostředku byl vydán 1 certifikát, žádné řízení nebylo ukončeno bez vydání certifikátu. Stav řízení je shrnut v následující tabulce.

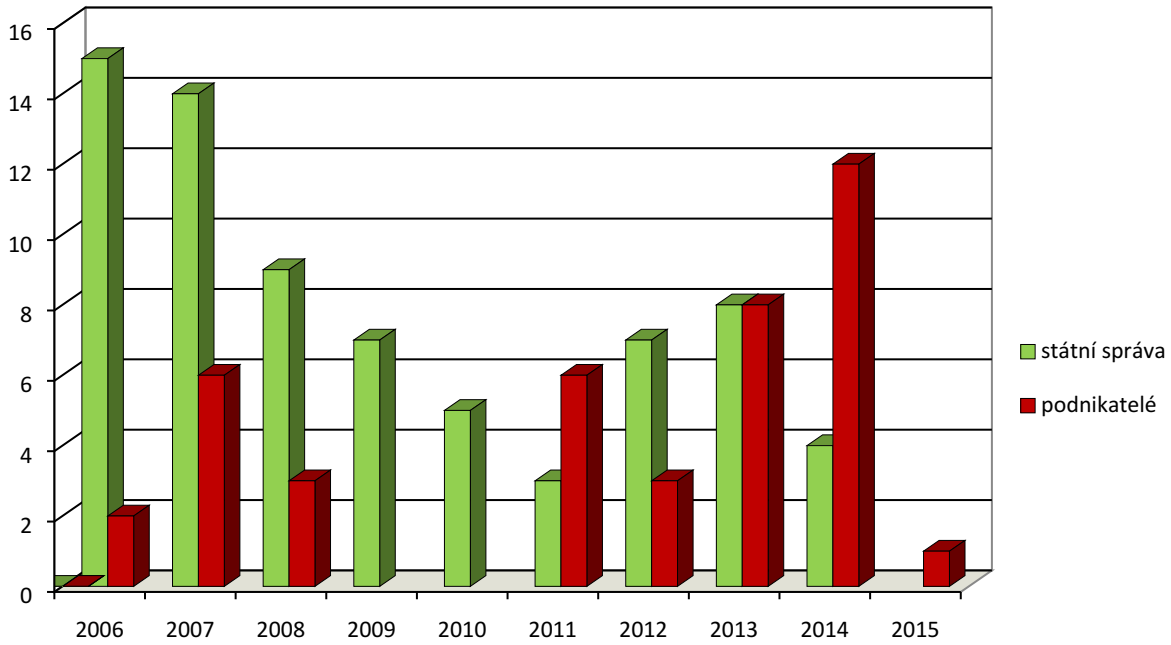
**Certifikace kryptografických prostředků v roce 2015**

| Přijaté žádosti vč. opak. | Probíhající řízení | | Ukonč. bez vydání certifikátu | | Vydané certifikáty | | Pro NATO a EU | |
|---|---|---|---|---|---|---|---|---|
| | státní správa | podnikatelé | státní správa | podnikatelé | st. správa | podnikatelé | NATO | EU |
| 9 | 4 | 5 | 0 | 0 | 0 | 1 | 1 | 1 |

**Přijaté žádosti o certifikaci kryptografického prostředku v letech 2006 až 2015**



**Vydané certifikáty kryptografických prostředků v letech 2006 až 2015**




Nově byl certifikován jen kryptografický prostředek PCA. Žádosti o certifikaci kryptografických prostředků tříd LANPCS a PCS1 v aktualizovaných verzích byly řešeny formou aktualizace příslušných certifikačních zpráv kryptografického prostředku.

Významný podíl pracovní kapacity pracoviště certifikace kryptografických prostředků byl zaměřen na doplňování a hodnocení podkladů k certifikaci kryptografických prostředků, u kterých probíhá certifikační řízení, na aktualizaci pravidel pro používání kryptografických prostředků a příslušného klíčového materiálu a úpravu podmínek pro zajištění výroby a servisu kryptografického prostředku PCA a prostředků tříd PCS1 a LANPCS. Nezanedbatelné byly také činnosti související se zástavbami kryptografických prostředků do mobilních a rozmístitelných systémů a příprava podkladů pro „duální“ hodnocení kryptografického prostředku LANPCSe-AES jako prostředku schváleného EU.

V souladu s požadavky bezpečnostního standardu NBÚ-1/2014 upravujícího podmínky, způsob a postupy vyřazování a ničení kryptografického prostředku a materiálu k zajištění jeho funkce vydal Úřad doplňující podmínky pro ničení kryptografických prostředků třídy KTA. Současně byly zahájeny práce na vytvoření expozice historie kryptografických prostředků používaných v ČR v prostorách Úřadu.

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

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

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

Do seznamu Úřadu materiálu „kontrolovaná kryptografická položka“ byly zařazeny kryptografické prostředky TCE 121 a PCA.

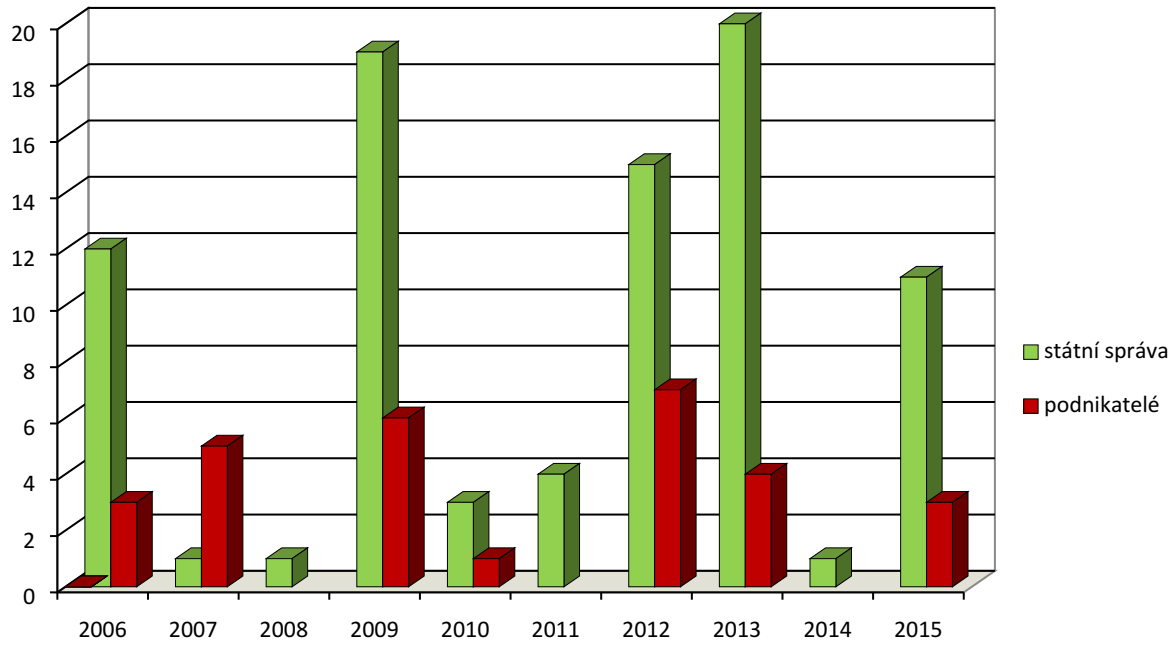
*2.6.1.3. Certifikace kryptografických pracovišť*

V roce 2015 bylo podáno celkem 14 žádostí o certifikaci kryptografického pracoviště. Většina žádostí o certifikaci spadá do kategorie opakovaných žádostí. Byla podána 1 žádost o certifikaci nového kryptografického pracoviště, která je ve stádiu posuzování. Z provedené certifikace vyplynulo, že umístění kryptografických pracovišť a provoz na nich je v souladu s reálnými potřebami příslušných organizací. V tomto rámci ovšem dochází k rozšiřování pracovišť o další kryptografické prostředky a ke změnám jejich umístění. Všechny změny musí být předem posouzeny a schváleny Úřadem. Stav řízení je shrnut v následující tabulce:

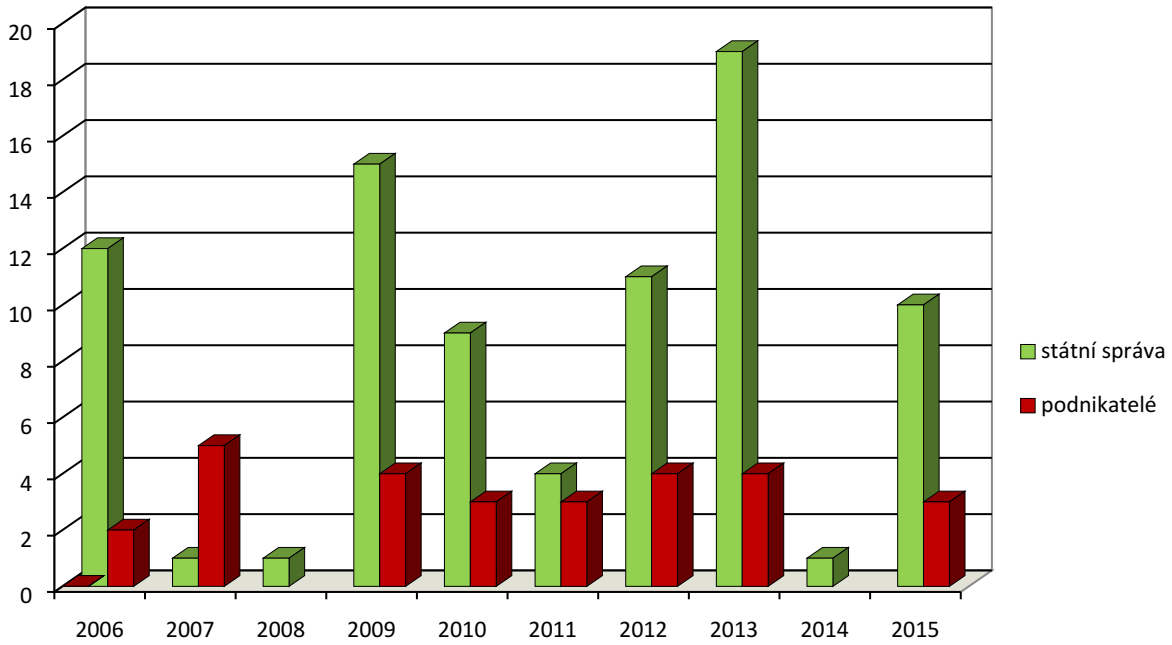
**Certifikace kryptografických pracovišť v roce 2015**

| | Přijaté žádosti | Rozpracováno | Certifikováno | Zamítnuto |
|---|---|---|---|---|
| **Státní správa** | 11 | 1 | 10 | 0 |
| **Podnikatelé** | 3 | 0 | 3 | 0 |
| **Celkem** | **14** | **1** | **13** | **0** |

**Přijaté žádosti o certifikaci kryptografického pracoviště v letech 2006 až 2015**



**Vydané certifikáty kryptografických pracovišť v letech 2006 až 2015**




*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 25 certifikátů stínicích komor, přičemž bylo využíváno i podkladů z měření provedených pracovníky Ministerstva zahraničních věcí a společnosti Techniserv, spol. s r.o., na základě smlouvy o zajištění činnosti.

## 2.6.2. Další odborná činnost

*2.6.2.1. Výroba kryptografického materiálu*

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

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

V roce 2015 bylo v Úřadu vygenerováno celkem 120 268 kryptografických klíčů a hesel uložených na 4 910 nosičích různých typů a dalších 7 771 ks jiného kryptografického materiálu (procesory, paměti, kryptografická dokumentace, instalační a šifrovací SW).

Úřad vzal do evidence a provedl distribuci celkem 1 950 ks nového kryptografického a CCI materiálu a dále zajistil servis a opravy na území ČR u 65 ks kryptografických prostředků a mimo ČR u 13 ks kryptografických prostředků.

V průběhu roku 2015 byla zahájena nová výroba klíčového materiálu pro kryptografický prostředek PCS1.

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 2015 TEMPEST měření podle standardů NATO řady SDIP, EU řady IASG 7 a podle metodiky MIL-STD 461. Objektem měření byla především zařízení orgánů státu. Jednalo se jak o měření komerčních zařízení, většinou pro účely výběrových řízení, tak speciálních informačních systémů.

Celkem bylo v roce 2015 hodnoceno více než 40 typů zařízení. Z toho bylo prováděno TEMPEST měření více než 5 ks zařízení EUROTEMPEST a Siltec, a to jako samostatného zařízení nebo v kombinaci s kryptografickým prostředkem KRYDEC. Dále bylo provedeno měření inovovaných systémů s kryptografickým prostředkem TCE 621 a PCA. Tato měření byla prováděna podle metodiky standardu SDIP-27/1. Většina zařízení splňovala požadavky tohoto standardu.

Další TEMPEST měření byla prováděna v rámci certifikace nebo akreditace informačních systémů pro zpracování utajovaných informací stupně utajení Důvěrné nebo Tajné, buď pro orgány státu (Úřad vlády ČR, 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 a Ministerstva vnitra. 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 2015 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 2015, je uveden v následující tabulce.

**Měřená zařízení a objekty v roce 2015**

| Typ měření[10)] | Počet |
|---|---|
| **Zónové měření** | 24 objektů |
| **Kryptografické prostředky** | 2 typy |
| **PC sestavy** | 8 sestav – třída 0; přes 40 typů – třída 1 a 2 |
| **Audiotechnika** | 2 typy zařízení |
| **Obranné prohlídky i v rámci certifikace IS** | 14 objektů |
| **Mobilní systémy** | 2 systémy |
| **Instalační záznamy** | 10 systémů |

*2.6.2.3. Schvalování projektů bezpečnosti komunikačních systémů*

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

V roce 2015 byla přijata pouze 1 žádost o schválení projektu bezpečnosti nového komunikačního systému, a to z Ministerstva obrany.

Nadále byl provozován komunikační systém v Bezpečnostní informační službě, mezirezortní komunikační systém MODUS a komunikační systém Panthon.

Správu komunikačního systému MODUS využívajícího certifikovaných kryptografických prostředků SECTRA Tiger XS (přídavný kryptografický modul k mobilnímu telefonu), umožňujících mobilní telefonii pro utajované informace do stupně utajení Tajné, v roce 2015 nadále zajišťoval Úřad.

Komunikační systém Panthon pro mobilní komunikaci informací stupně utajení Vyhrazené, který využívá certifikovaného kryptografického prostředku Panthon 3, je rovněž provozován z centra umístěného v Úřadu.

Hlasovou komunikaci utajovaných informací na mezirezortní úrovni poskytují rovněž 2 informační systémy, tzv. vládního utajeného spojení, provozované Ministerstvem vnitra, kterými jsou informační systém Vega-T (pro nakládání s utajovanými informacemi do stupně utajení Tajné) a informační systémem Vega-D (pro nakládání s utajovanými informacemi do stupně utajení Důvěrné). Oba informační systémy jsou certifikovány Úřadem podle zákona a jejich rozvoj a rozšiřování je pod dohledem Úřadu.

*2.6.2.4. Školení pracovníků kryptografické ochrany a zkoušky odborné způsobilosti*

Úřad v roce 2015 organizačně zajistil a provedl, v souladu se zákonem, celkem 20 školení skupin pracovníků kryptografické ochrany a po následující zkoušce odborné způsobilosti vydal 118 osvědčení o zvláštní odborné způsobilosti pracovníka kryptografické ochrany. Dále provedl zaškolení

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

pracovníků provozní obsluhy kryptografického prostředku a vydal 2 potvrzení o odborném zaškolení pracovníka provozní obsluhy kryptografického prostředku. Kromě toho probíhají další školení a zkoušky odborné způsobilosti na Ministerstvu vnitra, Ministerstvu obrany a Ministerstvu zahraničních věcí na základě smluv uzavřených mezi Úřadem a uvedenými ministerstvy. Úřad v roce 2015 schvaloval aktualizaci osnov a obsahu některých kurzů.

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

Zabezpečování zákonem stanovených činností Úřadu v oblasti kryptografické ochrany a bezpečnosti informačních systémů nakládajících s utajovanými informacemi probíhalo v roce 2015 bez větších problémů.

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

- Stálou výzvou je rychlý rozvoj informačních a komunikačních technologií (ICT) a s ním spjaté bezpečnostní problémy. Některé nové technologie nelze nasadit bez jejich důkladného testování anebo bez podkladů vzniklých jejich kvalifikovaným hodnocením z hlediska bezpečnosti podle uznávaných mezinárodních kritérií. Zároveň mají subjekty vedoucí útoky proti důvěrnosti, integritě a dostupnosti utajovaných nebo citlivých informací k dispozici stále sofistikovanější nástroje. Informace o skrytých zranitelnostech ICT produktů jsou obtížně dosažitelné a jejich objevení zpravidla vyžaduje vysoce nadstandardní technické vybavení.

- V oblasti kryptografické ochrany jsou v rámci ČR zajišťovány národní kryptografické prostředky certifikované pro ochranu utajované informace v různých komunikačních prostředích. Tato komunikační prostředí se však neustále mění (u mobilních komunikací zcela překotně). Vývoj národních kryptografických prostředků probíhá v podmínkách odborných pracovišť Úřadu a ve spolupráci se specializovanými subjekty ze soukromého sektoru v rámci externích vývojových projektů. Vzhledem k požadavkům průmyslové bezpečnosti, vysoké odborné náročnosti a nedostatečnému portfoliu privátních odborných pracovišť v ČR se projevuje jistý nedostatek zájmu kvalifikovaného soukromého sektoru účastnit se externího vývoje, ačkoliv je externí vývoj do značné míry financován z rozpočtu Úřadu (tedy státu). Zájem privátních subjektů také negativně ovlivňuje malý národní trh kryptografických prostředků (počty kusů kryptografických prostředků uplatnitelných v ČR).

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

## 2.7. ADMINISTRATIVNÍ A FYZICKÁ BEZPEČNOST, ÚSTŘEDNÍ REGISTR

### 2.7.1. Administrativní bezpečnost

Pracoviště koncepce administrativní bezpečnosti se podílelo na přípravě a průběhu vypořádání připomínek k návrhu novely vyhlášky č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací, ve znění pozdějších předpisů. Po jejím vydání realizovalo program osvěty a metodického výkladu k přijatým změnám. Další činnost pracoviště spočívá v pokračování popisu procesů, řešících manipulaci a archivaci utajovaných dokumentů v elektronické formě.

### 2.7.2. Fyzická bezpečnost

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

- činnosti spojené s členstvím v certifikační radě certifikačního orgánu Trezor Test s.r.o. (účast na výrobních auditech u 11 firem v rámci ČR, účast na certifikačních radách a účast při provádění zkoušek na mechanických zábranných systémech podle příslušných norem),

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

- metodickou pomoc v souvislosti s instalací technických prostředků a s návrhy opatření fyzické bezpečnosti na vyžádání u podnikatelů nebo orgánů státu (např. RETIA, a.s., Kancelář prezidenta republiky – objekt Lány, O2 Czech Republic a.s., Generální finanční ředitelství, Generální ředitelství Vězeňské služby ČR, Státní pokladna Centrum sdílených služeb s.p., Ministerstvo financí, Úřad pro civilní letectví aj.),

- účast na provedení bezpečnostní inspekce NATO v ČR, týkající se ochrany utajovaných informací NATO ve vybraných registrech utajovaných informací stupně utajení Přísně tajné a Tajné a registrech ATOMAL,

- školení v oblasti fyzické bezpečnosti složek Ministerstva obrany a pracovníků ATOMAL registrů.

#### *2.7.2.1. Certifikace technických prostředků*

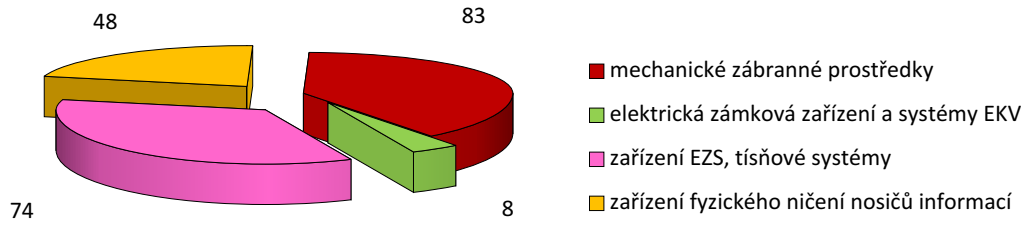
Nezbytnou zákonnou podmínkou pro používání technických prostředků k ochraně utajovaných informací je mj. i jejich certifikace. Úřad v roce 2015 přijal celkem 96 žádostí o certifikaci pro 215 technických prostředků. V rámci posuzovaní a vyhodnocování podkladů pro certifikaci bylo u 6 % žádostí vyžádáno jejich doplnění a upřesnění. Ve 2 případech byl certifikační proces ukončen bez vydání certifikátu, neboť nebyly poskytnuty dostatečné podklady pro vydání certifikátu.

Úřad vydal celkem 213 certifikátů technických prostředků. Počty vydaných certifikátů technických prostředků podle jednotlivých skupin definovaných zákonem jsou uvedeny v následující tabulce.

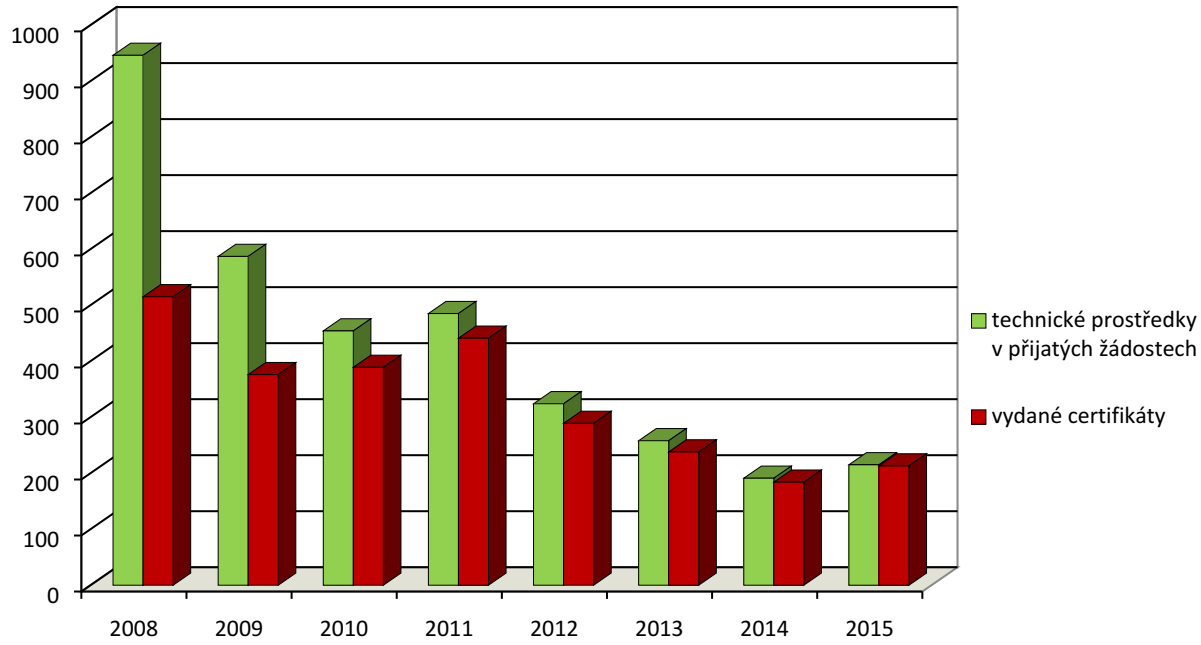
**Vydané certifikáty technických prostředků v roce 2015**

| | |
|---|---|
| **Mechanické zábranné prostředky**[11)] | 83 |
| **Elektrická zámková zařízení, systémy pro kontrolu vstupu**[12)] | 8 |
| **Zařízení elektrické zabezpečovací signalizace a tísňové systémy**[13)] | 74 |
| **Zařízení fyzického ničení nosičů informací**[14)] | 48 |
| **Celkem** | **213** |

**Certifikáty technických prostředků v roce 2015**



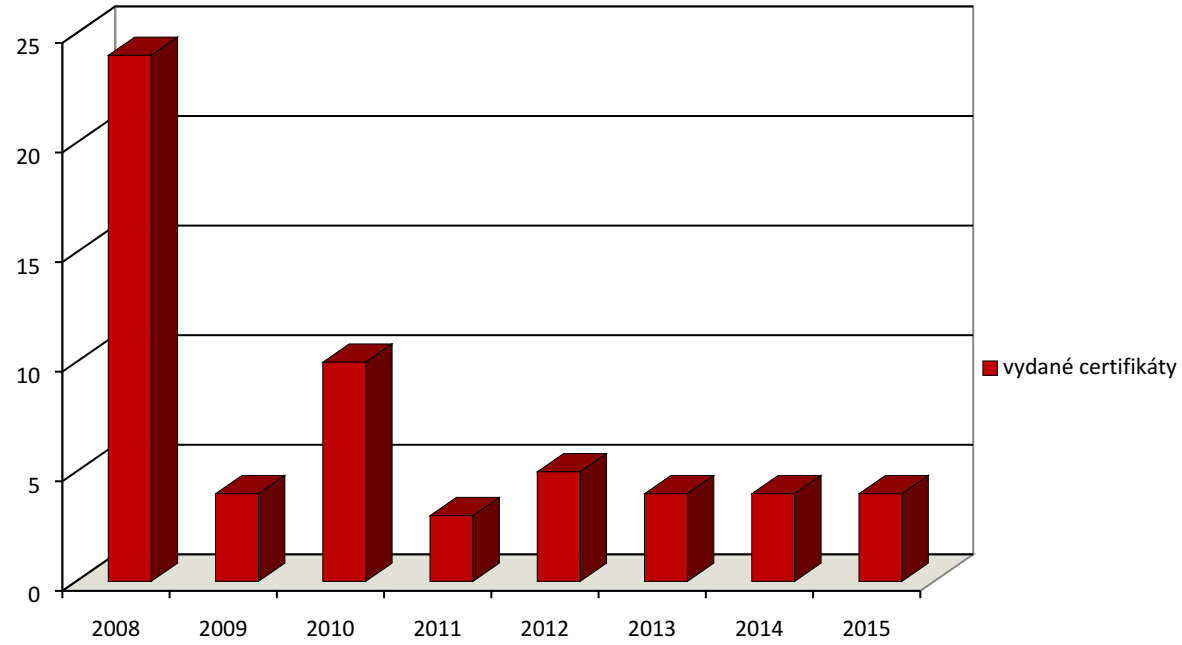

**Certifikace technických prostředků v letech 2008 až 2015**




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

Kromě certifikátů uvedených v předchozí tabulce a grafech byly v roce 2015, na základě podaných žádostí, vydány 4 certifikáty pro jednotlivé technické prostředky – uživatelské certifikáty. Jednalo se o 3 kusy trezorů a drtící a separační linku. 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 zobrazuje následující graf.

**Uživatelské certifikáty technických prostředků v letech 2008 až 2015**




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, které jsou zapracovávány do certifikačního postupu. Průběžně probíhá aktualizace certifikovaných technických prostředků na internetových stránkách Úřadu. Dále byla realizována metodická pomoc v problematice certifikace technických prostředků (např. ENVIROPOL s.r.o., XERTEC a.s., Sběrné suroviny UH, s.r.o., aj.).

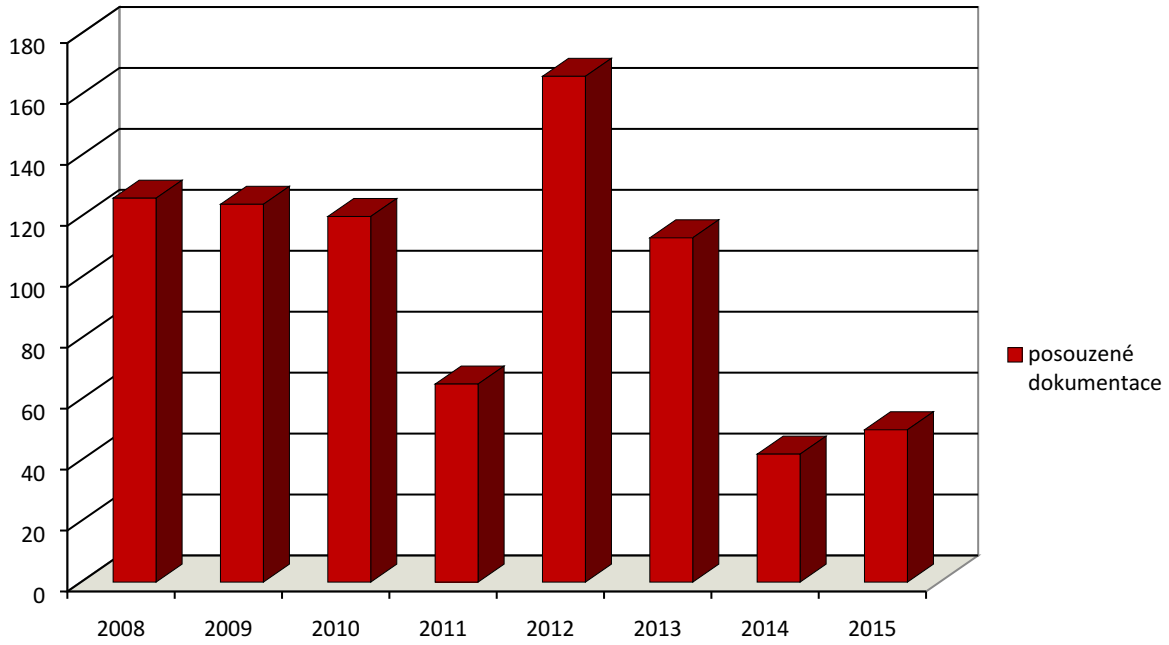
*2.7.2.2. Posuzování bezpečnostní dokumentace podnikatele z hlediska fyzické bezpečnosti*

V rámci vedených bezpečnostních řízení o vydání osvědčení podnikatele nebo při aktualizaci bezpečnostní dokumentace podnikatele, který je držitelem osvědčení podnikatele, bylo v roce 2015 přijato celkem 51 žádostí o stanovisko k bezpečnostní dokumentaci podnikatele z hlediska zajištění ochrany utajovaných informací fyzickou bezpečností. Při posuzování dokumentací byla ve 30 % případů provedena konzultace s podnikatelem v Úřadu nebo přímo v sídle podnikatele. Bylo posouzeno 50 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. Ve 2 případech byla bezpečnostní dokumentace podnikatele vrácena z důvodu zastavení řízení. K 1. lednu 2016 zbývalo posoudit 1 bezpečnostní dokumentaci podnikatele. Přehled přijatých žádostí, členěný podle kategorií zabezpečených oblastí, je uveden v následující tabulce.

**Přijaté žádosti a posouzené bezpečnostní dokumentace podnikatele v roce 2015**

| | Důvěrné | Tajné | Přísně tajné | Celkem |
|---|---|---|---|---|
| **Přijaté žádosti** | 32 | 19 | 0 | **51** |
| **Posouzené dokumentace** | 32 | 18 | 0 | **50** |

**Posouzené bezpečnostní dokumentace podnikatele v letech 2008 až 2015**




*2.7.2.3. Problémové oblasti fyzické bezpečnosti*

Certifikace technických prostředků:

- nedostatečné podkladové materiály k žádosti o certifikaci technického prostředku.

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

- nedostatky ve zpracování projektů fyzické bezpečnosti (nedostatečný popis rozmístění technických prostředků),
- nekompletní popis režimových opatření fyzické bezpečnosti (označování a evidence klíčů, neaktualizované seznamy oprávněných osob),
- nesoulad skutečného stavu se stavem deklarovaným v projektu fyzické bezpečnosti,
- nedostatky při instalaci technických prostředků (nesprávná funkčnost přístupového systému).

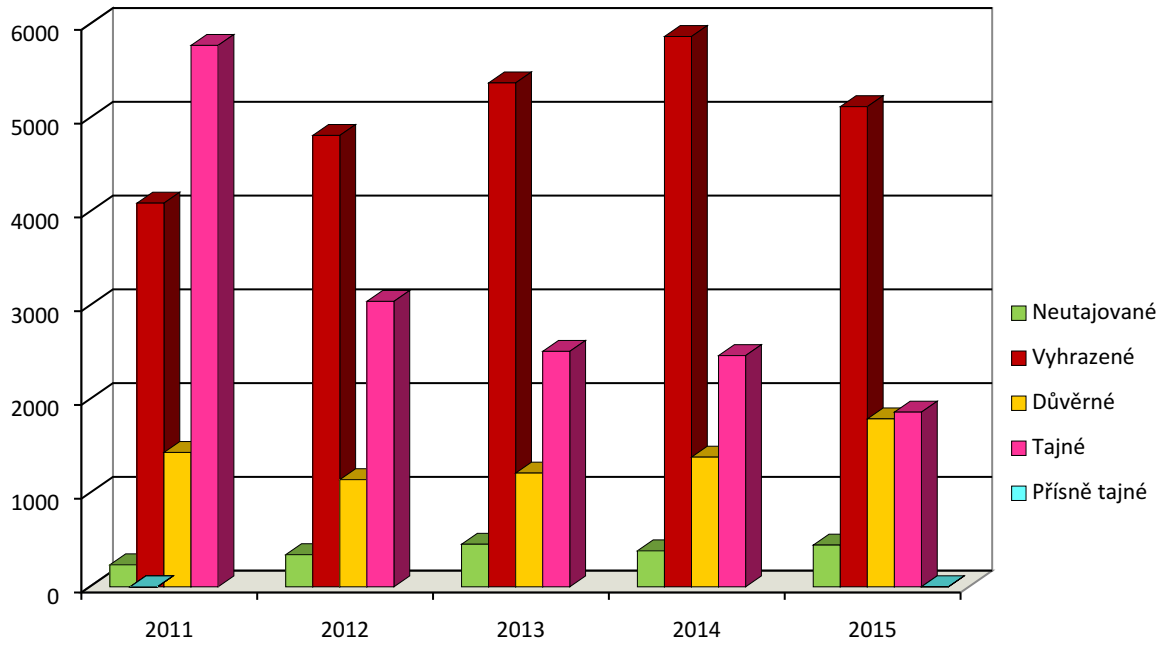
## 2.7.3. Ústřední registr

Prostřednictvím ústředního registru je realizováno poskytování utajovaných informací v rámci mezinárodního styku. V roce 2015 vykonával ústřední registr evidenci, distribuci a ukládání těchto utajovaných informací, a to zejména utajovaných informací NATO. U určených utajovaných dokumentů ústřední registr prováděl jejich distribuci podřízeným registrům utajovaných informací, zřízeným v rámci ústředních orgánů státní správy a právnických osob. Přehled dokumentů NATO evidovaných v ústředním registru za posledních 5 let je uveden v následující tabulce a grafu.

**Dokumenty NATO evidované v ústředním registru**

| NATO | 2011 | 2012 | 2013 | 2014 | 2015 | Celkem |
|---|---|---|---|---|---|---|
| **Neutajované** | 235 | 434 | 454 | 384 | 445 | **1 952** |
| **Vyhrazené** | 4 092 | 4 814 | 5 374 | 5 869 | 5 121 | **25 270** |
| **Důvěrné** | 1 433 | 1 143 | 1 213 | 1 383 | 1 719 | **6 891** |
| **Tajné** | 5 774 | 3 044 | 2 511 | 2 466 | 1 863 | **15 658** |
| **Přísně tajné** | 0 | 0 | 0 | 0 | 1 | **1** |
| **Celkem** | **11 534** | **9 435** | **9 552** | **10 102** | **9 149** | **49 772** |

**Dokumenty NATO evidované v ústředním registru**




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

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

V rámci kontrolní činnosti ústředního registru, podle § 79 odst. 7 zákona, bylo v loňském roce provedeno 10 kontrol podřízených registrů utajovaných informací. Zároveň se pracovníci ústředního registru účastnili kontrol v rámci výkonu státního dozoru u orgánů státu a podnikatelů, u nichž byly zřízeny registry utajovaných informací. Zjištěné nedostatky se týkaly zejména způsobu předávání utajovaných dokumentů, autentizace administrativních pomůcek, tvorby čísla jednacího a vedení seznamů zaměstnanců, kterým lze umožnit přístup k utajovaným informacím cizí moci.

V rámci metodického řízení bylo v roce 2015 provedeno školení vedoucích podřízených ATOMAL registrů a jejich zástupců, které bylo zaměřeno na bezpečnost utajovaných informací ATOMAL a prezentaci zkušeností získaných při cvičení ATOMAL. Rovněž bylo provedeno školení z oblasti ochrany utajovaných informací cizí moci a administrativní bezpečnosti pro zaměstnance rezortu Ministerstva obrany.

Ústřední registr ověřoval splnění podmínek nezbytných pro zřízení registru utajovaných informací u 3 subjektů, které podaly žádost o souhlas ke zřízení registru utajovaných informací cizí moci. V rámci Úřadu byl zřízen další pomocný registr, a to pro Sekci kybernetické bezpečnosti. V seznamu všech registrů zřízených na území ČR bylo ke konci roku 2015 evidováno celkem 47 registrů utajovaných informací (bez pomocných registrů).

Úřad vede přehled všech registrů na území ČR, a to včetně jmen, příjmení a podpisových vzorů jejich vedoucích a jejich zástupců. Rovněž byly průběžně aktualizovány seznamy zaměstnanců Úřadu, kterým lze umožnit přístup k utajovaným informacím NATO, EU a k ostatním utajovaným informacím poskytovaným v mezinárodním styku.

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

**Skartace utajovaných dokumentů cizí moci v roce 2015**

| Stupeň utajení | Počet čísel jednacích |
|---|---|
| **Neutajované** | 203 |
| **Vyhrazené** | 10 380 |
| **Důvěrné** | 2 250 |
| **Tajné** | 3 495 |
| **Celkem** | **16 328** |

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

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.

Na základě rozhodnutí Bezpečnostního úřadu NATO o provedení bezpečnostní inspekce NATO v ČR týkající se ochrany utajovaných informací NATO, kdy tuto kontrolní pravomoc poprvé v roce 2015 delegoval na národní bezpečnostní úřad členské země NATO, provedl Úřad bezpečnostní

inspekci NATO. Pracovníci ústředního registru Úřadu provedli v souladu s požadavkem Bezpečnostního úřadu NATO inspekci ve vybraných registrech utajovaných informací stupně utajení Přísně tajné a Tajné a registrech ATOMAL. V období od 22. ledna do 12. března 2015 bylo zkontrolováno celkem 8 registrů Přísně tajných a Tajných a 4 registry ATOMAL. Při inspekci bylo zjištěno, že všechny kontrolované subjekty splňují podmínky ochrany utajovaných informací v souladu s bezpečnostní politikou NATO. Zjištěné skutečnosti, dle jednotlivých druhů zajištění ochrany utajovaných informací, včetně návrhů opatření a doporučení, byly uvedeny do hlášení o výsledku inspekce, které bylo ústředním registrem Úřadu předáno Bezpečnostnímu úřadu NATO dne 24. března 2015. Dle vyjádření ředitele Bezpečnostního úřadu NATO byla bezpečnostní inspekce NATO provedena odpovědně, profesionálně a velmi důsledně.

## 2.8. KYBERNETICKÁ BEZPEČNOST

Rok 2015 znamenal další rozvíjení a prohlubování schopností ČR v oblasti kybernetické bezpečnosti. S Novým rokem nabyl účinnosti zákon o kybernetické bezpečnosti a prováděcí předpisy, které rámují činnost Úřadu jako gestora kybernetické bezpečnosti a mj. stanovují bezpečnostní standardy pro důležité sítě a informační systémy s celostátním významem.

V únoru 2015 byla schválena Národní strategie kybernetické bezpečnosti na období let 2015 – 2020. O 3 měsíce později na ni navázal Akční plán, který jednotlivým dotčeným subjektům ukládá konkrétní úkoly a termíny jejich plnění.

### 2.8.1. Budování NCKB/GovCERT.CZ

Úřad navázal na slavnostní otevření Národního centra kybernetické bezpečnosti (dále jen „NCKB“) z předchozího roku a i v roce 2015 pokračoval v budování vlastních kapacit a v technické i teoretické podpoře svých partnerů.

NCKB se skládá ze 2 oddělení. Prvním je vládní bezpečnostní tým GovCERT.CZ, jehož IT odborníci poskytují pomoc s technickým řešením kybernetických bezpečnostních incidentů, provádí penetrační testy, analýzu malware a zajišťují sdílení informací o incidentech a budoucích trendech v této oblasti s IT komunitou i veřejností. Druhým je Oddělení teoretické podpory, vzdělávání a výzkumu, které se soustředí na netechnické aspekty kybernetické bezpečnosti, zejména na tvorbu a implementaci kybernetické bezpečnostní politiky ČR, určování kritické informační infrastruktury (dále jen „KII“) a významných informačních systémů (dále jen „VIS“) podle zákona o kybernetické bezpečnosti a prováděcích předpisů, mezinárodní spolupráci, osvětu a vzdělávání, publikační činnost a další aktivity.

Nový právní rámec a koncepční dokumenty, jakož i ad hoc zadání znamenaly pro NCKB nárůst agendy. V roce 2015 proto Úřad pokračoval v rozšiřování jeho personálních i technických kapacit. Ke konci roku 2015 naplnilo NCKB počet přidělených pracovních míst, zejména specialisty na informační technologie, krizové řízení, právo či mezinárodní vztahy a bezpečnost. Usnesením č. 520 ze dne 1. července 2015 vláda ČR rozhodla o personálním a finančním posílení Úřadu v průběhu let 2016 až 2018, které reflektuje potřeby vyplývající ze zákona o kybernetické bezpečnosti a strategických dokumentů, jakož i rostoucí objem a kvalitu práce při řešení kybernetických bezpečnostních incidentů.

Z povahy pracoviště CERT a jeho úkolů vyplývá nezbytnost vysoké odbornosti jeho pracovníků a jejího neustálého prohlubování, aby mohli být rovnocennými partnery svým zahraničním kolegům

při spolupráci a řešení stále nových kybernetických hrozeb a útoků a důstojnými protivníky těch, kdo za těmito hrozbami a útoky stojí. Součástí je vzdělávání formou specializovaných školení, stáží a kurzů. Úřad proto na základě veřejné zakázky v květnu 2015 uzavřel smlouvu se společností SANS, Institute jedním ze světově nejuznávanějších poskytovatelů technické expertízy v oblasti kybernetické bezpečnosti. V letech 2015 až 2017 členové vládního CERT podle svého zaměření získají certifikaci v incident handlingu, forenzní analýze a vyšetřování, reverzním inženýrství a analýze malware, Windows security, UNIX security, virtualizaci a cloudové bezpečnosti, penetračním testování nebo ICS/SCADA bezpečnosti. Do konce roku 2015 školení SANS absolvovalo 11 zaměstnanců Úřadu a 1 zaměstnanec Úřadu stihl zakončit školení certifikátem.

### 2.8.2. Vývoj legislativy a koncepčních dokumentů

Nová Národní strategie kybernetické bezpečnosti na období let 2015 – 2020, schválená vládou ČR dne 16. února 2015, navázala na předchozí strategii pro období 2012 až 2015, jejíž hlavní úkoly byly úspěšně splněny či průběžně realizovány. ČR se tím posouvá od budování základních kapacit k pokročilejšímu a hlubšímu zajišťování kybernetické bezpečnosti. Strategie představuje ucelený soubor opatření, který definuje vizi ČR v oblasti kybernetické bezpečnosti a pojmenovává sledovaný cílový stav. Formuluje rovněž základní principy, které bude ČR při zajišťování kybernetické bezpečnosti následovat a dodržovat.

Na únorové přijetí Strategie navázal Akční plán, který vláda ČR přijala dne 25. května 2015. Akční plán vychází z hlavních cílů Strategie a na příštích 5 let definuje konkrétní úkoly k jejímu naplnění. U každého ze 141 úkolů je uveden subjekt, který za splnění odpovídá, a termín, do kdy se tak má stát. Na implementaci Akčního plánu a Strategie spolupracují s Úřadem zejména rezorty Ministerstva vnitra, Ministerstva obrany, Ministerstva zahraničních věcí, Ministerstva průmyslu a obchodu a Ministerstva financí. Nezastupitelnou úlohu hrají zpravodajské služby, na osvětové činnosti budou mít důležitý podíl Ministerstvo školství, mládeže a tělovýchovy a Ministerstvo práce a sociálních věcí. Ve vybraných úkolech se dále zapojí například Technologická agentura České republiky nebo Český telekomunikační úřad.

Nový právní rámec kybernetické bezpečnosti v ČR tvoří zejména zákon o kybernetické bezpečnosti, vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti, vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, a nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, ve znění nařízení vlády č. 315/2014 Sb.

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

S nabytím účinnosti zákona o kybernetické bezpečnosti a prováděcích předpisů Úřad zahájil proces určování prvků KII, jejichž správcům, stejně jako správcům VIS vznikly zákonné povinnosti ve vztahu k bezpečnostním opatřením a specifické povinnosti vůči Úřadu.

K 31. prosinci 2015 bylo formou opatření obecné povahy nebo usnesením vlády ČR určeno 76 prvků KII. Průběžně byly jednotlivými správci, kteří jsou orgánem veřejné moci, nahlašovány informační systémy, které naplňují kritéria pro VIS.

Proces určování KII probíhá prozatím ve třech vlnách. V první vlně se Úřad zaměřil na informační nebo komunikační systémy ve správě organizačních složek státu – ústředních orgánů státní správy. Určování v této vlně bylo spuštěno neprodleně po nabytí účinnosti zákona o kybernetické bezpečnosti a bylo završeno dne 15. února 2015, kdy Úřad k zařazení do KII navrhl 45

informačních a komunikačních systémů. Usnesením vlády ČR č. 390 ze dne 25. května 2015 byl tento seznam schválen.

Ve druhé vlně se Úřad zaměřil na zbývající organizační složky státu a dne 15. září 2015 předložil podle krizového zákona Ministerstvu vnitra další návrh KII k určení. Usnesením vlády ČR č. 981 ze dne 2. prosince 2015 byl navržený seznam prvků schválen. Tato skupina nicméně může být ještě rozšířena, nepředpokládá se však takové množství prvků KII jako ve vlně první.

Ve třetí vlně jsou identifikovány prvky KII, jejichž správcem nejsou organizační složky státu. Jedná se o strategické informační a komunikační systémy jak ve správě soukromých společností, tak ve správě státních podniků a obdobných subjektů. Tato fáze není doposud ukončena. Zatímco určení KII u organizačních složek státu je prováděno usnesením vlády ČR na návrh Úřadu, u ostatních subjektů se tak stane opatřením obecné povahy vydaným Úřadem. Ke dni 31. prosince 2015 bylo opatřením obecné povahy určeno 28 prvků KII.

Proces určování KII je vzhledem k dynamickému prostředí informačních a komunikačních technologií kontinuální činností. Úřad nepředpokládá výrazný nárůst počtu prvků KII u organizačních složek státu. Naproti tomu u ostatních subjektů je nárůst očekáván a podle odhadů budou mít tyto subjekty ve správě více než polovinu všech určených prvků KII.

Na rozdíl od KII je za posouzení naplnění kritérií pro VIS odpovědný sám správce systému. Seznam těchto systémů je uveden v příloze vyhlášky č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, která v současnosti uvádí 92 VIS spravovaných celkem 35 subjekty. Podobně jako proces určování KII je však i posuzování VIS kontinuální činností a stav se proto v průběhu roku 2015 měnil; některé systémy byly přeřazeny do KII a mnoho jiných systémů bylo jednotlivými správci nově posouzeno a nahlášeno. Ke dni 31. prosince 2015 Úřad evidoval cca 105 VIS a začal připravovat aktualizaci předmětné přílohy.

Zákon o kybernetické bezpečnosti ukládá správcům KII a správcům VIS množství povinností. Kromě obecných povinností, jako jsou například hlášení kontaktních údajů a hlášení kybernetických bezpečnostních incidentů Úřadu, jde o povinnosti spojené se zavedením mnoha organizačních a technických bezpečnostních opatření podle vyhlášky č. 316/2014 Sb. Správci KII a VIS mají pro naplnění většiny povinností roční přechodnou lhůtu. U KII se tato lhůta počítá od určení, u VIS od posouzení. V průběhu roku 2015 probíhaly přípravy na kontrolu dodržování zákonných povinností, kterou bude od roku 2016 Úřad provádět.

### 2.8.4. Spolupráce Úřadu v oblasti kybernetické bezpečnosti

Stejně jako v předchozích letech, i v roce 2015 pokračoval Úřad v navazování a rozvíjení bilaterální a multilaterální mezinárodní spolupráce. Přehled mezinárodních aktivit v této oblasti je uveden v kapitole 2.2.3.

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

Významnou úlohu hrál tradičně národní tým CSIRT.CZ provozovaný sdružením CZ.NIC, které své postavení stvrdilo ve výběrovém řízení a bude ve výkonu funkce národního CERT nadále pokračovat na základě veřejnoprávní smlouvy s Úřadem uzavřené na základě zákona o kybernetické bezpečnosti, podepsané v prosinci 2015.

Dosavadní technická spolupráce Úřadu s CSIRT.CZ při řešení bezpečnostních incidentů byla v roce 2015 rozšířena o krátkodobé stáže pracovníků GovCERT.CZ. Týmy spolupracovaly i na mezinárodních cvičeních kybernetické bezpečnosti.

Dalším bezpečnostním týmem úzce spolupracujícím s Úřadem je Centrum CIRC v rezortu Ministerstva obrany (C-CIRC MO), jehož zástupci se aktivně zapojují do mezinárodních kybernetických cvičení a podílejí se na výměně informací o bezpečnostních událostech. Z ostatních bezpečnostních týmů je namístě zmínit zejména tým sdružení CESNET (CESNET-CERTS) podílející se na sdílení dat o stanicích zapojených do botnetu získávaných na základě spolupráce se společností Microsoft a v budoucnu snad i sdílení know-how a dat z honeypotů, jež CESNET-CERTS provozuje. Obdobně nelze pominout CERT tým operátora O2 Czech Republic, s nímž Úřad v roce 2015 realizoval finální fázi projektu automatického rozhraní pro hlášení kybernetických bezpečnostních incidentů týkajících se VIS v operátorově síti.

V rámci koordinační úlohy Úřadu při řešení kybernetických bezpečnostních incidentů a s cílem posílit komunikační kanály s ostatními bezpečnostními týmy a dalšími případnými partnery z řad KII a VIS v roce 2015 Úřad rovněž připravoval spuštění elektronické komunikační a kolaborační platformy. Prakticky se jedná o videokonferenční systém, který kromě teleprezenčních a komunikačních služeb může nabídnout možnost online kolaborace zapojených účastníků nad zpracovávaným obsahem. Celá platforma poběží v zabezpečeném režimu a bude pod výlučnou správou a kontrolou Úřadu. Systém pracuje samostatně, nezávisle na službách třetích stran nebo podpůrných technologií typu cloud. Veškerá komunikace mezi účastníky bude probíhat šifrovaně. Dostupnost platformy je zajištěna prostřednictvím internetového připojení, s minimálními nároky na stanice zapojených účastníků. Přístupová práva budou distribuována mezi kooperující subjekty a jednotlivé uživatele prostřednictvím Úřadu. Vysoký potenciál kolaborační platformy lze dále využít v průběhu příprav kybernetických cvičení nebo v neposlední řadě pro pořádání online jednání, školení a jinou vzdělávací činnost.

K zajištění rychlé a operativní vzájemné spolupráce s Ministerstvem obrany Úřad dne 9. května 2015 uzavřel „Prováděcí ujednání o vzájemné podpoře v oblasti kybernetické bezpečnosti a kybernetické obrany“ na základě „Rámcové dohody o vzájemné podpoře vybraných činností mezi MO a NBÚ“.

Mezi důležité partnery Úřadu v kybernetické bezpečnosti patří akademická obec. Spolupráce začala přípravou zákona o kybernetické bezpečnosti, pokračuje při realizaci národních i mezinárodních cvičení kybernetické bezpečnosti a sdílení informací a zkušeností z řešení kybernetických bezpečnostních incidentů a v roce 2015 se rozšířila i do oblasti vzdělávání. Ve spolupráci s Ministerstvem školství, mládeže a tělovýchovy, Ministerstvem práce a sociálních věcí, odborníky z dalších orgánů veřejné správy, neziskových organizací a partnery ze soukromého sektoru byl v roce 2015 vypracován první „Návrh koncepce vzdělávání v oblasti kybernetické bezpečnosti“.

Tradičně intenzivní spolupráce Úřadu probíhala s Masarykovou univerzitou v Brně. Úřad se podílel na projektu Kybernetického polygonu poskytujícího virtuální prostředí pro simulaci kybernetických útoků využitelné pro cvičení kybernetické bezpečnosti, slavnostně otevřeného v dubnu 2015. Spolupráce byla i v roce 2015 posilována krátkodobými stážemi zástupců GovCERT.CZ u CSIRT-MU, kde se seznámili s jejich pracovními postupy a vyměnili si zkušenosti ze zvládání incidentů. Kromě technické spolupráce týmů CSIRT-MU při Fakultě informatiky, ÚVT-MU a GovCERT.CZ se zástupci Úřadu podíleli i na výuce na Fakultě sociálních studií, kde v zimním semestru 2015/2016 zajišťovali výuku ve 4 předmětech bakalářského a magisterského programu o tématech spojených s kybernetickou bezpečností. Právnická fakulta, jmenovitě Ústav práva a technologií, v tomtéž semestru iniciovala neformální diskusní platformu pro pravidelná setkávání právníků zabývajících se kybernetickou bezpečností a souvisejícími obory v akademii, Úřadu, justici

a dalších složkách státní správy, tzv. CyberCake. V roce 2015 Úřad navíc spustil program studentských stáží v NCKB, který do konce roku v rozsahu 1 až 3 měsíce absolvovalo 8 studentů z Fakulty sociálních studií a Pedagogické fakulty Masarykovy univerzity a z Fakulty podnikatelské Vysokého učení technického v Brně.

O kybernetické bezpečnosti zástupci Úřadu v zimním semestru 2015/2016 přednášeli i na Palackého univerzitě v Olomouci. V průběhu roku Úřad uzavřel rámcové smlouvy o spolupráci s Vysokou školou báňskou – Technickou univerzitou Ostrava, Univerzitou Tomáše Bati ve Zlíně, Jihočeskou univerzitou v Českých Budějovicích a Karlovou univerzitou v Praze. Vzdělávání v kybernetické bezpečnosti i společné výzkumné či jiné projekty tedy budou mít v budoucnosti příležitost rozvíjet se i na dalších veřejných vysokých školách.

Mezi další partnery, se kterými v průběhu roku 2015 rozvíjel Úřad spolupráci, patří například peeringové sdružení NIX.CZ, projekt FÉNIX, Asociace krajů a její jednotliví členové jako Kraj Vysočina, AFCEA, nebo nevládní sdružení Národní centrum bezpečnějšího internetu. Prostřednictvím České bankovní asociace spolupracuje Úřad s bankami, které mají zájem na zvyšování ochrany své počítačové infrastruktury.

Ve dnech 16. až 18. června 2015 uspořádal Úřad národní cvičení CYBER CZECH 2015, v uvedeném termínu teoretické cvičení, v říjnu 2015 pak, ve spolupráci s Ústavem výpočetní techniky Masarykovy univerzity, cvičení technické, které se odehrálo ve speciálním prostředí Kybernetického polygonu v Brně.

### 2.8.5. Zvyšování povědomí a osvěta

Vzhledem k tomu, že od 1. ledna 2015 je účinný zákon o kybernetické bezpečnosti, se Úřad v uplynulém roce zaměřil především na vysvětlování jednotlivých ustanovení zákona o kybernetické bezpečnosti a z nich vyplývající práva a povinnosti, zejména pro správce prvků KII a VIS. Úřad k tomu využíval zejména různé konference a semináře, kde účastníky zajímaly především konkrétní dopady nových právních předpisů na jejich činnost, kritéria a způsob, jakým budou jednotlivé prvky KII a VIS určovány, a v neposlední řadě termíny, ve kterých budou muset plnit stanovené povinnosti. Konkrétní informační akcí k zákonu o kybernetické bezpečnosti byl například květnový celodenní seminář, který NCKB uspořádalo na půdě Fakulty podnikatelské Vysokého učení technického v Brně. Odborníci Úřadu na KII a VIS pak v průběhu roku přednášeli nebo se účastnili jako panelisté celkem 20 konferencí a v rámci své činnosti proškolili na 970 osob.

Pro pomoc a usnadnění orientace v problematice zákona o kybernetické bezpečnosti Úřad pravidelně vydává a aktualizuje množství podpůrných materiálů, které průběžně zveřejňuje na webových stránkách NCKB www.govcert.cz. Obdobnou osvětovou činnost vyvíjí i CSIRT.CZ a další české bezpečnostní týmy.

V květnu byl pod záštitou Úřadu, Masarykovy univerzity v Brně a odborného časopisu Global Politics uspořádán 2. ročník konference „CyberCon Brno 2015“. Konference byla primárně určena pro odbornou veřejnost a akademickou sféru.

Úřad dále vypracoval Návrh koncepce vzdělávání v oblasti kybernetické bezpečnosti, který vychází z aktuálních domácích i zahraničních zkušeností. Materiál vznikal především ve spolupráci s Ministerstvem školství, mládeže a tělovýchovy a jeho Národním ústavem pro vzdělávání, dále s Ministerstvem práce a sociálních věcí a za podpory dalších odborníků, kteří se vzděláváním v ICT a zvyšováním digitální gramotnosti dlouhodobě zabývají. Materiál především určuje podobu bezpečnostního vzdělávání pro jednotlivé cílové skupiny a doporučuje vhodné nástroje. Úloha Úřadu

spočívá vedle poskytnutí vlastní expertízy i v koordinaci vzdělávacích kapacit národních i zahraničních partnerských organizací.

Ve spolupráci s českou pobočkou AFCEA byl v září 2015 uskutečněn na Policejní akademii ČR seminář o kybernetické bezpečnosti. Zástupci Úřadu rovněž prezentovali na stánku AFCEA v rámci Mezinárodního veletrhu obranné a bezpečnostní techniky IDET. Sdružení AFCEA také ve spolupráci s Úřadem a Policejní akademií ČR vydalo 3. edici slovníku kybernetické bezpečnosti, který je široké veřejnosti k dispozici zdarma na internetových stránkách Úřadu.

Odborníci Úřadu přednášeli o kybernetické bezpečnosti i na dalších fórech, pořádaných např. Parlamentem České republiky.

Úřad svou záštitou podpořil vybrané významné osvětové akce, například mezinárodní kampaň „Evropský měsíc kybernetické bezpečnosti 2015“ vyhlašovanou každoročně Evropskou agenturou pro síťovou a informační bezpečnost (ENISA) a organizovanou neziskovým sdružením Národní centrum bezpečnějšího internetu, nebo řadu odborných konferencí organizovaných společností IDG, které byly zaměřeny na problematiku bezpečnosti pro IT profesionály z různých oborů.

V neposlední řadě odborníci Úřadu mnohokrát vystoupili na odborných konferencích, seminářích a diskutovali u kulatých stolů nad aktuálními tématy z oblasti kybernetické bezpečnosti, a to jak na národní, tak na mezinárodní úrovni. Zástupci Úřadu vysvětlovali důležitost kybernetické bezpečnosti včetně problematiky zákona o kybernetické bezpečnosti rovněž médiím, kde komentovali různé události, které byly způsobeny hackery nebo nestandardním chováním některých informačních systémů, vyjadřovali se k preventivním krokům a k eliminaci následků těchto událostí.

Seznam některých zkratek a pojmů použitých v této části je uveden v příloze.

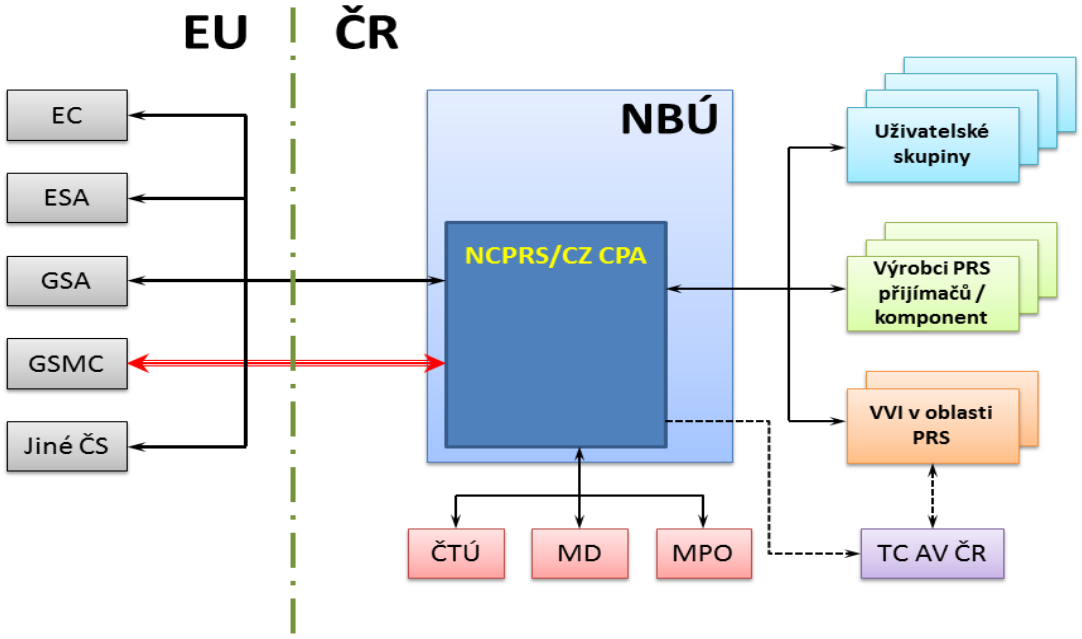
## 2.9. VÝKON FUNKCE PŘÍSLUŠNÉHO ORGÁNU PRS

Usnesením vlády ČR ze dne 30. ledna 2013 č. 71 k Akčnímu plánu implementace veřejně regulované služby programu Galileo (PRS) v České republice byla převedena problematika veřejně regulované služby programu Galileo (dále jen „služba PRS“) z kompetence rezortu Ministerstva dopravy na Úřad a ředitel Úřadu byl, v souladu s čl. 5 Rozhodnutí Evropského Parlamentu a Rady č. 1104/2011/EU ze dne 25. října 2011, o podmínkách přístupu k službě PRS nabízené globálním navigačním družicovým systémem na základě programu Galileo, pověřen výkonem funkce Příslušného orgánu PRS (Competent PRS Authority, dále jen „CPA“).

### 2.9.1. Budování národního centra PRS

Implementace služby PRS v ČR probíhá na základě schváleného Akčního plánu implementace veřejně regulované služby programu Galileo v České republice. V souladu se schváleným finančním rámcem a personálními opatřeními začal Úřad budovat Národní centrum PRS (dále jen „NCPRS“), které je zodpovědné za organizační zabezpečení přístupu ke službě PRS a za výkon funkce CPA. Organizační schéma zabezpečení služby PRS v ČR je zobrazeno na následujícím obrázku.

**Organizační schéma zabezpečení služby PRS v ČR**




Pro potřeby NCPRS byly v rámci rekonstrukce budovy Úřadu v Brně připraveny kancelářské prostory a zabezpečená oblast. V průběhu roku 2015 byla v těchto prostorách instalována technologie zabezpečující utajené spojení mezi NCPRS a Evropskou kosmickou agenturou (ESA), která je zodpovědná za vývoj systému Galileo.

V rámci řešení projektu bezpečnostního výzkumu Ministerstva vnitra VF20112013015 – „Pilotní projekt veřejně regulované služby evropského globálního navigačního družicového systému GALILEO“ byla v letech 2013 až 2015 vyvinuta aplikace pro evidenci a správu uživatelských skupin, citlivého materiálu a kryptografických klíčů pro zpřístupnění služby PRS. Tato aplikace odpovídá požadavkům stanoveným v zákoně a ve vyhlášce č. 432/2011 Sb., o zajištění kryptografické ochrany utajovaných informací.

V souladu s postupně uvolňovanými informacemi ze strany Evropské komise a ESA jsou realizovány nákupy techniky a technologií nezbytných pro zabezpečení chodu NCPRS.

### 2.9.2. Personální obsazení NCPRS

V současné době se problematice služby PRS věnují pouze 2 zaměstnanci Úřadu. Těžiště jejich činnosti spočívá v řešení problematiky služby PRS na evropské úrovni a zapojení ČR do pilotních projektů služby PRS, které jsou připravovány Evropskou komisí a Agenturou pro evropský GNSS a budou zahájeny po deklaraci dostupnosti služby PRS.

Z důvodu opožďování vývoje programu a faktického zpoždění při budování nezbytné infrastruktury bylo prozatím pozastaveno přijímání nových zaměstnanců do NCPRS.

### 2.9.3. Spolupráce s ostatními subjekty při implementaci služby PRS

Při řešení problematiky služby PRS NCPRS úzce spolupracuje zejména s Ministerstvem dopravy, jakožto národním koordinátorem pro správu a řízení evropských systémů družicové navigace. Další spolupráce byla navázána s Českým telekomunikačním úřadem a Ministerstvem obrany z důvodu plánovaného zapojení do pilotního programu PRS. Ministerstvo obrany a Úřad uzavřely v roce 2014 rámcovou dohodu o vzájemné podpoře vybraných činností, mezi které byla zařazena i oblast GNSS. V roce 2015 probíhala příprava prováděcího ujednání za oblast GNSS k provedení této dohody mezi Úřadem a Odborem vojskového průzkumu a elektronického boje.

Dalším důležitým úkolem NCPRS je koordinace aktivit spojených s přístupem k informacím a technologiím služby PRS. CPA má za povinnost zajistit, aby subjekty se sídlem na jeho území, které se chtějí podílet na výrobě nebo vývoji přijímačů PRS, bezpečnostních modulů nebo technologií s integrovanou službou PRS, splňovaly požadavky fyzické a administrativní bezpečnosti a byla jim udělena bezpečnostní akreditace v souladu se stanovenými podmínkami.

Na odborné úrovni rovněž probíhá komunikace se zástupci potenciálních uživatelů služby PRS.

## 2.10. OPRAVNÉ PROSTŘEDKY

### 2.10.1. Bezpečnostní řízení

V roce 2015 rozhodoval ředitel Úřadu o opravných prostředcích ze strany fyzických osob a podnikatelů podaných podle příslušných ustanovení zákona formou rozkladu proti následujícím rozhodnutím Úřadu:

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

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

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

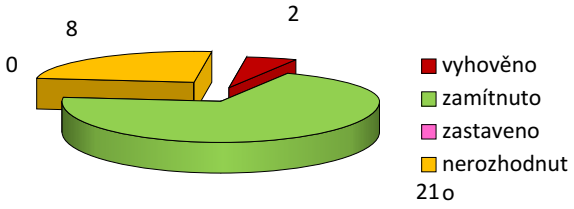
*2.10.1.1. Statistické přehledy*

*2.10.1.1.1. Rozklady*

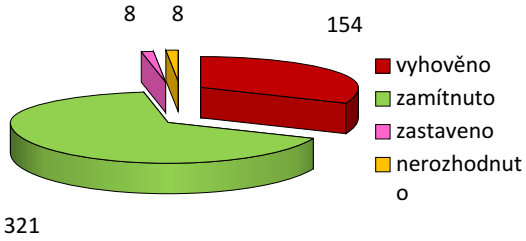
**Rozklady proti rozhodnutím Úřadu v oblasti bezpečnostního řízení**
*(rozhoduje ředitel Úřadu)*

| Rok | Dosud nerozhodnuto | Vyhověno | Zamítnuto | Zastaveno | Celkem |
|---|---|---|---|---|---|
| **2014** | 0 | 13 | 26 | 1 | **40** |
| **2015** | 8 | 2 | 21 | 0 | **31** |

**Řízení o rozkladu v roce 2015**




**Řízení o rozkladu v letech 2006 až 2015**




*2.10.1.1.2. Žaloby správní*

**Žaloby proti rozhodnutím ředitele Úřadu o rozkladu podle zákona v letech 2006 až 2015**
*(rozhoduje Městský soud v Praze)*

| Celkem | Dosud nerozhodnuto | Řízení zastaveno | Vyhověno | Zamítnuto | Odmítnuto |
|---|---|---|---|---|---|
| **100** | 23 | 17 | 13 | 45 | 2 |

*2.10.1.1.3. Kasační stížnosti*

**Kasační stížnosti podané účastníky řízení proti rozhodnutím Městského soudu v Praze o zamítnutí žaloby v letech 2006 až 2015** *(rozhoduje Nejvyšší správní soud v Brně)*

| Celkem | Dosud nerozhodnuto | Řízení zastaveno | Vyhověno | Zamítnuto | Odmítnuto |
|---|---|---|---|---|---|
| **25** | 2 | 0 | 5 | 16 | 2 |

**Kasační stížnosti podané Úřadem proti rozhodnutím Městského soudu v Praze o vyhovění žalobě v letech 2006 až 2015** *(rozhoduje Nejvyšší správní soud v Brně)*

| Celkem | Dosud nerozhodnuto | Řízení zastaveno | Vyhověno | Zamítnuto | Odmítnuto |
|---|---|---|---|---|---|
| **4** | 0 | 0 | 4 | 0 | 0 |

*2.10.1.1.4. Ústavní stížnosti*

**Ústavní stížnosti podané účastníky řízení v letech 2006 až 2015** *(rozhoduje Ústavní soud v Brně)*

| Celkem | Dosud nerozhodnuto | Řízení zastaveno | Vyhověno | Zamítnuto | Odmítnuto |
|---|---|---|---|---|---|
| **4** | 0 | 0 | 0 | 0 | 4 |

*2.10.1.1.5. Stížnosti k Evropskému soudu pro lidská práva*

V roce 2015 rozhodoval Evropský soud pro lidská práva o 1 stížnosti, která se týkala rozhodnutí Úřadu o zrušení platnosti osvědčení fyzické osoby a souvisejícího rozhodnutí ředitele Úřadu o zamítnutí rozkladu. Evropský soud pro lidská práva jednomyslně shledal, že v dané věci nedošlo k porušení práva stěžovatele na spravedlivý proces podle č. 6 odst. 1 Evropské úmluvy o lidských právech (uvedený rozsudek doposud nenabyl právní moci).

*2.10.1.2. Hodnocení rozhodovací praxe Úřadu*

Jak vyplývá z výše uvedených údajů, v současné době je rozhodnuto v 77 případech o žalobách proti rozhodnutí ředitele Úřadu o rozkladu, přičemž pouze 13 těchto žalob bylo shledáno důvodnými. „Úspěšnost" ředitele Úřadu tedy činí 83 %.

Všechny ústavní stížnosti podané proti rozhodnutím Úřadu, resp. jeho ředitele, podle zákona, byly Ústavním soudem odmítnuty pro zjevnou neopodstatněnost.

### 2.10.2. Správní řízení o pokutě

V roce 2015 ředitel Úřadu rozhodoval ve 3 případech o opravných prostředcích – rozkladech – uplatněných ze strany právnických osob ve správním řízení pro porušení povinností v oblasti ochrany utajovaných informací, přičemž všechna podání byla ředitelem Úřadu zamítnuta. Žaloba k Městskému soudu v Praze nebyla účastníky řízení ani v jednom případě podána.

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

V roce 2015 ředitel Úřadu nerozhodoval o žádném opravném prostředku – rozkladu – uplatněnému v řízení podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů.

## 2.11.VÝZKUMNÁ A VÝVOJOVÁ ČINNOST ÚŘADU

### 2.11.1. Cíle a organizace výzkumu a vývoje

Stejně jako v předchozích letech byl základním cílem v oblasti výzkumu a vývoje rozvoj bezpečnostních technologií pro ochranu utajovaných informací v komunikačních a informačních systémech. V důsledku rychlého rozvoje informačních technologií a nárůstu hrozeb kybernetických útoků se stále zvyšuje náročnost výzkumu a vývoje v oblasti bezpečnosti informačních technologií. S ohledem na kapacitní možnosti využívá Úřad pro řešení vývojových a výzkumných projektů osvědčený model – kromě vlastních pracovišť zapojuje externí odborná pracoviště popřípadě jednotlivé externí odborníky.

### 2.11.2. Projekty realizované v roce 2015

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

Některé realizované projekty navazovaly na projekty řešené v minulých letech. Hlavní příčinou této skutečnosti je již výše zmíněný rychlý technologický pokrok, vzhledem k němuž je nutná neustálá inovace již vyvinutých produktů.

V roce 2015 byly řádně dokončeny 2 projekty zahájené v letech 2013 a 2014, u dalších 4 projektů bylo úspěšně předáno dílo a počátkem roku 2016 proběhne oponentní řízení. Dále byly zahájeny 3 nové projekty. Všechny projekty byly realizovány ve spolupráci s externími řešiteli.

Projekty byly zaměřeny na oblast kryptografické ochrany a ochrany proti úniku utajovaných informací kompromitujícím vyzařováním.

Výsledkem realizovaných projektů jsou metodiky, analýzy, specializovaný hardware a software, technické a kryptografické prostředky a speciální měřící zařízení sloužící k uspokojení reálných potřeb bezpečnostní praxe, využitelné na národní úrovni zejména orgány státní správy a bezpečnostními složkami pracujícími s utajovanými informacemi.

V rámci projektů byl realizován vývoj a pilotní nasazení prostředků Sacom pro kryptografickou ochranu mobilních komunikací a USB kryptografických prostředků Klíčenka, o které je u orgánů státu značný zájem. Také byl finalizován vývoj, hodnocení a příprava výroby certifikovaných kryptografických prostředků PCA, kterých bylo v první etapě objednáno orgány státu 266 ks. Dále pokračoval vývoj různých modifikací prostředků typu PCS i LanPCS a byla finalizována výroba certifikovaných verzí kryptografických prostředků PCS i LanPCS objednávaných orgány státu.

V obecnější rovině jsou projekty prezentovány i na mezinárodní úrovni zahraničním bezpečnostním autoritám, s nimiž Úřad spolupracuje.

V souvislosti s projekty řešenými v rámci výzkumu a vývoje došlo k vylepšení technologického vybavení laboratoří Úřadu v souladu s aktuálními potřebami.

V roce 2015 Úřad dále rozvíjel svoji koncepci výzkumu a vývoje v oblasti kryptografické ochrany a ochrany proti úniku utajovaných informací kompromitujícím vyzařováním tak, aby mj. reflektovala požadavky rezortů státní správy, pro které jsou tyto druhy zajištění ochrany utajovaných informací nezbytné.

## 2.12. STÁTNÍ DOZOR

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

Cílem státního dozoru je především zjistit skutečný stav ochrany utajovaných informací, resp. plnění povinností v oblasti bezpečnostní způsobilosti u kontrolovaných osob, ověřit praktickou

aplikaci právních norem upravujících kontrolovanou oblast a zároveň přispět k zabezpečení ochrany utajovaných informací předcházením neoprávněnému nakládání s utajovanými informacemi a k posilování právního vědomí kontrolovaných osob a sjednocování způsobu aplikace právních předpisů v této oblasti.

O kontrole činnosti registrů utajovaných informací prováděné Úřadem podle § 79 odst. 7 zákona viz kapitolu 2.7.3.; o kontrole v oblasti kybernetické bezpečnosti prováděné Úřadem podle § 23 odst. 1 zákona o kybernetické bezpečnosti, viz kapitolu 2.8.

### 2.12.1. Kontroly provedené v roce 2015

Stejně jako v předchozích letech byly i v tomto roce kontroly prováděny na základě průběžně doplňovaných půlročních plánů kontrol schvalovaných ředitelem Úřadu. Z hlediska rozsahu byly realizovány zejména komplexní kontroly v oblasti ochrany utajovaných informací zaměřené na ověření skutečného stavu ve všech druzích zajištění ochrany utajovaných informací, které byly kontrolovanými osobami realizovány, a tematické kontroly v oblasti ochrany utajovaných informací, při kterých byly kontrolovány pouze vybrané oblasti. Ve druhém pololetí roku 2015 byla dále provedena 1 následná kontrola zaměřená na ověření odstranění nedostatků zjištěných při předcházející kontrole v oblasti ochrany utajovaných informací a bezpečnostní způsobilosti.

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

V roce 2015 provedl Úřad celkem 82 kontrol, z toho 13 v orgánech státu, jejich složkách nebo jimi zřizovaných příspěvkových organizacích, 4 v krajských a obecních úřadech a 65 u podnikatelů. Souhrnné údaje o kontrolách a přehled jednotlivých kontrolních akcí realizovaných v roce 2015 je uveden v následujících tabulkách.

**Kontroly provedené v roce 2015**

| Kontroly | Komplexní | Tematické | Následné | Celkem |
|---|---|---|---|---|
| **Orgány státu** | 11 | 1 | 1 | **13** |
| **Krajské a obecní úřady** | 4 | 0 | 0 | **4** |
| **Podnikatelé** | 56 | 9 | 0 | **65** |
| **Celkem** | **71** | **10** | **1** | **82** |

**Kontroly v orgánech státu, jejich součástech a jimi zřizovaných příspěvkových organizacích v roce 2015**

| Kontrolovaná osoba | Kontrolovaná osoba |
|---|---|
| Ministerstvo práce a sociálních věcí | Ministerstvo zahraničních věcí – zastupitelský úřad ČR v Madridu |
| Vězeňská služba ČR | |
| Ministerstvo zahraničních věcí – zastupitelský úřad ČR v Lisabonu | Ministerstvo zahraničních věcí – zastupitelský úřad ČR v Kodani |

| Kontrolovaná osoba | Kontrolovaná osoba |
|---|---|
| Ministerstvo zahraničních věcí – zastupitelský úřad ČR v Oslu | Ministerstvo zahraničních věcí – zastupitelský úřad ČR v Dillí |
| Úřad průmyslového vlastnictví | Ministerstvo zahraničních věcí – zastupitelský úřad ČR v Tel Avivu |
| Ministerstvo zemědělství | |
| Kancelář poslanecké sněmovny Parlamentu ČR | Národní muzeum |
| Ředitelství silnic a dálnic ČR | |

**Kontroly v krajských a obecních úřadech v roce 2015**

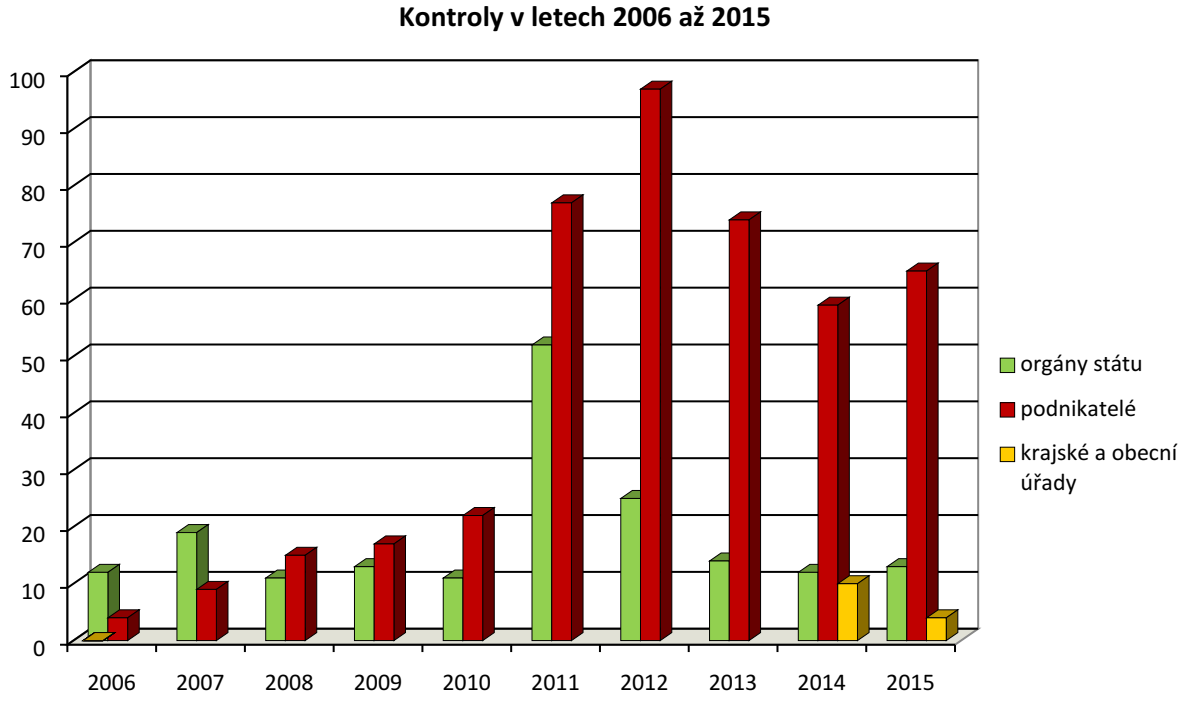
| Kontrolovaná osoba | Kontrolovaná osoba |
|---|---|
| Krajský úřad Karlovarského kraje | Krajský úřad Ústeckého kraje |
| Krajský úřad Olomouckého kraje | Magistrát hlavního města Prahy |

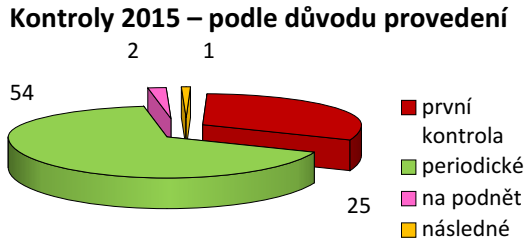
**Kontroly u podnikatelů v roce 2015**

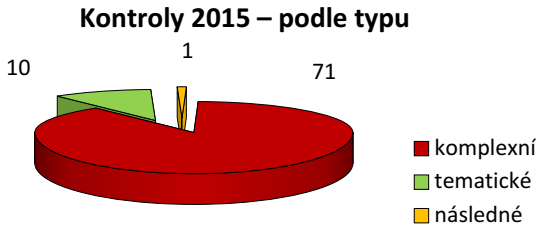
| Kontrolovaná osoba | Kontrolovaná osoba |
|---|---|
| ANECT a.s. | INKOS-OSTRAVA, a.s. |
| ARYKA IN-WEST a.s. | Jiří Vrba |
| Atos IT Solutions and Services, s.r.o. | KALÁB-stavební firma, spol. s r.o. |
| B.O.I.S. – FILTRY, spol. s r.o. | KAPPENBERGER + BRAUN, Elektro-Technik, spol. s r.o. |
| BDO IT a.s. | KELCOM International Liberec, společnost s ručením omezeným |
| CB SERVIS CENTRUM s.r.o. | |
| CENTR GROUP, a.s. | KOMIX s.r.o. |
| COLAS CZ, a.s. | KonekTel, a.s. |
| Comproject s.r.o. | Lesní stavby, s.r.o. |
| Czasch spol. s r.o. | LETIŠTĚ BRNO a.s. |
| ČD – Informační Systémy, a.s. | MERO ČR, a.s. |
| ČD – Telematika a.s. | MHM computer a.s. |
| ČD Cargo, a.s. | OMNICON s.r.o. |
| ČEZ, a. s. | OPTOKON, a.s. |
| G4S Secure Solutions (CZ), a.s. | OPTYS spol. s r.o. |
| GiTy, a.s. | PERFECTED s.r.o. |
| Griffin, a.s. | Prototypa-ZM, s.r.o. |
| ha-vel internet s.r.o. | První brněnská strojírna Velká Bíteš, a.s. |
| HEWLETT-PACKARD s.r.o. | První KEY – STAV, a.s. |
| HOCHTIEF CZ a.s. | RAPOS, spol. s r.o. |
| IBM Česká republika, spol. s r.o. | ROHDE & SCHWARZ – Praha, s.r.o. |
| Indra Czech Republic s.r.o. | SAP ČR, spol. s r.o. |

| Kontrolovaná osoba | Kontrolovaná osoba |
|---|---|
| SATRA, spol. s r.o. | TIPA Telekom plus a.s. |
| Sec-Communication, a.s. | T-Mobile Czech Republic a.s. |
| SIEZA, a.s. (PUY Czech, a.s.) | Tractebel Engineering a.s. |
| Simac Technik ČR, a.s. | UJP PRAHA a.s. |
| SITEL, spol. s r.o. | ÚJV Řež, a.s. |
| SKILL s.r.o. | UNIS, a.s. |
| SKS s.r.o. | VAE CONTROLS, s.r.o. |
| STAVITELSTVÍ ŘEHOŘ, s.r.o. | VARIEL, a.s. |
| Svoboda a syn, s.r.o. | VÍTKOVICE IT SOLUTIONS a.s. |
| SYSCOM SOFTWARE spol. s r.o. | Vodafone Czech Republic a.s. |
| Technický a zkušební ústav stavební Praha, s.p. | |

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






## 2.12.2. Výsledky kontrol

Nedostatky zjištěné při kontrolách, vyplývající z porušení nebo nedodržení jednotlivých ustanovení zákona a dalších právních předpisů, jsou uváděny jako kontrolní zjištění v protokolech o jednotlivých kontrolách. Z celkového počtu 82 kontrol provedených v roce 2015 byly nedostatky zjištěny ve 48 případech (59 %). V 10 případech (12 %) byl, vzhledem k charakteru zjištěných nedostatků, podán podnět k zahájení správního řízení pro podezření ze spáchání přestupku nebo správního deliktu.

Nedostatky se, obdobně jako v předcházejících letech, objevovaly téměř ve všech druzích zajištění ochrany utajovaných informací. Rovněž byly zjištěny nedostatky v oblasti bezpečnostní způsobilosti. Příčinou nedostatků bylo ve většině případů selhání lidského činitele. Při kontrolách provedených v roce 2015 byly zjištěny zejména následující nedostatky (včetně nedostatků zjištěných při kontrole zahájené v roce 2014, která byla dokončena až začátkem roku 2015 – viz zprávu o činnosti Úřadu za rok 2014):

Obecné nedostatky

- nesplnění některé z podmínek pro výkon funkce bezpečnostního ředitele,
- neoznámení zřízení nebo obsazení funkce bezpečnostního ředitele,
- nekontrolování dodržování povinností stanovených zákonem,
- nesoulad postupu stanoveného vnitřním předpisem pro manipulaci s utajovaným dokumentem s platnou právní úpravou (neaktuální vnitřní předpis).

Personální bezpečnost

- neoprávněný přístup k utajované informaci zjištěný u fyzické osoby, která nesplňovala některou ze zákonem stanovených podmínek pro tento přístup (neprovedení poučení, absence osvědčení fyzické osoby nebo oznámení o splnění podmínek pro přístup k utajované informaci stupně utajení Vyhrazené, případně dokladu, nedodržení principu „need to know“),
- nesplnění některé z podmínek pro přístup k utajované informaci u osoby vykonávající činnost nebo funkci, pro kterou to vyžaduje právní předpis (výkon správy informačních systémů),
- neprovádění pravidelného školení osob, které mají přístup k utajovaným informacím,
- neprovádění ověření, zda fyzická osoba po uplynutí zákonem stanovené lhůty i nadále splňuje podmínky pro přístup k utajované informaci stupně utajení Vyhrazené,
- nezaslání výtisku poučení Úřadu podle § 11 odst. 2 zákona,

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

- nedostatky ve vedení evidence osob, které mají přístup k utajované informaci (nedostatečné, chybné nebo neaktuální údaje),

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

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

Průmyslová bezpečnost

- nesplnění povinnosti oznámit Úřadu změny údajů uvedených v žádosti podnikatele.

Administrativní bezpečnost

- nedostatky ve způsobu vedení evidence utajovaných dokumentů a ve vedení dalších administrativních pomůcek (neúplné nebo nesprávné zápisy, chybně prováděné opravy, neuzavírání zápisů v jednacím protokolu na konci kalendářního roku, neuvedení všech osob, které se seznámily s obsahem utajovaného dokumentu, v kontrolním listu),

- neevidování utajovaného dokumentu,

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

- neplnění dalších povinností stanovených v oblasti administrativní bezpečnosti právními předpisy (např. při změně nebo zrušení stupně utajení nebo při změně osoby pověřené vedením evidence utajovaných dokumentů, neuvádění údajů o skartaci utajovaných dokumentů).

Činnost registrů utajovaných informací

- neaktuální evidenční list registru,

- neoznámení změn stanovených právními předpisy,

- nedostatky ve vedení seznamů osob, kterým lze v registru umožnit přístup k utajovaným informacím cizí moci (neaktuální údaje),

- nedostatky při manipulaci a evidenci utajovaných dokumentů cizí moci (chybně provedené opravy evidenčních údajů na utajovaném dokumentu, používání administrativních pomůcek, které nejsou evidovány).

Fyzická bezpečnost

- nedostatky v realizaci opatření fyzické bezpečnosti (nesplnění požadavků na zajištění nepřetržité ostrahy objektu),

- nesoulad skutečného stavu opatření fyzické bezpečnosti se stavem deklarovaným v projektu fyzické bezpečnosti (nesprávné bodové hodnocení informačního systému v projektu),

- neplnění dalších povinností stanovených v oblasti fyzické bezpečnosti právními předpisy (neaktualizování projektu fyzické bezpečnosti, absence průběžného provádění hodnocení rizik nebo ověřování, zda použitá opatření fyzické bezpečnosti odpovídají projektu fyzické bezpečnosti, neprovádění funkčních zkoušek technických prostředků po uplynutí doby platnosti jejich certifikátu).

Bezpečnost informačních a komunikačních systémů

- zpracování utajovaných informací v informačním systému, který nebyl certifikován Úřadem,

- absence jmenování osob do rolí ve správě informačního sytému,

- nesplnění požadavků na konfiguraci a provoz informačního systému (nedostatky v nastavení systému, např. uzamčení administrátorských účtů, nepodporovaný antivirový SW nebo neprovádění aktualizace virové databáze, používání neznámého SW, připojení neschválených periferních zařízení, použití neevidovaných nosičů informací),

- nedostatky v dokumentaci IS (rozpory údajů uvedených v dokumentaci se skutečným stavem, např. u stanovené kategorie zabezpečené oblasti, nebo s údaji uvedenými v projektu fyzické bezpečnosti).

Bezpečnostní způsobilost

- výkon citlivé činnosti osobou, která není držitelem dokladu nebo osvědčení fyzické osoby,

- nevedení evidence osob, které vykonávají citlivou činnost,

- nezaslání oznámení o zahájení nebo oznámení o skončení výkonu citlivé činnosti.

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

## 2.13. METODICKÁ ČINNOST ÚŘADU

Metodickou činnost vůči orgánům státu a jejich organizačním složkám a vůči podnikatelům vykonával Úřad v roce 2015 především v rámci odborné činnosti jednotlivých organizačních celků Úřadu, a to prostřednictvím poskytování osobních konzultací, odpovídání na telefonické, písemné nebo elektronickou formou položené dotazy a rovněž při výkonu státního dozoru a provádění tzv. dohlídek v průběhu bezpečnostního řízení u podnikatelů.

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

Nejčastěji kladené dotazy a odpovědi stejně jako vydávaná stanoviska a jednotné návody Úřad uveřejňuje na svých internetových stránkách (viz kap. 2.14.2.).

### 2.13.1. Metodická činnost v oblasti bezpečnostního řízení

Metodická činnost Úřadu v oblasti bezpečnostního řízení je nezbytným, trvalým a kontinuálním procesem, který probíhal i v roce 2015. 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, nebo s postupem podle § 103 zákona, podle kterého je Úřad oprávněn požadovat upřesnění údajů uvedených v žádosti nebo sdělení doplňujících údajů k ověření splnění podmínek pro vydání osvědčení fyzické osoby nebo podnikatele nebo dokladu.

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

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

I nadále bylo výraznou oblastí metodické činnosti Úřadu poskytování konzultací, doporučení a stanovisek pro podnikatele v souvislosti s institutem prohlášení podnikatele podle § 15a zákona.

Těžiště metodické činnosti v hodnoceném roce bylo orientováno do oblastí poskytování prvotních informací a metodických doporučení před podáním žádosti, poskytování pomoci, konzultací a metodických doporučení při odstraňování nedostatků žádosti a zejména do oblasti metodického vedení osob, které jsou již držiteli osvědčení, a dále poskytování informací a metodické pomoci pro podnikatelské subjekty, které hodlaly učinit prohlášení.

V souvislosti s konzultační a metodickou činností Úřadu nelze opomenout účast jeho zaměstnanců na přednáškách, seminářích a školeních organizovaných různými státními, ale i soukromými subjekty. Tato metodická činnost Úřadu byla zaměřena na poskytnutí informací k zákonu, otázkám bezpečnostního řízení a povinnostem držitelů osvědčení.

## 2.14. VĚSTNÍK ÚŘADU A INTERNETOVÉ STRÁNKY ÚŘADU

### 2.14.1. Věstník Úřadu

Úřad vydává, v souladu se zákonem, Věstník Úřadu jako periodickou tiskovinu, která vychází dvakrát ročně, v případě potřeby i vícekrát. V roce 2015 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, bezpečnostní způsobilosti a kybernetické bezpečnosti. Dále jsou zveřejňovány metodické návody, různé pokyny, návody a instrukce, žádosti a informace určené odborné veřejnosti.

Věstník Úřadu není distribuován formou volného prodeje. Lze jej zakoupit pouze předplatitelskou formou. Věstník lze rovněž objednat přímo v obchodním oddělení Tiskárny Ministerstva vnitra.

Obsah Věstníku Úřadu je zveřejňován také na internetových stránkách Úřadu.

### 2.14.2. Internetové stránky Úřadu

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

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

a zpřístupněny jsou i elektronické verze dotazníků a žádostí. Je zde umístěn i odkaz na protikorupční linku 199. Internetové stránky vždy obsahují poslední číslo Věstníku Úřadu.

Obsahem svých internetových stránek Úřad také reaguje na nejčastěji kladené dotazy tak, aby na nich jejich uživatelé nalezli vše, co potřebují vědět o problematice utajovaných informací, bezpečnostní způsobilosti i o Úřadu samotném. V roce 2015 zůstaly nejvíce vyhledávanými informace týkající se bezpečnostního řízení.

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

Internetové stránky Úřadu splňují pravidla přístupnosti podle vyhlášky č. 64/2008 Sb., o formě uveřejňování informací souvisejících s výkonem veřejné správy prostřednictvím webových stránek pro osoby se zdravotním postižením (vyhláška o přístupnosti), a s jejich obsahem se tak mohou seznámit i osoby se zdravotním postižením.

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

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

V roce 2015 bylo Úřadu podáno 10 žádostí o informace podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů.

Všem žádostem bylo v plném rozsahu vyhověno a požadované informace byly žadatelům poskytnuty. Rozhodnutí o odmítnutí žádosti tedy nebylo vydáno žádné.

V roce 2015 nebyla poskytnuta žádná výhradní licence ani nebyla podána žádná stížnost podle § 16a zákona č. 106/1999 Sb.

## 2.16. INSPEKCE ŘEDITELE ÚŘADU

Inspekce ředitele Úřadu v průběhu roku 2015 prováděla, v rámci plnění dlouhodobých úkolů, činnosti související s výkonem interní kontroly určených oblastí působnosti Úřadu.

V roce 2015 nebyla inspekcí ředitele Úřadu řešena žádná stížnost.

# 3. BEZPEČNOSTNÍ, EKONOMICKÉ A PERSONÁLNÍ ZABEZPEČENÍ ÚŘADU

## 3.1.OCHRANA UTAJOVANÝCH INFORMACÍ A KRIZOVÉ ŘÍZENÍ V ÚŘADU

### 3.1.1. Vnitřní kontrola ochrany utajovaných informací

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

V roce 2015 byla kontrolní činnost zaměřena na dodržování povinností stanovených zákonem a interními akty řízení Úřadu, zejména směrnicí ředitele Úřadu č. 13/2007, o provozním řádu Národního bezpečnostního úřadu (dále jen „provozní řád“).

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

V roce 2015 nebylo zjištěno závažné porušení ochrany utajovaných informací zaměstnanci Úřadu. Rovněž ustanovení provozního řádu byla v roce 2015 zaměstnanci Úřadu dodržována a při kontrolách nebyly zjištěny závažné nedostatky.

### 3.1.2. Personální bezpečnost v rámci Úřadu

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

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

V roce 2015 bylo evidováno 63 žádostí o vydání osvědčení fyzické osoby, vydáno bylo 55 osvědčení fyzické osoby. Ve zbývajících případech nebyla bezpečnostní řízení k 31. prosinci 2015 ukončena.

**Vydaná osvědčení fyzické osoby v rámci Úřadu v roce 2015**

| | |
|---|---|
| **Důvěrné** | 3 |
| **Tajné** | 34 |
| **Přísně tajné** | 18 |
| **Celkem** | **55** |

**Důvody zániku platnosti osvědčení fyzické osoby v rámci Úřadu v roce 2015**

| | |
|---|---|
| **Doručení nového osvědčení** | 51 |
| **Změna některého z údajů uvedených v osvědčení** | 2 |
| **Vráceno uživatelem** | 2 |
| **Celkem** | **55** |

**Vydaná osvědčení fyzické osoby pro cizí moc v rámci Úřadu v roce 2015**

| | |
|---|---|
| **COSMIC TOP SECRET ATOMAL** | 1 |
| **COSMIC TOP SECRET** | 8 |
| **NATO SECRET** | 7 |
| **Celkem** | **16** |

V roce 2015 bylo dále vydáno 9 oznámení o splnění podmínek pro přístup k utajované informaci stupně utajení Vyhrazené.

### 3.1.3. Fyzická bezpečnost v rámci Úřadu

V roce 2015 byla dokončena rekonstrukce elektrické požární signalizace a byl modernizován poplachový zabezpečovací a tísňový systém pro objekty areálu Úřadu v Praze. Dále v loňském roce Úřad převzal zrealizovanou zakázku rozšíření uzavřeného kamerového televizního okruhu v areálu NCKB v Brně.

### 3.1.4. Krizové řízení v rámci Úřadu

V roce 2015 se zástupci Úřadu účastnili jednání se zástupci Ministerstva vnitra, Ministerstva obrany, Generálního ředitelství Hasičského záchranného sboru a s Výborem pro civilní nouzové plánování. Uvedeným subjektům byla poskytována nezbytná součinnost.

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

### 3.1.5. Ostatní činnosti

Odbor bezpečnostní zajišťuje rovněž evidenční ochranu zaměstnanců Úřadu v případě jejich ohrožení v souvislosti s výkonem povolání. V roce 2015 byla opakovaně prováděna periodická aktualizace seznamu chráněných osob.

V rámci bezpečnostní agendy boje proti korupci byla v roce 2015 vytvořena analýza korupčních rizik, která slouží k aktualizaci Interního protikorupčního programu Úřadu, který byl rovněž aktualizován.

V rámci zajišťování provozu vozového parku v Úřadu byl v roce 2015 proveden nákup 4 nových vozidel. Na základě harmonogramu obměny vozového parku pro roky 2015 až 2017 byla 3 vozidla vyřazena. V průběhu roku 2015 probíhal zkušební provoz elektronické knihy jízd.

## 3.2. ARCHIV NÁRODNÍHO BEZPEČNOSTNÍHO ÚŘADU

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

Archiv v rámci činnosti bezpečnostního archivu pečuje o archiválie označené stupněm utajení a v rámci činnosti specializovaného archivu o neutajované archiválie. Archiv dohlíží na výkon spisové služby Úřadu a pravidelně provádí výběr archiválií ve skartačním řízení. Archiválie jsou vedeny v základní evidenci Národního archivního dědictví. V roce 2015 bylo provedeno 22 archivních prohlídek a vydáno 22 protokolů o provedeném skartačním řízení. Celkový rozsah archiválií je ke dni 31. prosince 2015 v bezpečnostním archivu 9,62 běžných metrů a ve specializovaném archivu 10,24 běžných metrů. V roce 2015 navštívil bezpečnostní archiv 1 interní badatel a specializovaný archiv také 1 interní badatel.

Na konci roku 2015 byl zahájen proces zpracování analýzy současného stavu Archivu a návrh řešení výstavby digitálního archivu. Analýza bude dokončena v průběhu roku 2016.

## 3.3. EKONOMICKÉ ZABEZPEČENÍ ÚŘADU

Úřad je od 1. listopadu 1998 samostatnou kapitolou státního rozpočtu „308“. V roce 2015 byla jeho činnost financována výhradně ze státního rozpočtu; dále odvedl do státního rozpočtu celkem 30 544 tis. Kč. Tato částka je tvořena příjmy z rozpočtu EU ve výši 29 270 tis. Kč za projekt, který byl realizován v roce 2014. Dalšími příjmy jsou správní poplatky vybrané ve výši 240 tis. Kč, vybrané pokuty ve výši 228 tis. Kč, příjem z licenční smlouvy ve výši 270 tis. Kč a nahodilé příjmy např. přeplatky z minulých let ve výši 535 tis. Kč (např. refundace letenek ve výši 117 tis. Kč, vratka za stravné ve výši 185 tis. Kč).

Konečný rozpočet výdajů činil v roce 2015, po rozpočtových opatřeních, 393 754 tis. Kč. Celkové výdaje zahrnují 108 221 tis. Kč na budování NCKB v souladu s usnesením vlády ČR č. 781 ze dne 19. října 2011, o ustavení Národního bezpečnostního úřadu gestorem problematiky kybernetické bezpečnosti.

Rozpočet roku 2015 byl dále posílen o nespotřebované výdaje roku 2014 ve výši 64 531 tis. Kč. Důvodem nespotřebování těchto výdajů byl zejména fakt, že bylo vládou odloženo čerpání výdajů ve výši 8 267 tis. Kč na plnění úkolů souvisejících s implementací služby PRS. Dále pak byly do rozpočtu roku 2015 převedeny nespotřebované finanční prostředky v objemu 39 167 tis. Kč, a to na dobudování NCKB, kdy v roce 2014 bylo rozhodnuto o realizaci projektu – vybudování přístavby

ke stávající budově v Brně, speciálně zabezpečeného jednacího sálu pro cca 60 osob. Stavební akce bude financována z NNV roku 2014.

Rozpočet roku 2015 byl čerpán ve výši 310 410 tis. Kč. Největší objem běžných výdajů tvořily, jako každým rokem, mzdové výdaje a zákonem dané odvody, které byly vyčerpány na 96 %. Nevyužitá mzdová část z nenaplněných tabulek NCPRS, které není zatím plně funkční, bude vrácena do státního rozpočtu.

Běžné výdaje na provoz, zejména platby v oblasti energií, nezbytných služeb a nákupů k zajištění činnosti Úřadu, NCKB a NCPRS, činily po rozpočtových změnách 81 198 tis. Kč (posíleny byly o nespotřebované výdaje roku 2014) a byly čerpány na úrovni 92,31 %.

Kapitálové výdaje byly posíleny o nespotřebované výdaje roku 2014 a konečné čerpání činilo 31 010 tis. Kč, z čehož na budování NCKB a NCPRS bylo vyčerpáno 8 838 tis. Kč, a to zejména na informační technologie. Kapitálové výdaje ve výši 11 398 tis. Kč byly vyčerpány na projekty výzkumu a vývoje.

Výzkum a vývoj byl v plném rozsahu financován z vlastních prostředků kapitoly, tj. bez dotací výzkumu a vývoje z jiných částí státního rozpočtu, v celkové výši 17 568 tis. Kč. Vyčerpáno bylo 14 219 tis. Kč. Z toho v rámci uzavřených smluvních závazků s externími řešiteli bylo na výzkumné projekty vyčerpáno 11 733 tis. Kč a v rámci vlastních výzkumných kapacit bylo vyčerpáno 2 485 tis. Kč.

Celkem činí nároky nespotřebovaných výdajů z rozpočtu roku 2015 částku 83 343 tis. Kč, z toho jsou kapitálové výdaje ve výši 68 544 tis. Kč, jedná se zejména o finanční prostředky určené na vybudování přístavby budovy NCKB v Brně, včetně akustiky a vnitřního zařízení. Záměr stavby je ve fázi stavebního řízení. Dále jsou prostředky určeny na nákup speciálních přístrojů a technologií potřebných pro řádné fungování nově vznikajícího NCKB a budoucího pracoviště NCPRS. Dále jsou výdaje určeny na pokrytí smluvních závazků uzavřených v roce 2015.

Každoroční tlak Ministerstva financí na snižování rozpočtů kapitol státního rozpočtu se Úřadu od roku 2013 daří na základě odůvodněných požadavků stabilizovat a lze jej již čtvrtým rokem považovat za vyrovnaný. Rozpočet se navyšuje pouze o financování nově svěřených činností dle výše uvedených usnesení vlády, tzn., že bylo pro rok 2015 rozpočtováno na financování budování NCKB 108 221 tis. Kč (včetně nespotřebovaných výdajů roku 2014). Tyto výdaje jsou vykazovány a sledovány zvlášť, včetně tabulkových počtů, mezd a zákonem daných odvodů, tj. mimo rozpočet na provoz Úřadu, stejně tak výdaje na NCPRS, na které měl Úřad k dispozici, včetně nespotřebovaných výdajů roku 2014, 15 778 tis. Kč, které však byly čerpány z výše uvedených důvodů pouze z jedné třetiny, a to zejména na mzdy a s tím související výdaje.

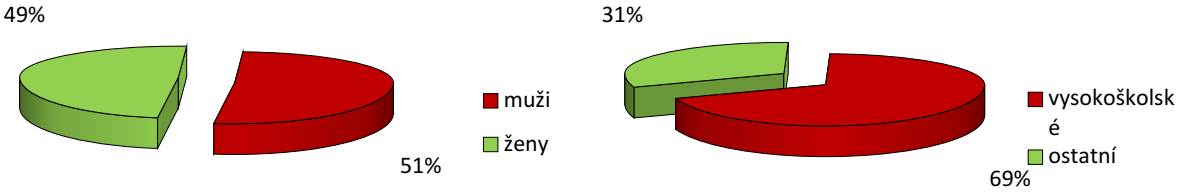
Veškeré finanční prostředky, určené na financování činnosti Úřadu, projednává čtvrtletně komise pro hospodaření s finančními prostředky Úřadu a procházejí předběžnou a průběžnou finanční kontrolou. Následná kontrola je prováděna na pozici hlavní účetní a u vybraných finančních operací průřezově i správcem rozpočtu. Příkazci operací úzce spolupracují se správcem rozpočtu a majetkovou evidencí, což lze považovat i za částečnou následnou kontrolu nad rámec zákona o finanční kontrole.

## 3.4. PERSONÁLNÍ ZABEZPEČENÍ ÚŘADU

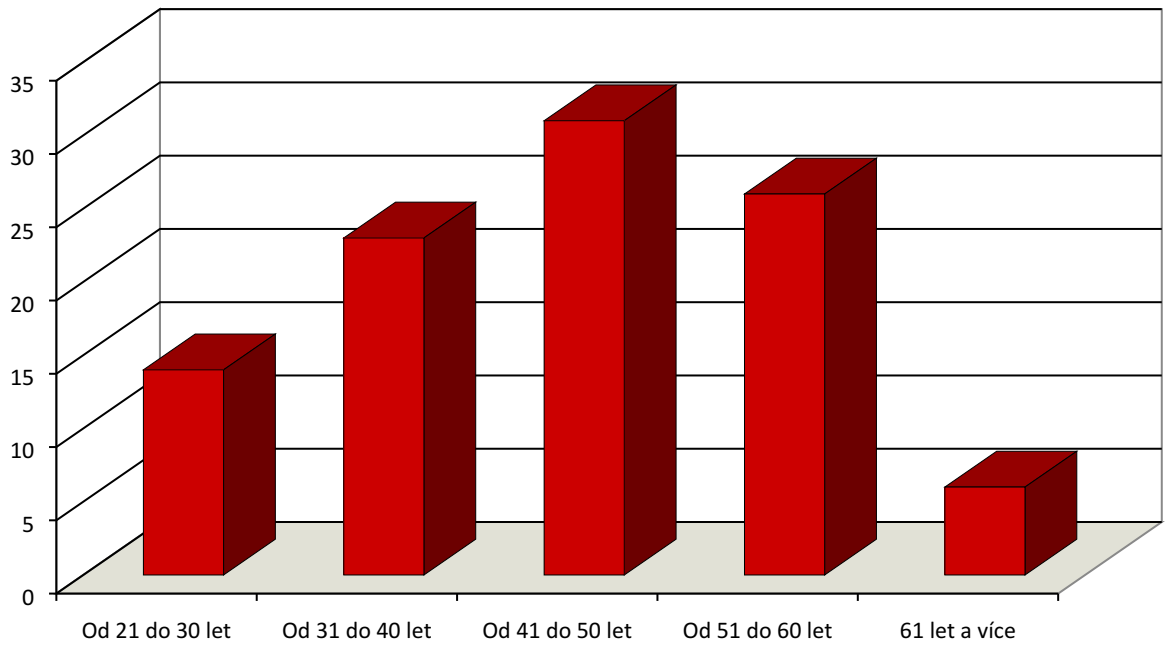
Pro rok 2015 měl Úřad 316 systemizovaných pracovních míst, z tohoto počtu bylo 30 míst určeno pro NCKB, resp. problematiku kybernetické bezpečnosti, a 7 míst pro NCPRS. V průběhu roku byla všechna pracovní místa v NCKB obsazována novými, převážně mladými odborníky. Dále se rozvíjí spolupráce s vysokými školami a dalšími subjekty působícími v této oblasti. Celkem 4 pracovní místa v NCPRS nebyla koncem roku obsazena, protože zatím nebyly vládou ČR schváleny příslušné dokumenty a činnosti na pracovišti nemohou být vykonávány v plném rozsahu.

K 31. prosinci 2015 bylo aktuálně obsazeno 307 pracovních míst, z toho bylo 157 mužů a 150 žen. Průměrný věk zaměstnanců byl 47 let, více než 68,5 % 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**




**Struktura zaměstnanců Úřadu podle věku (v %)**



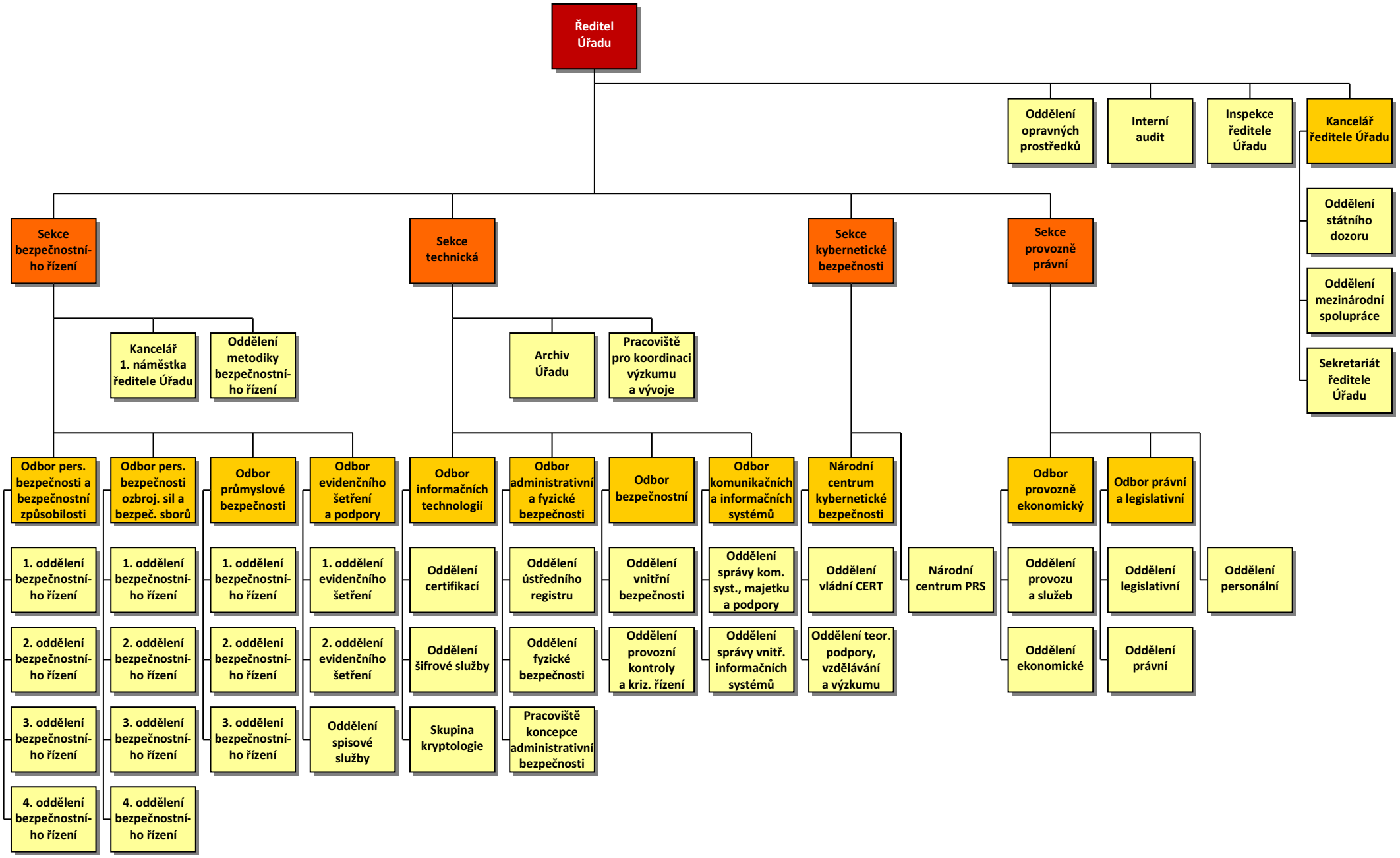
V Úřadu je průběžně realizován systém vzdělávání zaměstnanců. V roce 2015 pokračovalo skupinové i individuální jazykové vzdělávání, kterého se pravidelně účastnilo více než 80 zaměstnanců. Probíhaly jazykové kurzy angličtiny, němčiny, francouzštiny a ruštiny (v NCKB Brno).

Dále probíhala odborná školení především v oblasti informačních technologií a kybernetické bezpečnosti, a to v ČR i v zahraničí. Úřad navázal úzkou spolupráci se společností SANS Institute. V rámci této spolupráce se pracovníci NCKB v roce 2015 zúčastnili odborných školení nejvyšší úrovně pořádané společností SANS Institute v oblasti předcházení, detekce a reakce na kybernetické útoky, plánování a provádění penetračního testování, digitální forenzní analýzy a bezpečnosti průmyslových systémů (viz kap. 2.8.1.).

Dále byla věnována pozornost zdokonalení komunikačních dovedností zaměstnanců, kteří přicházejí do kontaktu s veřejností. Školení byla účastníky hodnocena velmi kladně, s velkým přínosem pro praxi.

Zaměstnanci měli možnost se dále vzdělávat v oblastech, které bezprostředně souvisejí s jejich pracovními činnostmi, tj. především v oblasti právní, ekonomické a technické. Možnost odborného a jazykového vzdělávání zaměstnanců je jedním z motivačních prvků, které Úřad využívá.

# Organizační schéma Úřadu v roce 2015



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

AFCEA – Armed Forces Communications and Electronics Association

CCDCOE – Cooperative Cyber Defence Centre of Excellence

CECSP – Central European Cyber Security Platform

CERT – Computer Emergency Response Team

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

CSIRT – Computer Security Incident Response Team

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

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

EU – Evropská unie

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

HONEYPOT – slouží jako návnada lákající útočníka, přičemž po zachycení potenciálně nebezpečného software dochází k jeho automatizované analýze

IDG konference – International Data Group konference

KII – Kritická informační infrastruktura

MALWARE – počítačový program určený ke vniknutí nebo poškození počítačového systému

NATO – Severoatlantická aliance (North Atlantic Treaty Organization)

NCKB – Národní centrum kybernetické bezpečnosti

PHISHING – podvodná metoda usilující o zcizení citlivých údajů uživatele za účelem jejich zneužití, většinou vytvořením podvodné zprávy, šířené většinou elektronickou poštou, jež se snaží citlivé údaje z uživatelů vylákat; zprávy mohou být maskovány tak, aby co nejvíce imitovaly důvěryhodného odesílatele

SCADA systém (Supervisory Control And Data Acquisition) – počítačový systém pro dispečerské řízení a sběr údajů. Mohou to být průmyslové řídicí systémy, nebo počítačové systémy monitorování a řízení procesů. Procesy mohou být průmyslové (např. výroba elektrické energie), infrastrukturní (např. rozvod pitné vody) nebo zařízení (např. železniční stanice).

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

VIS – Významný informační systém

**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. | Legislativní činnost v rámci EU | 4 |
| 2.1.3. | Vnitřní legislativní činnost | 5 |
| 2.1.4. | Vyjádření k oznámení podle § 69 odst. 1 písm. r) zákona | 5 |
| 2.1.5. | Právní činnost | 5 |
| 2.2. | MEZINÁRODNÍ SPOLUPRÁCE ÚŘADU | 7 |
| 2.2.1. | Mezinárodní smlouvy | 7 |
| 2.2.1.1. | Hodnocení sjednávání smluv o ochraně utajovaných informací za rok 2015 | 7 |
| 2.2.1.2. | Výhled na rok 2016 | 8 |
| 2.2.2. | Aktivity v rámci NATO a EU a spolupráce s bezpečnostními úřady partnerských států | 8 |
| 2.2.3. | Mezinárodní aktivity v oblasti kybernetické bezpečnosti | 9 |
| 2.3. | PERSONÁLNÍ BEZPEČNOST | 11 |
| 2.3.1. | Bezpečnostní řízení o žádostech fyzických osob | 11 |
| 2.3.2. | Prověřování splňování podmínek po vydání osvědčení fyzické osoby | 12 |
| 2.3.3. | Analýza důvodů nevydání nebo zrušení platnosti osvědčení fyzické osoby | 12 |
| 2.3.4. | Přehled ostatních důvodů zániku platnosti osvědčení fyzické osoby | 13 |
| 2.3.5. | Statistické přehledy | 13 |
| 2.3.6. | Personální projekt | 17 |
| 2.4. | BEZPEČNOSTNÍ ZPŮSOBILOST | 18 |
| 2.4.1. | Statistické přehledy | 19 |
| 2.5. | PRŮMYSLOVÁ BEZPEČNOST | 19 |
| 2.5.1. | Bezpečnostní řízení o žádostech podnikatelů | 20 |
| 2.5.2. | Prověřování splňování podmínek po vydání osvědčení podnikatele | 20 |
| 2.5.3. | Analýza důvodů nevydání nebo zrušení platnosti osvědčení podnikatele | 21 |
| 2.5.4. | Přehled ostatních důvodů zániku platnosti osvědčení podnikatele | 21 |
| 2.5.5. | Statistické přehledy | 21 |
| 2.6. | BEZPEČNOST INFORMAČNÍCH A KOMUNIKAČNÍCH SYSTÉMŮ A KRYPTOGRAFICKÁ OCHRANA | 23 |
| 2.6.1. | Certifikační a akreditační činnost | 24 |
| 2.6.1.1. | Certifikace a akreditace informačních systémů | 24 |
| 2.6.1.2. | Certifikace kryptografických prostředků | 26 |
| 2.6.1.3. | Certifikace kryptografických pracovišť | 28 |
| 2.6.1.4. | Certifikace stínicích komor | 29 |
| 2.6.2. | Další odborná činnost | 29 |
| 2.6.2.1. | Výroba kryptografického materiálu | 29 |
| 2.6.2.2. | Měření kompromitujícího vyzařování (TEMPEST) | 30 |

2.6.2.2.1. TEMPEST měření elektronických zařízení 30
2.6.2.2.2. Zónové měření, instalační záznamy, obranné prohlídky 30
2.6.2.2.3. Přehled provedených měření 30
2.6.2.3. Schvalování projektů bezpečnosti komunikačních systémů 31
2.6.2.4. Školení pracovníků kryptografické ochrany a zkoušky odborné způsobilosti 31
2.6.3. Problémové oblasti bezpečnosti informačních a komunikačních systémů a kryptografické ochrany 32
2.7. ADMINISTRATIVNÍ A FYZICKÁ BEZPEČNOST, ÚSTŘEDNÍ REGISTR 33
2.7.1. Administrativní bezpečnost 33
2.7.2. Fyzická bezpečnost 33
2.7.2.1. Certifikace technických prostředků 33
2.7.2.2. Posuzování bezpečnostní dokumentace podnikatele z hlediska fyzické bezpečnosti 35
2.7.2.3. Problémové oblasti fyzické bezpečnosti 36
2.7.3. Ústřední registr 37
2.8. KYBERNETICKÁ BEZPEČNOST 39
2.8.1. Budování NCKB/GovCERT.CZ 39
2.8.2. Vývoj legislativy a koncepčních dokumentů 40
2.8.3. Informační systémy důležité pro stát a komunikace se subjekty, které provozují KII a VIS 40
2.8.4. Spolupráce Úřadu v oblasti kybernetické bezpečnosti 41
2.8.5. Zvyšování povědomí a osvěta 43
2.9. VÝKON FUNKCE PŘÍSLUŠNÉHO ORGÁNU PRS 44
2.9.1. Budování národního centra PRS 44
2.9.2. Personální obsazení NCPRS 45
2.9.3. Spolupráce s ostatními subjekty při implementaci služby PRS 46
2.10. OPRAVNÉ PROSTŘEDKY 46
2.10.1. Bezpečnostní řízení 46
2.10.1.1. Statistické přehledy 47
2.10.1.1.1. Rozklady 47
2.10.1.1.2. Žaloby správní 47
2.10.1.1.3. Kasační stížnosti 47
2.10.1.1.4. Ústavní stížnosti 48
2.10.1.1.5. Stížnosti k Evropskému soudu pro lidská práva 48
2.10.1.2. Hodnocení rozhodovací praxe Úřadu 48
2.10.2. Správní řízení o pokutě 48
2.10.3. Řízení podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím 48
2.11. VÝZKUMNÁ A VÝVOJOVÁ ČINNOST ÚŘADU 48
2.11.1. Cíle a organizace výzkumu a vývoje 48
2.11.2. Projekty realizované v roce 2015 49
2.12. STÁTNÍ DOZOR 49
2.12.1. Kontroly provedené v roce 2015 50
2.12.2. Výsledky kontrol 53
2.13. METODICKÁ ČINNOST ÚŘADU 56

| | | |
|---|---|---|
| 2.13.1. | Metodická činnost v oblasti bezpečnostního řízení | 56 |
| 2.14. | VĚSTNÍK ÚŘADU A INTERNETOVÉ STRÁNKY ÚŘADU | 57 |
| 2.14.1. | Věstník Úřadu | 57 |
| 2.14.2. | Internetové stránky Úřadu | 57 |
| 2.15. | POSKYTOVÁNÍ INFORMACÍ PODLE ZÁKONA Č. 106/1999 SB., O SVOBODNÉM PŘÍSTUPU K INFORMACÍM | 58 |
| 2.16. | INSPEKCE ŘEDITELE ÚŘADU | 58 |
| 3. | BEZPEČNOSTNÍ, EKONOMICKÉ A PERSONÁLNÍ ZABEZPEČENÍ ÚŘADU | 59 |
| 3.1. | OCHRANA UTAJOVANÝCH INFORMACÍ A KRIZOVÉ ŘÍZENÍ V ÚŘADU | 59 |
| 3.1.1. | Vnitřní kontrola ochrany utajovaných informací | 59 |
| 3.1.2. | Personální bezpečnost v rámci Úřadu | 59 |
| 3.1.3. | Fyzická bezpečnost v rámci Úřadu | 60 |
| 3.1.4. | Krizové řízení v rámci Úřadu | 60 |
| 3.1.5. | Ostatní činnosti | 60 |
| 3.2. | ARCHIV NÁRODNÍHO BEZPEČNOSTNÍHO ÚŘADU | 61 |
| 3.3. | EKONOMICKÉ ZABEZPEČENÍ ÚŘADU | 61 |
| 3.4. | PERSONÁLNÍ ZABEZPEČENÍ ÚŘADU | 63 |
| Příloha | Seznam některých zkratek a pojmů použitých v textu k oblasti kybernetické bezpečnosti | 66 |