Z P R Á V A

O ČINNOSTI

NÁRODNÍHO BEZPEČNOSTNÍHO ÚŘADU

ZA ROK 2016

Praha 2017

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 2016 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,
- činnosti vykonávané v souvislosti s gescí za oblast kybernetické bezpečnosti, implementace Národní strategie kybernetické bezpečnosti na období let 2015-2020 a návazného Akčního plánu, určování prvků kritické informační infrastruktury (dále jen „KII“) a významných informačních systémů (dále jen „VIS“), provádění kontrol podle zákona o kybernetické bezpečnosti, analýzy kybernetických bezpečnostních incidentů, realizace a účast na cvičeních s tematikou kybernetické bezpečnosti, mezinárodní i vnitrostátní spolupráce, vzdělávání, osvěta, poskytování informací veřejnosti atd.

2. ČINNOST ÚŘADU

2.1. LEGISLATIVNÍ A PRÁVNÍ ČINNOST ÚŘADU

2.1.1. Vnější legislativní činnost

Zákon, byl v roce 2016 třikrát novelizován, a to

- zákonem č. 375/2015 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o ozdravných postupech a řešení krize na finančním trhu a v souvislosti s úpravou systému pojištění vkladů,

- zákonem č. 298/2016 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o službách vytvářejících důvěru pro elektronické transakce, zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, a zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, a

- zákonem č. 135/2016 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o zadávání veřejných zakázek.

Úřad v roce 2016 dále zpracoval novelu vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů, která nabyla účinnosti dne 14. července 2016. Předmětná novela měla za cíl uvést přílohu č. 1 k vyhlášce č. 528/2005 Sb., resp. její bod 4.1., do souladu s novými českými technickými normami. Další vyhláška v gesci Úřadu, která byla novelizována, je vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích. S účinností k 1. červenci 2016 se prostřednictvím novely mění příloha č. 1 k vyhlášce č. 317/2014 Sb. a stanoví nový výčet určených VIS. V roce 2016 též došlo ze strany Úřadu ke zpracování novely vyhlášky č. 363/2011 Sb., o personální bezpečnosti a o bezpečnostní způsobilosti, ve znění pozdějších předpisů, která s účinností k 1. lednu 2017 redukuje výčet písemností přikládaných k žádosti fyzické osoby a k žádosti o doklad, a dále redukuje změny údajů, které je fyzická osoba povinna hlásit Úřadu podle § 66 odst. 1 písm. d) zákona.

Intenzivně se připravuje právní úprava nakládání s utajovanými dokumenty v digitální podobě, 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. Do Plánu legislativních prací vlády pro rok 2017 tak byl pro Úřad zařazen legislativní úkol do února 2017 předložit novelu zákona.

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 zadávání veřejných zakázek nebo atomového zákona.

Úřad v rámci mezirezortního připomínkového řízení dále zpracoval stovky stanovisek k návrhům právních předpisů předkládaných ministerstvy nebo jinými ústředními správními úřady. V průběhu roku 2016 se Úřad rovněž vyjadřoval k materiálům nelegislativní povahy a k návrhům mezinárodních smluv.

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 informačních systémů v Unii (směrnice NIS). Tato směrnice byla velmi intenzivně projednávána již od roku 2013, přičemž Úřad po dobu celého projednávání zastával pozici jejího gestora na národní úrovni a aktivně se zapojoval do jejího projednávání na půdě evropských institucí. Dne 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). V roce 2016 dále probíhaly legislativně-technické korektury, přičemž podepsání směrnice předsedou Evropského parlamentu a předsedou Rady EU proběhlo dne 6. července 2016. Směrnice pak byla vyhlášena v Úředním věstníku Evropské unie 19. července 2016, platnosti nabyla 8. srpna 2016 a její transpoziční lhůta činí 21 měsíců ode dne nabytí platnosti, tj. do 9. května 2018.

S ohledem na výše uvedené skutečnosti započaly na přelomu března a dubna roku 2016 práce na transpoziční novele zákona o kybernetické bezpečnosti, která doplňuje zákon o kybernetické bezpečnosti o další náležitosti stanovené směrnicí NIS. Jedná se zejména o rozšíření povinných subjektů podle tohoto zákona, a to o provozovatele základních služeb a poskytovatele digitálních služeb. Tento návrh zákona byl v prosinci 2016 postoupen do Poslanecké sněmovny Parlamentu ČR, přičemž jeho projednávání bude pokračovat i v roce 2017. V souvislosti s tím zahájil Úřad na podzim roku 2016 i práce na vyhlášce, kterou budou stanovena kritéria pro určování provozovatelů základních služeb.

2.1.3. Vnitřní legislativní činnost

V průběhu roku 2016 bylo vydáno celkem 39 nových interních aktů řízení ředitele Úřadu. Konkrétně se jednalo o 16 směrnic a 23 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. Oproti roku 2015 bylo vydáno o 3 interní akty řízení více, přičemž lze konstatovat, že i nadále pokračuje trend vydávání vyššího počtu interních aktů řízení oproti předchozím letům, neboť si to vyžaduje aplikační praxe.

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

Úřad již pátým 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 oznámením veřejných zadavatelů podle § 69 odst. 1 písm. r) zákona. Tato činnost spočívá v posuzování oznámení učiněných veřejnými zadavateli z hlediska ochrany utajovaných informací. V souvislosti s nově přijatým zákonem č. 134/2016 Sb., o zadávání veřejných zakázek, došlo prostřednictvím zákona č. 135/2016 Sb. k novele zákona, přičemž došlo k úpravě okruhu veřejných zakázek, které je zadavatel povinen podle § 69 odst. 1 písm. r) zákona neprodleně písemně oznamovat Úřadu. Konkrétně se oznamuje skutečnost, že zadavatel bude zadávat veřejnou zakázku mimo zadávací řízení z důvodu ochrany utajovaných informací, nebo že v zadávacím řízení stanoví opatření k zajištění ochrany utajované informace stupně utajení Důvěrné a vyšší. Dále zadavatel oznamuje stanovení požadavku na profesní způsobilost v zadávacím řízení spočívající v předložení dokladu prokazujícího schopnost dodavatele zabezpečit ochranu utajovaných informací stupně utajení Důvěrné nebo vyšší nebo oprávnění ke vstupu osob dodavatele do zabezpečené oblasti kategorie Důvěrné nebo vyšší anebo jednací oblasti podle tohoto zákona, nebo stanovení podmínky na uzavření smlouvy v zadávacím řízení spočívající v předložení dokladu prokazujícího schopnost dodavatele zabezpečit ochranu utajovaných informací stupně utajení Důvěrné nebo vyšší.

V roce 2016 se Úřad vyjádřil k 96 podaným oznámením, tj. o 21 více než v roce 2015. Největší podíl na oznámeních mělo Ministerstvo obrany, celkem 52 oznámení, a v pořadí druhé Ministerstvo vnitra podalo oznámení 20.

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 2016 bylo pro porušení povinností stanovených zákonem ukončeno celkem 34 správních řízení, z toho ve 14 případech s fyzickými osobami a ve 20 případech s právnickými

osobami, ve všech případech byla uložena sankce (ve 33 případech peněžitá pokuta, v 1 případě napomenutí). V 5 dalších případech nebylo správní řízení dosud ukončeno. Celková výše uložených pokut dosáhla částky 161 000 Kč. Dále v celkem 9 případech nebyla řízení prozatím zahájena, neboť jsou Úřadem činěny patřičné kroky v rámci přípravného řízení.

V roce 2016 došlo k zastavení řízení pouze v jediném případě. Ve 28 dalších případech byla věc odložena nebo správní řízení nebylo zahájeno (v 16 případech u fyzických osob, ve 12 případech u právnických osob). V 10 případech byla věc z důvodu nepříslušnosti postoupena k projednání příslušnému služebnímu funkcionáři.

Správní řízení v roce 2016

	Fyzická osoba	Právnická osoba	Celkem
Ukončená správní řízení	14	20	**34**
Počet uložených sankcí	14	20	**34**
Zastavená správní řízení	1	0	**1**
Dosud neukončená správní řízení	2	3	**5**

V souvislosti s nabytím účinnosti nového zákona č. 134/2016 Sb., o zadávání veřejných zakázek, připravilo právní oddělení, které v rámci Úřadu agendu zadávání veřejných zakázek zabezpečuje, novou směrnici ředitele Úřadu č. 9/2016, o zadávání veřejných zakázek v Národním bezpečnostním úřadu, která upravuje postup Úřadu v oblasti zadávání veřejných zakázek. 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. 134/2016 Sb., o zadávání veřejných zakázek. Převážnou většinu veřejných zakázek zadávaných Úřadem v roce 2016 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 vyjadřuje prostřednictvím schvalovacího nástroje v elektronickém tržišti. Zakázky s předpokládanou hodnotou nad 500 000 Kč bez DPH je možné v rámci Úřadu zadat pouze po kladném vyjádření odboru právního a legislativního, vydaném na základě žádosti věcně příslušného organizačního celku. V případě podlimitních a nadlimitních veřejných zakázek pak odbor právní a legislativní přímo vede zadávací řízení.

V oblasti právní činnosti bylo v roce 2016 dále uzavřeno 95 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.

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 2016

V roce 2016 byly vyvíjeny následující aktivity v rámci sjednávání mezinárodních smluv:

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

  V roce 2016 proběhlo první jednání o smlouvě s tureckou stranou.

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

  Expertní jednání probíhala i v roce 2016, avšak doposud se nepodařilo dosáhnout shody nad textem smlouvy.

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

  Obě strany si vyměnily návrhy na sjednání smlouvy, text smlouvy byl dohodnut korespondenčně, nicméně obě strany se dohodly na uskutečnění expertního jednání v roce 2017.

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

  V roce 2016 proběhlo na základě iniciativy korejské strany první kolo expertních jednání.

2.2.1.2. Výhled na rok 2017

V roce 2017 Úřad předpokládá dokončení expertních jednání u výše uvedených smluv. Vzhledem k nečinnosti partnerských úřadů se nedá předpokládat dokončení jednání o smlouvách s Belgií, Nizozemskem, Irákem, USA a Velkou Británií. Naopak se očekává zahájení jednání s Jordánským 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).

2.2.3. Mezinárodní aktivity v oblasti kybernetické bezpečnosti

Mezinárodní spolupráce představovala v roce 2016 jeden z hlavních pilířů zajišťování kybernetické bezpečnosti státu. Na poli mezinárodních organizací jsou pro ČR tradičními partnery NATO a EU. V příštím roce by se mohl seznam organizací a fór, kterých se ČR účastní, opět rozrůst. Národní centrum kybernetické bezpečnosti (dále jen „NCKB“) aktivně zkoumá příležitosti zapojení se například do Global Forum on Cyber Expertise, kde dochází ke sdílení know-how a osvědčených postupů při budování kybernetických kapacit. V oblasti mezinárodní spolupráce vedle Úřadu působí i další rezorty, zejména Ministerstvo obrany, Ministerstvo zahraničních věcí či Ministerstvo průmyslu a obchodu.

Nejvýraznějším počinem v oblasti kybernetické bezpečnosti na evropské úrovni v roce 2016 bylo bezesporu přijetí směrnice Evropského parlamentu a Rady EU č. 2016/1148, o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (směrnice NIS). Návrh předložený Evropskou komisí v roce 2013 doznal v průběhu vyjednávání značných změn, zejména v otázce rozsahu dopadu této regulace.

Dalším významným fórem pro kybernetickou bezpečnost na půdě EU byla i v roce 2016 pro ČR skupina přátel předsednictví pro kybernetické otázky (Friends of Presidency on Cyber Issues), která se pravidelně schází od roku 2013. V uplynulém roce byl na její půdě draftován Diplomatic Toolbox formulující možné diplomatické nástroje, které mají členské státy k dispozici při řešení závažných kybernetických útoků. S nástupem slovenského předsednictví se pak pozornost přenesla zejména na navyšování kybernetické odolnosti a kybernetických kapacit.

Úřad je zastoupen i v Evropské agentuře pro bezpečnost sítí a informací (ENISA) prostřednictvím účasti na formálních a neformálních jednáních. ENISA i v roce 2016 pokračovala v poskytování poradenství Evropské komisi a členským státům EU při tvorbě a implementaci politik týkajících se kybernetické bezpečnosti, koordinovala opatření vydávaná pro zabezpečení jejich sítí a informačních systémů a prostřednictvím kurzů a školení podporovala budování kapacit CERT

v jednotlivých členských státech. Zaměřila se přitom zejména na témata a výzvy související s nově přijatou evropskou směrnicí NIS.

Nejvýznamnější události v NATO v oblasti kybernetické bezpečnosti se stal varšavský summit, během něhož uznali nejvyšší představitelé členských států kybernetický prostor jako další operační doménu. Během summitu byl přijat také Cyber Defence Pledge, na jehož finální podobě se podílelo i NCKB. Státy se v tomto dokumentu zavázaly budovat a posilovat bezpečnost národních sítí a informační infrastruktury a navýšit tak svou i alianční odolnost proti kybernetickým útokům. V návaznosti na Cyber Defence Pledge schválila Severoatlantická rada metriku, jejímž cílem je zhodnotit, zda spojenci skutečně navyšují své kybernetické schopnosti tak, jak se na summitu zavázali. Za ČR bude hodnocení zpracovávat Úřad spolu s Ministerstvem obrany. První zprávu o stavu českých kybernetických schopností by měly členské státy NATO odevzdat v únoru 2017.

ČR se již třetím rokem také aktivně podílela na činnosti NATO Cooperative Cyber Defence Centre of Excellence (CCDCoE), které se zaměřuje na výzkumnou a vědeckou činnost v oblasti kybernetické bezpečnosti a obrany. ČR je členem Řídícího výboru (Steering Committee) centra. Do jeho právní divize byl počátkem roku 2014 vyslán pracovník Úřadu a na základě jeho pracovních výsledků požádalo vedení centra o prodloužení jeho vyslání o další rok.

V roce 2016 se Úřad coby národní gestor kybernetické bezpečnosti zapojil do činnosti mezirezortní pracovní skupiny Ministerstva zahraničních věcí pro spolupráci ČR s Organizací pro ekonomickou spolupráci a rozvoj (OECD). Problematika kybernetické bezpečnosti má důležité místo i v ekonomickém rozvoji, na který se tato organizace zaměřuje; odráží se např. v instrumentech týkajících se řízení digitálních bezpečnostních rizik, rozvoje digitální ekonomiky nebo ochrany práv spotřebitele, které OECD přijala v letech 2015-2016.

V roce 2016 došlo k významnému prohloubení vztahů se Spojenými státy americkými a Izraelem, v nichž začali působit čeští cyber attachés. Spolupráce byla posílena i s dalšími zahraničními partnery, ke kterým patří Korejská republika či Singapur.

Působení kybernetického odborníka v Tel Avivu bylo v roce 2016 primárně zaměřeno na vybudování povědomí mezi hlavními izraelskými hráči v oblasti kybernetické bezpečnosti o procesu implementace zákona o kybernetické bezpečnosti v ČR.

Vedle vyslání cyber attaché bylo významnou událostí v česko-izraelských vztazích podepsání Memoranda o porozumění. Memorandum, které bylo podepsáno během květnového jednání vlád (G2G), vytvoří užší rámec spolupráce mezi Úřadem a izraelským Národním úřadem pro kybernetickou bezpečnost (NCSA – National Cyber Security Authority). V návazosti na závěry jednání G2G proběhla v polovině prosince v prostorách Ministerstva zahraničních věcí prezentace izraelských a českých firem v oblasti kybernetické bezpečnosti. Na organizaci semináře se za českou stranu se podílel Svaz průmyslu a dopravy, Ministerstvo obrany a Česko-izraelská smíšená obchodní komora. Hlavním cílem semináře byla výměna zkušeností na vládní úrovni při ochraně kritické infrastruktury a setkání českých a izraelských firem vyvíjejících řešení pro ochranu před kybernetickými hrozbami.

Strategická spolupráce byla prohloubena i se Spojenými státy americkými. Vyslání českého cyber attaché na zastupitelský úřad ve Washingtonu, D.C., vedlo k navázání kontaktů s představiteli několika amerických státních institucí, mezi něž patřila ministerstva vnitřní bezpečnosti a zahraničí. Komunikace byla zahájena i se zástupci ministerstva energetiky a jeho podřízeného pracoviště Idaho National Laboratory, které se specializuje na výzkum a vývoj ochrany kritické informační infrastruktury nejen v oblasti jaderné energetiky. V rámci spolupráce Úřadu a americké FBI se vedoucí pracovník NCKB účastnil dvouměsíční stáže v National Cyber-Forensics and Training Alliance (NCFTA). Hlavním cílem stáže, na kterou byli vysláni zástupci států z celého světa, bylo navázat

spolupráci při sdílení informací o kybernetických incidentech a o probíhajících vyšetřováních kybernetických zločinů.

V rámci naplňování strategického partnerství ČR s Korejskou republikou, uzavřeného v roce 2015 proběhly v červnu 2016 první bilaterální konzultace o otázkách kybernetické bezpečnosti. Za českou stranu na jejich přípravě spolupracoval Úřad s Ministerstvem zahraničních věcí, Ministerstvem průmyslu a obchodu, Ministerstvem obrany a Ministerstvem vnitra.

Úřad dále v roce 2016 pokračoval v poskytování asistence státům, které budují svůj systém kybernetické bezpečnosti. Tento rok se Úřad v rámci 2 evropských projektů zaměřil na balkánské státy. V rámci pokračujícího projektu Enhancing Cyber Security český zástupce spoluorganizoval workshop pro členy makedonských, kosovských a moldavských CERT/CSIRT týmů, který se konal v Kišiněvě. Hlavním cílem bylo předat zkušenosti s budováním obdobného pracoviště v ČR. Workshop byl rozdělen do 2 částí – technické a teoretické. Obě vedle přednášek obsahovaly i cvičení, během nichž měli účastníci za úkol řešit bezpečnostní incidenty.

Úřad se v roce 2016 účastnil řady mezinárodních cvičení. Jednalo se zejména o:

- cvičení orgánů krizového řízení NATO CMX 2016,
- 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 2016 Úřad uspořádal 2 cvičení připravená na míru pro zahraničního partnera. Akce se skládala ze specializovaného školení a návazného strategického table-top cvičení reflektujícího aktuální dění ve světě. První cvičení proběhlo v červnu na zastupitelském úřadu ČR ve Washingtonu, D.C. Cvičení bylo zorganizováno za pomoci zde vyslaného cyber attaché. Druhé cvičení se uskutečnilo na Velitelství pro transformaci NATO ACT v Norfolku. Účastníky cvičení zde byli civilní a vojenští činitelé z různých divizí mezinárodního sekretariátu. Na základě hodnocení účastníků doporučilo NATO ACT, aby se cvičení připravené NCKB zařadilo do celoaliančních NATO cvičení.

2.3. PERSONÁLNÍ BEZPEČNOST

V oblasti personální bezpečnosti Úřad v roce 2016 prováděl zejména bezpečnostní řízení o vydání osvědčení fyzické osoby, v jejichž závěru vydával osvědčení fyzické osoby nebo rozhodnutí o nevydání osvědčení fyzické osoby. Dále Úřad přijímal žádosti o vydání osvědčení fyzické osoby pro cizí moc a při splnění zákonem stanovených podmínek vydával osvědčení fyzické osoby pro cizí moc, potvrzující cizí moci provedení bezpečnostního řízení u této osoby a vydání 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 jeho vydání. V této souvislosti Úřad vedl řízení o zrušení platnosti osvědčení fyzické osoby a v případech, kdy fyzická osoba přestala splňovat podmínky pro jeho vydání, 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 2016 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 nová dohoda o postupu při poskytování informací mezi Národním bezpečnostním úřadem, Ministerstvem obrany – Odborem bezpečnosti, Ministerstvem obrany – Sekcí dozoru a kontroly, Ministerstvem obrany – Hlavním velitelstvím Vojenské policie a Ministerstvem obrany – Agenturou personalistiky.

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 235 osobám a na základě jejich žádostí prováděl šetření k 63 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 5 739 žádostí o vydání osvědčení fyzické osoby, to je o 497 žádostí méně než v předchozím roce.

Největší podíl tvořily žádosti o vydání osvědčení fyzické osoby pro stupeň utajení Tajné (53 %) a pro stupeň utajení Důvěrné (43 %). Nejvíce žádostí bylo podáno v měsíci červnu, a to v počtu 666 žádostí. Velký objem žádostí byl podán rovněž koncem roku v měsících listopadu a prosinci, kdy bylo podáno po 580 žádostech (viz graf Celkové počty přijatých žádostí v jednotlivých měsících roku 2016).

Celkem bylo v loňském roce rozhodnuto v 5 487 případech o vydání osvědčení fyzické osoby a v 16 případech o nevydání osvědčení. Ve 137 případech bylo bezpečnostní řízení zastaveno. Nejčastějším důvodem zastavení bezpečnostního řízení bylo zpětvzetí žádosti účastníkem řízení (57 případů). Ve 33 případech bylo bezpečnostní řízení zastaveno, protože účastník řízení ve stanovené lhůtě neodstranil nedostatky v žádosti fyzické osoby nebo v rozkladu. Významný podíl na zastavení bezpečnostního řízení měla také povinnost odpovědné osoby neprodleně oznámit Úřadu pominutí skutečností odůvodňujících nutnost přístupu fyzické osoby k utajovaným informacím (30 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 3 996 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 by držitel

osvědčení fyzické osoby 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 111 případech toto prověřování vyústilo v zahájení řízení o zrušení platnosti osvědčení fyzické osoby, které bylo v 18 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

V loňském roce Úřad rozhodl o nevydání osvědčení fyzické osoby v 16 případech a v 18 případech platnost osvědčení fyzické osoby zrušil.

Většina z výše uvedeného počtu rozhodnutí byla vydána z důvodu 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.

Jednání, kterými žadatelé a držitelé osvědčení skutkovou podstatu tohoto bezpečnostního rizika naplnili, byla různorodá, nicméně i v roce 2016 se jednalo zejména o neodpovědné nakládání s vlastními finančními prostředky a z toho plynoucí neschopnost dostát svým finančním závazkům.

Z fakultativních bezpečnostních rizik se na důvodech shledání bezpečnostně nespolehlivým v roce 2016 dále významněji podílelo bezpečnostní riziko podle § 14 odst. 3 písm. g) zákona, tedy uvedení nepravdivé informace nebo zamlčení informace rozhodné pro objektivní zjištění skutečného stavu věci v řízení podle části čtvrté, kdy takto byly zejména zamlčovány informace k finanční situaci. V případě držitelů osvědčení fyzické osoby, jejichž platnost v loňském roce Úřad zrušil, se rovněž více objevovalo bezpečnostní riziko podle 14 odst. 3 písm. i) zákona, tedy opakované neposkytnutí nezbytné součinnosti při bezpečnostním řízení zahájeném podle § 101 odst. 1 zákona.

V loňském roce byla v několika případech rovněž konstatována přítomnost obligatorních bezpečnostních rizik, a to zejména bezpečnostního rizika podle § 14 odst. 2 písm. b) zákona, tedy činnost spočívající v potlačování základních lidských práv a svobod, která byla převážně shledána ve formě pravicového extremismu.

Ostatní rizika uvedená v § 14 odst. 2 a 3 zákona byla konstatována v roce 2016 ojediněle.

V loňském roce byl zaznamenán významný pokles počtu rozhodnutí o zrušení platnosti osvědčení z důvodu nesplnění podmínky podle § 12 odst. 1 písm. b) zákona ve spojení s § 6 odst. 2 písm. c) zákona, tedy nesplnění podmínky bezúhonnosti.

2.3.4. Přehled ostatních důvodů zániku platnosti osvědčení fyzické osoby

V uplynulém období zanikla platnost celkem 7 943 osvědčení, přičemž největší část případů představoval zánik uplynutím doby platnosti osvědčení, a to v celkovém počtu 3 681 osvědčení a zánik platnosti doručením nového osvědčení fyzické osoby v celkovém počtu 3 265 osvědčení. 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 (671 případů).

Z výše uvedeného je zřejmé, že se stále pozitivně projevují dva z principů novelizace zákona z roku 2011, 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. Uplatnění těchto ustanovení v praxi snižuje počet vydaných osvědčení, a tím i administrativní zátěž Úřadu.

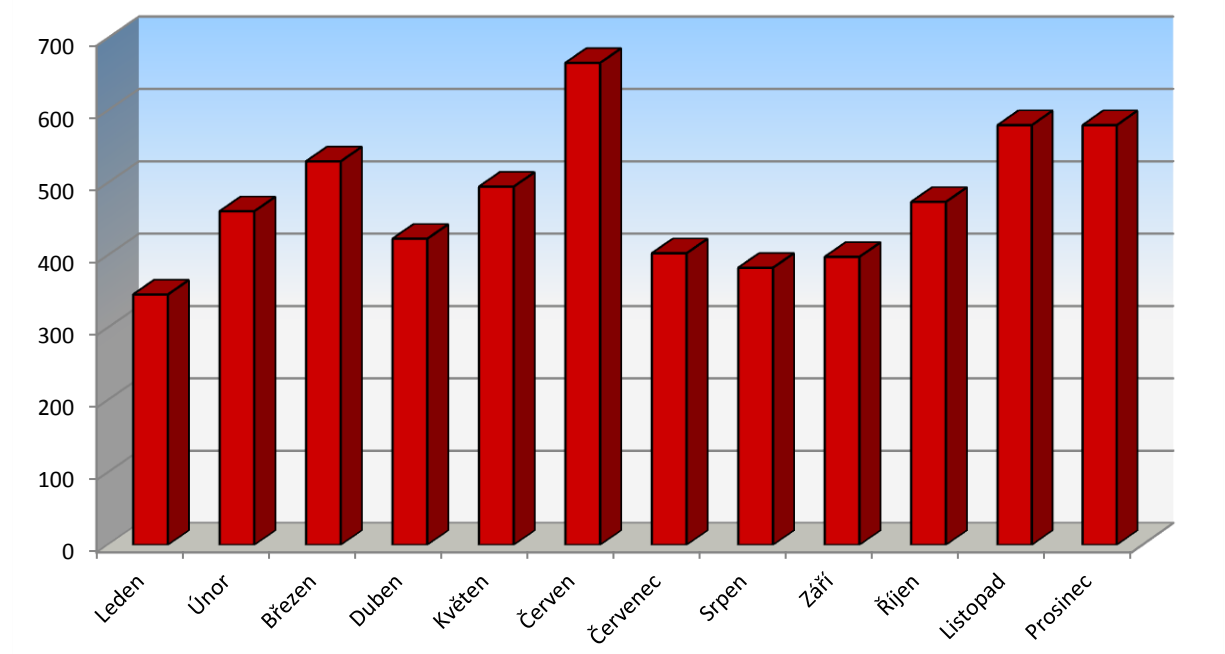
Počet případů zániku platnosti osvědčení fyzické osoby v roce 2016 podle jednotlivých důvodů je přehledně uveden v následující kapitole 2.3.5.

2.3.5. Statistické přehledy

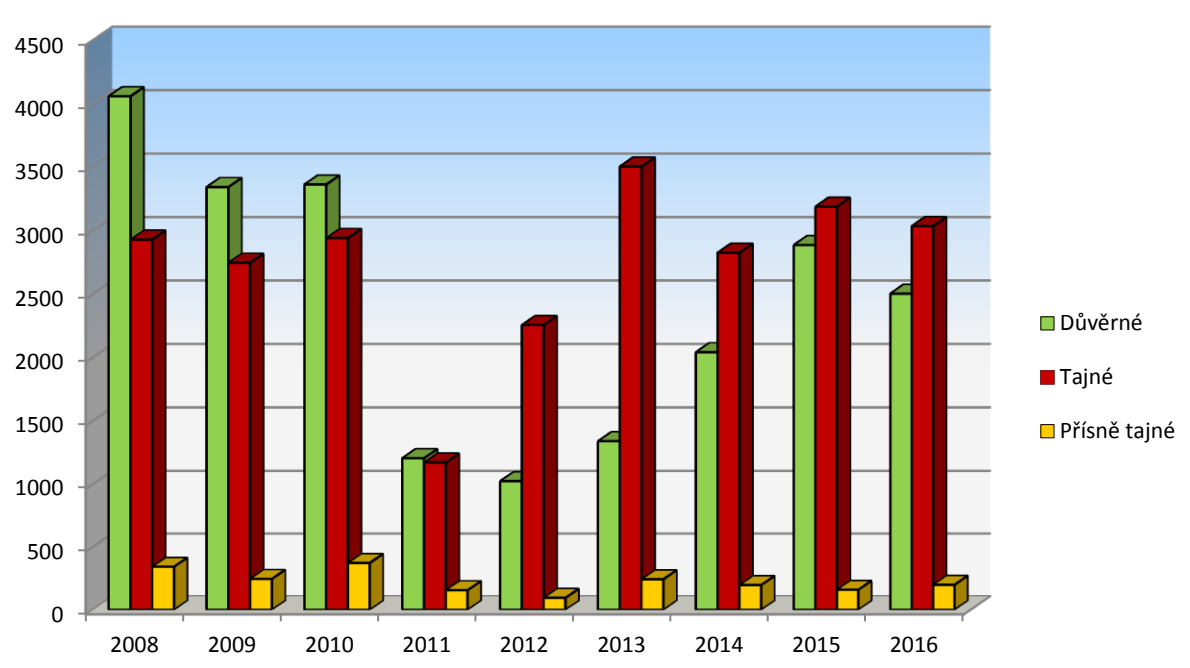
Přijaté žádosti a ukončená bezpečnostní řízení v roce 2016

	Důvěrné	Tajné	Přísně tajné	Celkem
Přijaté žádosti	2 504	3 036	199	**5 739**
Osvědčení vydáno	2 367	2 946	174	**5 487**
Osvědčení nevydáno	3	13	0	**16**
Řízení zastaveno	78	55	4	**137**

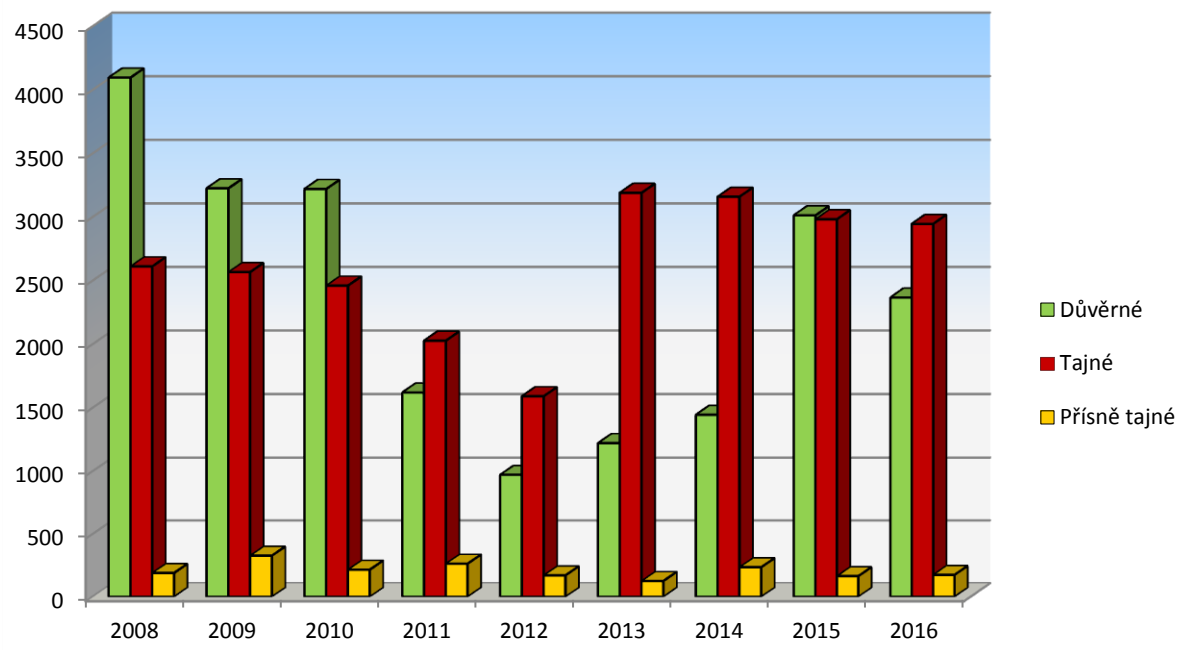
Celkové počty přijatých žádostí v jednotlivých měsících roku 2016



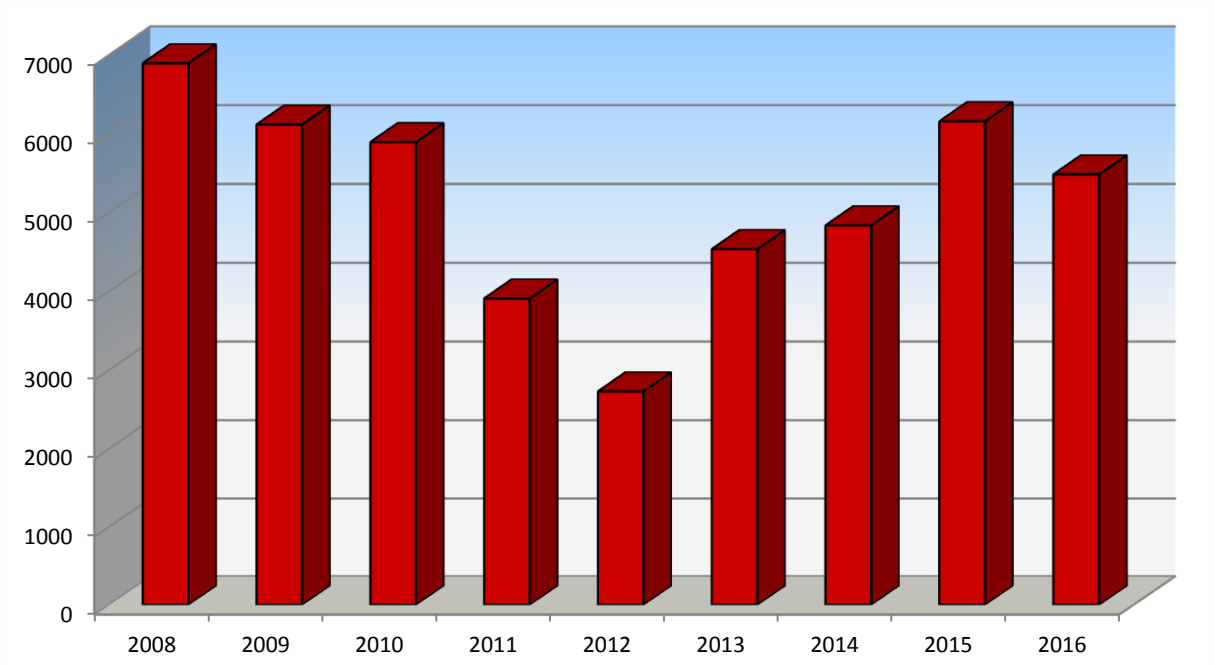
Přijaté žádosti o vydání osvědčení fyzické osoby v letech 2008 až 2016



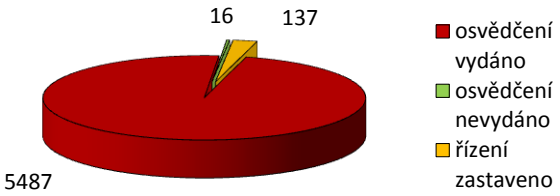
Vydaná osvědčení fyzické osoby v letech 2008 až 2016



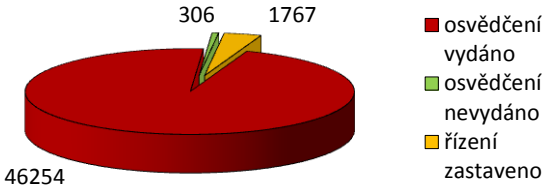
Vydaná osvědčení fyzické osoby v letech 2008 až 2016 celkem



Ukončená bezpečnostní řízení v roce 2016



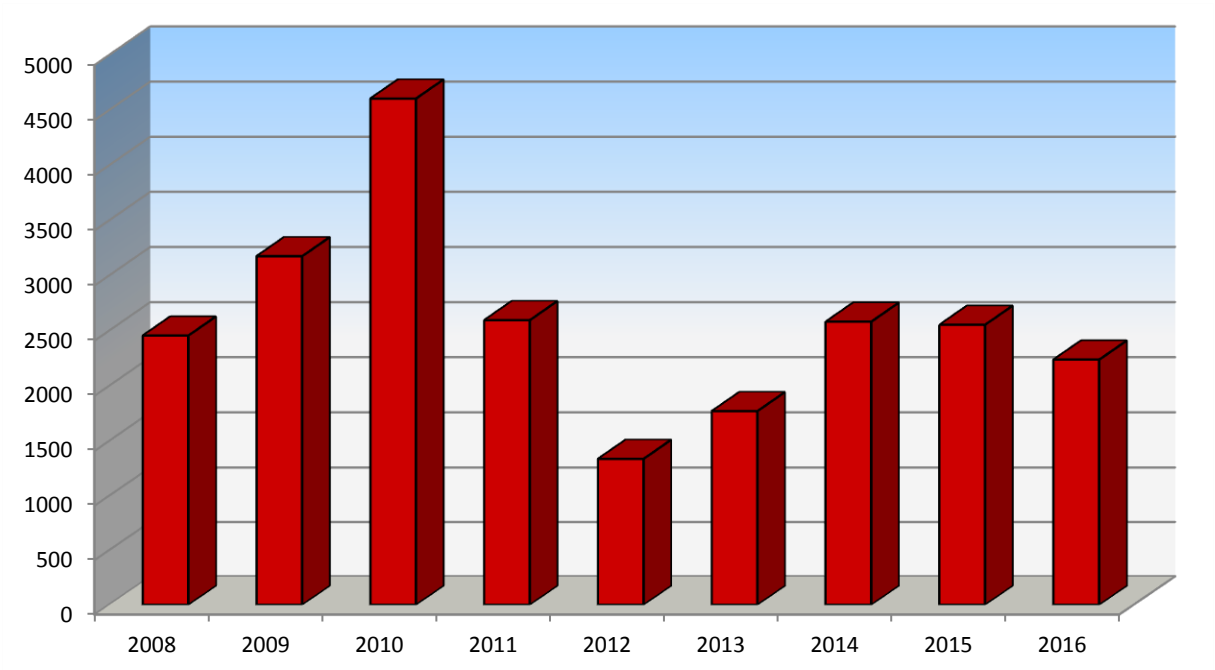
Ukončená bezpečnostní řízení v letech 2008 až 2016



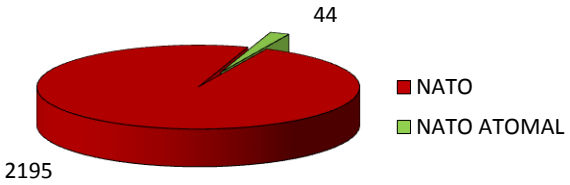
Vydaná osvědčení fyzické osoby pro cizí moc v roce 2016

COSMIC TOP SECRET	253
COSMIC TOP SECRET ATOMAL	31
NATO SECRET	1 771
NATO SECRET ATOMAL	13
NATO CONFIDENTIAL	171
Celkem	**2 239**

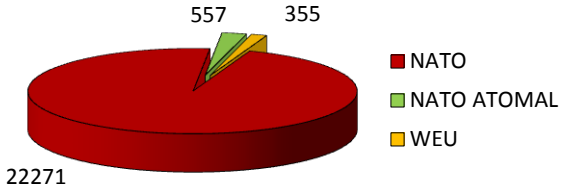
Vydaná osvědčení fyzické osoby pro cizí moc v letech 2008 až 2016 celkem



Osvědčení pro cizí moc v roce 2016



Osvědčení pro cizí moc v letech 2008 až 2016[1)]



Zánik platnosti osvědčení fyzické osoby podle důvodu v roce 2016

Uplynutí doby platnosti osvědčení	3 681
Zrušení platnosti osvědčení	18
Úmrtí držitele osvědčení	21
Ohlášení odcizení nebo ztráty osvědčení	33
Poškození osvědčení	9
Změna některého z údajů uvedených v osvědčení	187
Vrácení osvědčení	671
Doručení nového osvědčení	3 265
Vznik služebního nebo pracovního poměru u zpravodajské služby	58
Celkem	**7 943**

[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.

Zastavení bezpečnostního řízení v roce 2016

Nedání souhlasu podle § 107 zákona	6
Neodstranění nedostatků v žádosti ve stanovené lhůtě	33
Uvedení nepravdivé nebo neúplné výpovědi	6
Nesplnění podmínek – dosažení 18 let věku, svéprávnosti, bezúhonnosti	2
Opakované nedostavení se k pohovoru	1
Úmrtí žadatele	2
Oznámení odpovědné osoby, že pominuly skutečnosti, kterými byla žádost odůvodněna	30
Zpětvzetí žádosti	57
Celkem	**137**

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 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 2016 bylo vyjádření Úřadu k personálním projektům předloženo do připomínkového řízení dotčeným ministerstvům a orgánům státní správy. Největší počet žádostí na rok 2017 je plánován rezortem Ministerstva obrany (3 830 žádostí) a Ministerstva vnitra (1 126 žádostí).

Na základě předložených personálních projektů a vypořádání vznesených připomínek zpracoval Úřad materiál pro jednání vlády, který vláda ČR projednala dne 16. listopadu 2016 a vydala usnesení č. 1004, kterým schválila předložené personální projekty. Tímto usnesením zároveň uložila členům vlády 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 člena vlády nebo vedoucího ústředního správního úřadu metodickou podporu při plnění uvedených úkolů.

2.4. BEZPEČNOSTNÍ ZPŮSOBILOST

V roce 2016 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 2016 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.

Dne 1. října 2015 nabyl účinnosti nový zákon č. 134/2016 Sb., o zadávání veřejných zakázek, který v § 220 nově definuje citlivé činnosti v této oblasti.

2.4.1. Statistické přehledy

Přehled přijatých žádostí a ukončených bezpečnostních řízení v roce 2016

Citlivá činnost podle	Přijaté žádosti	Doklad vydán	Doklad nevydán	Řízení zastaveno	Zrušení platnosti dokladu
§ 8 zákona č. 38/1994 Sb.[2)]	88	77	0	8	0
§ 2a zákona č. 18/1997 Sb.[3)]	71	65	0	5	0
§ 25c odst. 10 zákona č. 61/1988 Sb.[4)]	1	2	0	0	0
§ 157a zákona č. 137/2006 Sb.[5)]	3	2	0	0	0
§ 2a zákona č. 312/2006 Sb.[6)]	2	4	0	0	0
Ostatní	1	1	0	0	0
Celkem	**166**	**151**	**0**	**13**	**0**

[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. 61/1988 Sb., o hornické činnosti, výbušninách a o státní báňské správě, ve znění pozdějších předpisů.
[5)] Zákon č. 137/2006 Sb., o veřejných zakázkách, ve znění pozdějších předpisů.
[6)] Zákon č. 312/2006 Sb., o insolvenčních správcích, ve znění pozdějších předpisů.

2.5. PRŮMYSLOVÁ BEZPEČNOST

Mezi hlavní činnosti, které Úřad realizoval v oblasti průmyslové bezpečnosti v roce 2016, 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 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 2016 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 2016 bylo Úřadem přijato 96 žádostí podnikatelů o vydání osvědčení podnikatele. Z tohoto počtu bylo k 31. prosinci 2016 rozhodnuto o 53 žádostech, u zbylých 43 žádostí k tomuto datu bezpečnostní řízení o žádosti podnikatele probíhala.

Ve srovnání s rokem 2015 došlo k nárůstu počtu přijatých žádostí, a to celkem o 15 žádosti. Z hlediska struktury podaných žádostí v roce 2016 převažovaly žádosti podnikatelů o vydání osvědčení podnikatele podané podle § 96 odst. 4 zákona, tj. podané podnikateli, kteří i po uplynutí doby platnosti dosavadního osvědčení mají mít přístup k utajovaným informacím. Počty zahájených bezpečnostních řízení reflektují změnu právních předpisů účinnou od 1. ledna 2012, na jejímž základě bylo zrušeno bezpečnostní řízení pro přístup podnikatele k utajované informaci stupně utajení Vyhrazené. Z pohledu počtů žádostí podaných po 1. lednu 2012 však lze vypozorovat trend každoročního zvyšování počtů podaných žádostí o vydání osvědčení podnikatele.

2.5.2. Prověřování splňování podmínek po vydání osvědčení podnikatele

V roce 2016 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 v 16 případech zahájeno řízení o zrušení platnosti osvědčení podnikatele, které bylo v 5 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 2016 rozhodl Úřad ve 3 bezpečnostních řízeních vedených o žádosti podnikatele o nevydání osvědčení podnikatele. Z hlediska struktury spočíval důvod nevydání v nesplnění podmínky podle § 16 odst. 1 písm. b) zákona.

Za totéž období Úřad rozhodl v 5 případech o zrušení platnosti osvědčení podnikatele. Důvodem pro zrušení platnosti osvědčení bylo ve 4 případech nesplnění podmínky bezpečnostní spolehlivosti podle § 16 odst. 1 písm. b) zákona, v 1 případě 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 2016 převažoval mezi důvody zániku platnosti osvědčení podnikatele zánik platnosti osvědčení podnikatele z důvodu doručení nového osvědčení podnikatele pro stejnou formu přístupu podnikatele k utajované informaci, celkem 34 případů. Druhým nejčastějším důvodem zániku platnosti osvědčení podnikatele pak byl zánik osvědčení podnikatele uplynutím doby jeho platnosti, celkem 18 případů. Dalším významným důvodem pak byl zánik platnosti osvědčení podnikatele jeho vrácením držitelem, celkem 16 případů.

Počet případů zániku platnosti osvědčení podnikatele v roce 2016 podle jednotlivých důvodů je uveden v kapitole 2.5.5.

2.5.5. Statistické přehledy

Přijaté žádosti o vydání osvědčení podnikatele v roce 2016

Důvěrné	Tajné	Přísně tajné	Celkem
66	29	1	**96**

Stav zpracování žádostí o vydání osvědčení podnikatele přijatých v roce 2016

Osvědčení vydáno	Osvědčení nevydáno	Řízení zastaveno	Probíhalo k 31. 12. 2016	Celkem
45	1	7	43	**96**

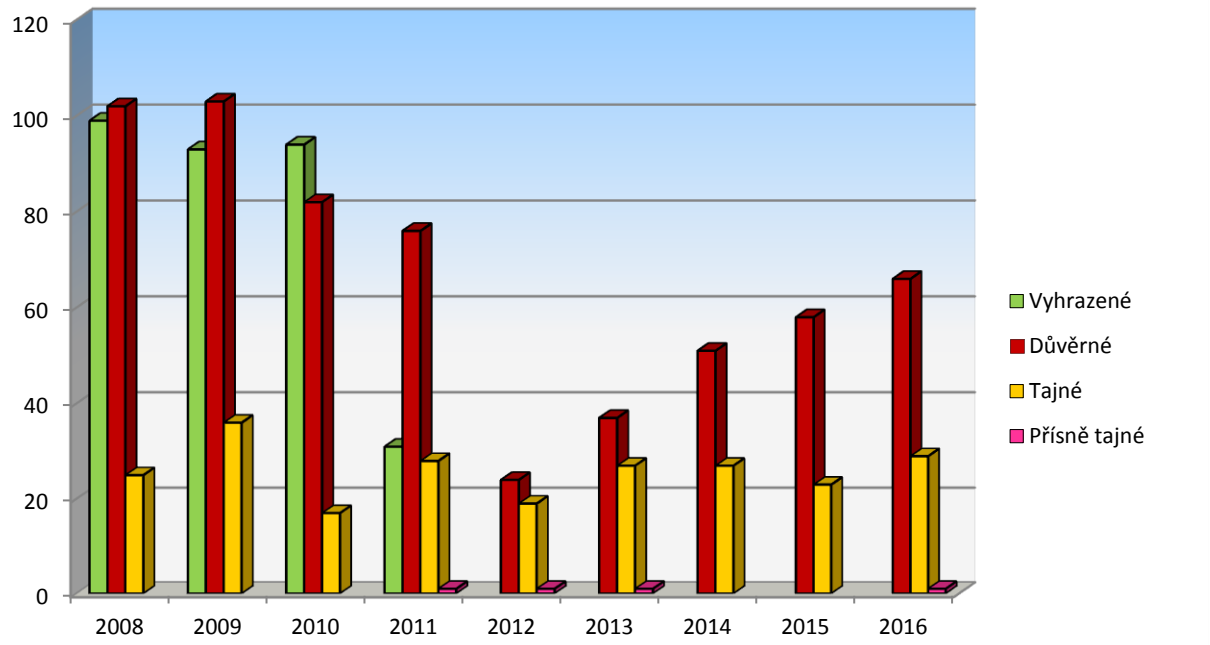
Vydaná osvědčení podnikatele v roce 2016

Důvěrné	Tajné	Přísně tajné	Celkem
79	39	0	**118**[7)]

Řízení o zrušení platnosti osvědčení podnikatele v roce 2016

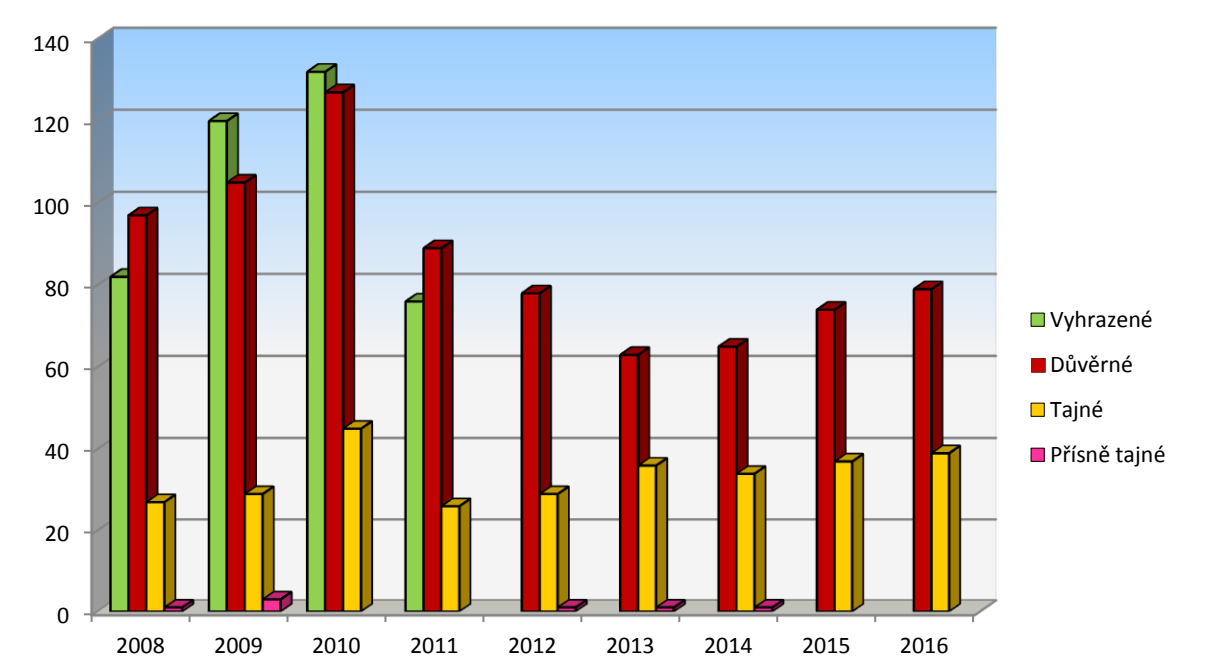
Zahájená řízení	Platnost zrušena	Řízení zastaveno	Probíhalo k 31. 12. 2016
16	5	15	14

Přijaté žádosti o vydání osvědčení podnikatele v letech 2008 až 2016



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

Vydaná osvědčení podnikatele v letech 2008 až 2016



Zánik platnosti osvědčení podnikatele podle důvodu v roce 2016

Uplynutí doby platnosti osvědčení	18
Zrušení platnosti osvědčení	5
Zrušení podnikatele	1
Ohlášení odcizení nebo ztráty osvědčení	3[8)]
Poškození osvědčení	0[8)]
Změna některého z údajů uvedených v osvědčení	1[8)]
Vrácení osvědčení	16
Doručení nového osvědčení pro stejnou formu přístupu k UI	34
Doručení rozhodnutí o nevydání osvědčení pro stejnou formu přístupu k UI	1
Celkem	**79**

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

[8)] 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.

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.

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

V roce 2016 probíhalo řízení o certifikaci 157 informačních systémů. K 51 žádostem o certifikaci informačního systému, jejichž zpracování bylo zahájeno v přechozím roce, přibylo v roce 2016 dalších 106 žádostí, a to 43 ze státní správy nebo samosprávy a 63 ze soukromé sféry. Ve většině případů se jednalo o žádosti o opakovanou certifikaci již provozovaných informačních systémů. Ve 14 případech byla podána žádost o certifikaci nově budovaného informačního systému, přičemž pouze 2 z těchto žádostí pocházejí ze státní správy.

V uvedeném roce bylo vydáno celkem 121 certifikátů informačních systémů, z toho 54 pro žadatele ze státní správy nebo samosprávy a 67 ze soukromé sféry.

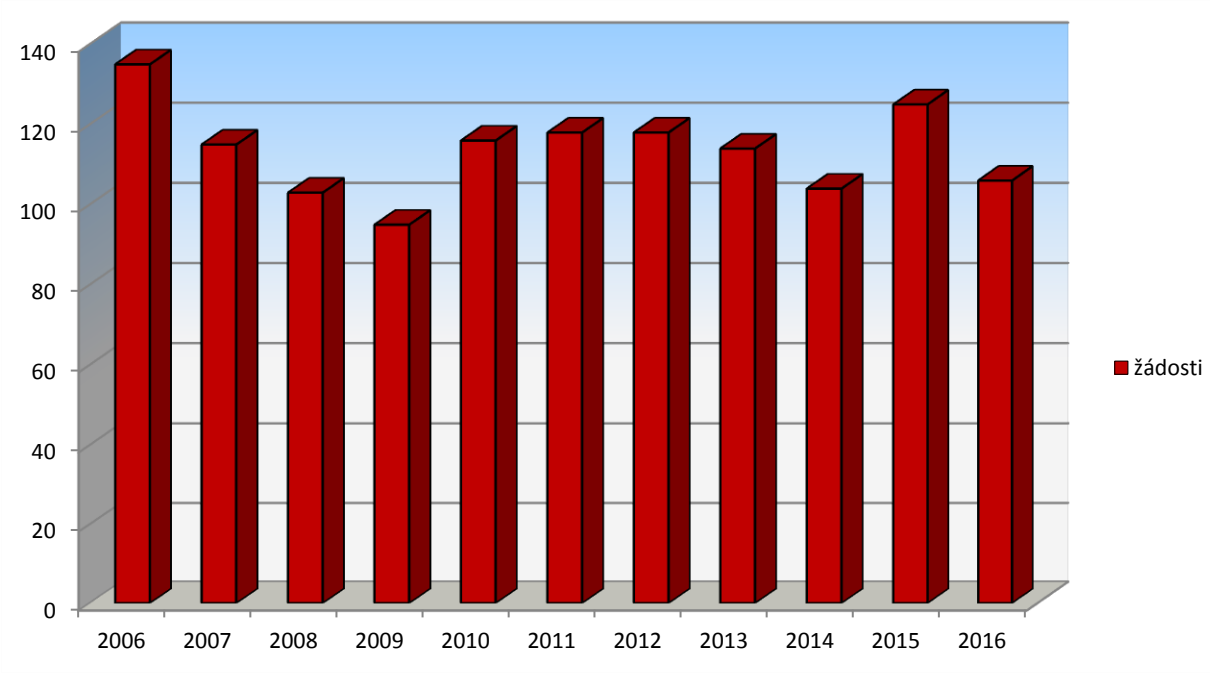
Celkem 64 certifikátů informačních systémů bylo vydáno na žádost podanou v roce 2016, a to 22 pro informační systémy provozované státní správou nebo samosprávou a 42 pro informační systémy podnikatelů. O nově vybudovaný a certifikovaný informační systém se jednalo pouze jedenkrát u žadatele ze státní správy a pětkrát u žadatele z komerční sféry.

V 15 případech provozovatel informačního systému s certifikátem platným do data spadajícího do roku 2016 nepožádal o opakovanou certifikaci a platnost certifikátu automaticky skončila. V 5 případech bylo řízení o certifikaci informačního systému zastaveno Úřadem (např. pro nezájem žadatele nebo na jeho žádost).

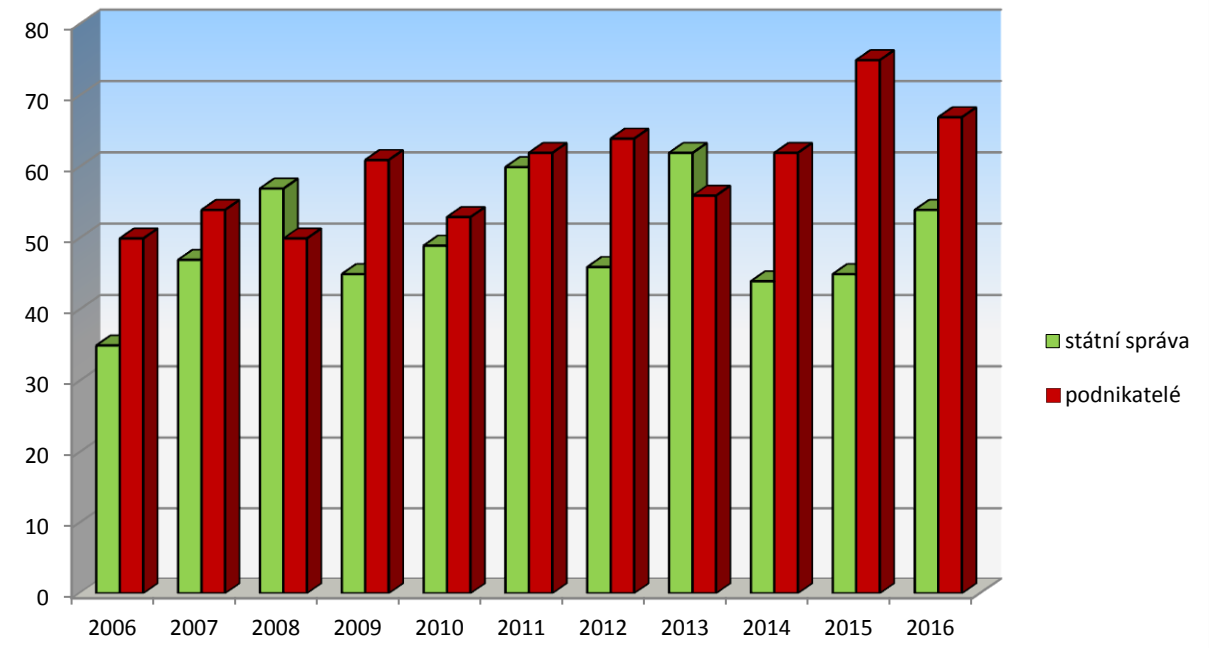
Certifikace informačních systémů v roce 2016

Řešené žádosti v roce 2016	Vydané certifikáty podle stupně utajení				Vydané certifikáty	
	Vyhrazené	Důvěrné	Tajné	Přísně tajné	státní správa	podnikatelé
157	24,8 %	50,4 %	24,0 %	0,8 %	54	67

Přijaté žádosti o certifikaci informačního systému v letech 2006 až 2016



Vydané certifikáty informačních systémů v letech 2006 až 2016



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 v roce 2016 přibyla pouze 1 žádost o certifikaci nově budovaného informačního systému ze státní správy a 5 žádostí od podnikatelů. Většina informačních systémů pro zpracování utajovaných informací je totiž 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. Podle zákona musí být podána žádost o opakovanou certifikaci informačního systému nejpozději 6 měsíců před koncem platnosti jeho certifikátu.

V roce 2016, kromě certifikace menších informačních systémů podnikatelů, několika ministerstev a úřadů (Ministerstvo životního prostředí, Ministerstvo průmyslu a obchodu, Ministerstvo práce a sociálních věcí, Ministerstvo dopravy, Úřad vlády ČR, Ústavní soud, Generální inspekce bezpečnostních sborů, Generální finanční ředitelství, několik krajských a městských úřadů) proběhla opakovaná nebo nová certifikace řady rozsáhlých informačních systémů rezortu Ministerstva vnitra a Policie ČR, rezortu Ministerstva obrany včetně Vojenského zpravodajství, Ministerstva zahraničních věcí, Bezpečnostní informační služby a Generálního ředitelství cel.

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 splněny podmínky pro vydání certifikátu informačního systému.

V roce 2016 Úřad provedl pro rezort Ministerstva obrany národní akreditaci lokalit 2 důležitých součinnostních systémů NATO a pro Ministerstvo vnitra národní akreditaci lokalit 2 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.

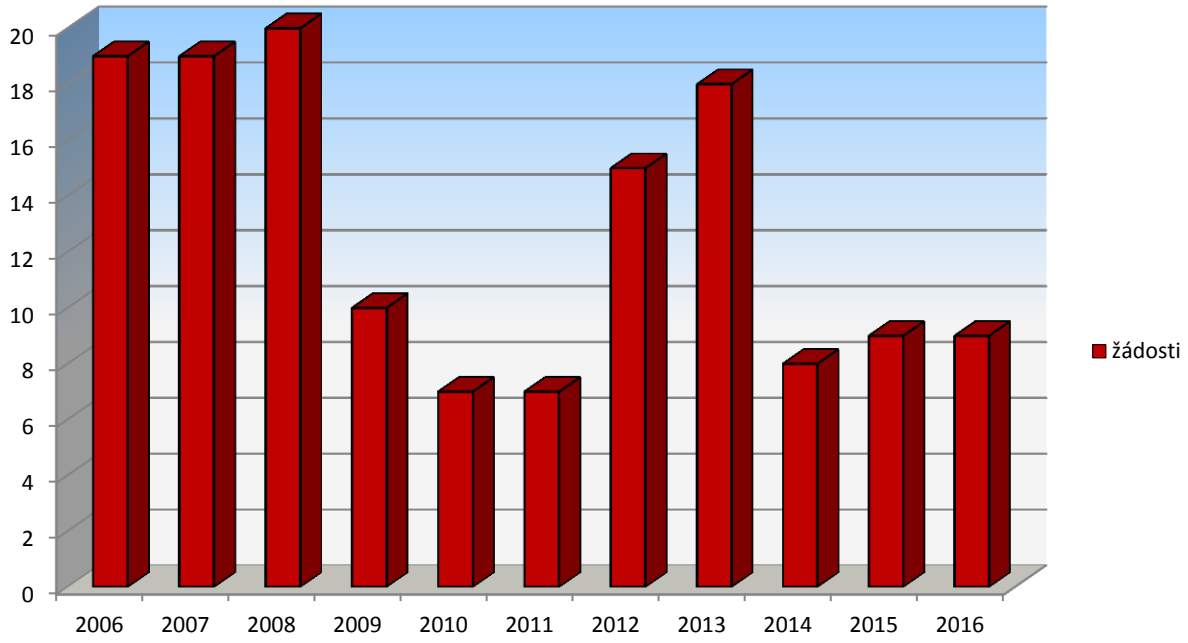
2.6.1.2. Certifikace kryptografických prostředků

V roce 2016 bylo Úřadu podáno celkem 9 žádostí o certifikaci kryptografického prostředku, z toho 4 pro nový kryptografický prostředek. V řízeních k certifikaci kryptografického prostředku bylo vydáno 7 certifikátů, 1 řízení bylo ukončeno bez vydání certifikátu. Stav řízení je shrnut v následující tabulce.

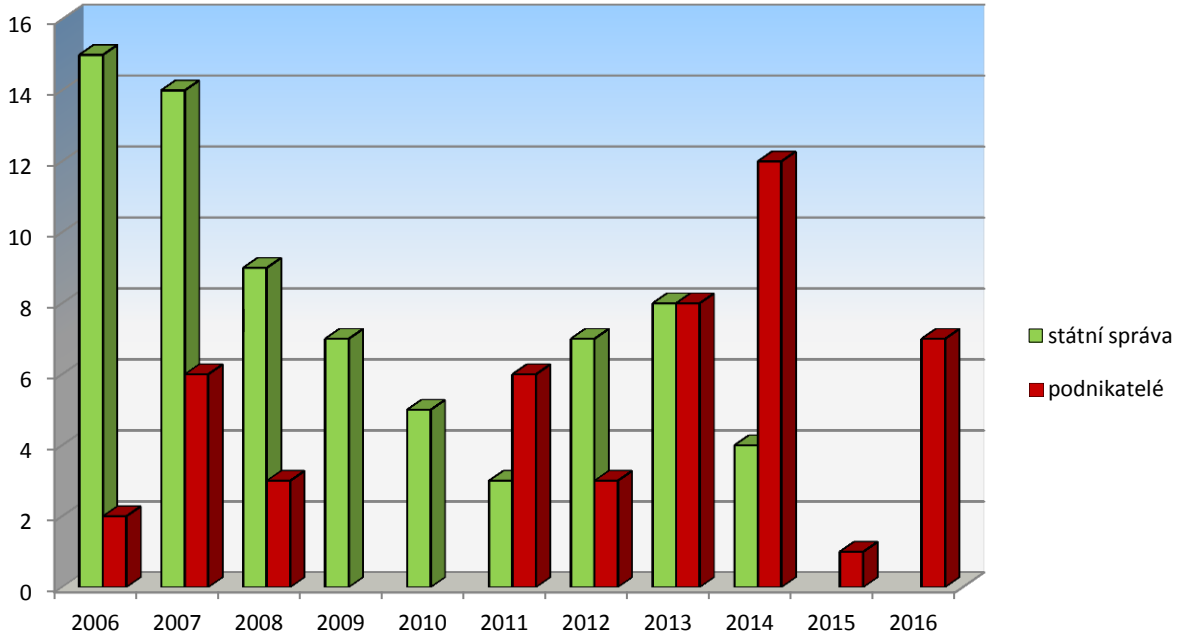
Certifikace kryptografických prostředků v roce 2016

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	7	5	0	1	0	7	5	2

Přijaté žádosti o certifikaci kryptografického prostředku v letech 2006 až 2016



Vydané certifikáty kryptografických prostředků v letech 2006 až 2016



V roce 2016 nebyl certifikován žádný nový kryptografický prostředek, všechny žádosti se týkaly opakované certifikace. V návaznosti na dílčí změny v podmínkách provozování kryptografických prostředků současně probíhaly aktualizace příslušných certifikačních zpráv kryptografických prostředků.

Významný podíl pracovní kapacity pracoviště certifikace kryptografických prostředků byl zaměřen na doplňování a hodnocení podkladů k certifikaci kryptografických prostředků, u kterých probíhá certifikační řízení a na zpracování nebo aktualizaci pravidel pro používání kryptografických

prostředků a příslušného klíčového materiálu kryptografického prostředku (např. PCA a prostředky třídy LANPCS). Nezanedbatelné byly také činnosti související s přípravou podkladů pro „duální“ hodnocení kryptografického prostředku LANPCSe-AES jako prostředku schváleného EU a zahájení jednání s jeho hodnotitelem. V návaznosti na vydané dokumenty NATO a EU ke kryptografické ochraně byla zpracovávána stanoviska k jejich aplikaci do podmínek provozování kryptografických prostředků v ČR.

Současně pokračovaly 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). Přehled aktuálně certifikovaných kryptografických prostředků je pravidelně zveřejňován ve Věstníku Úřadu.

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“ nebyl nově zařazen žádný kryptografický prostředek.

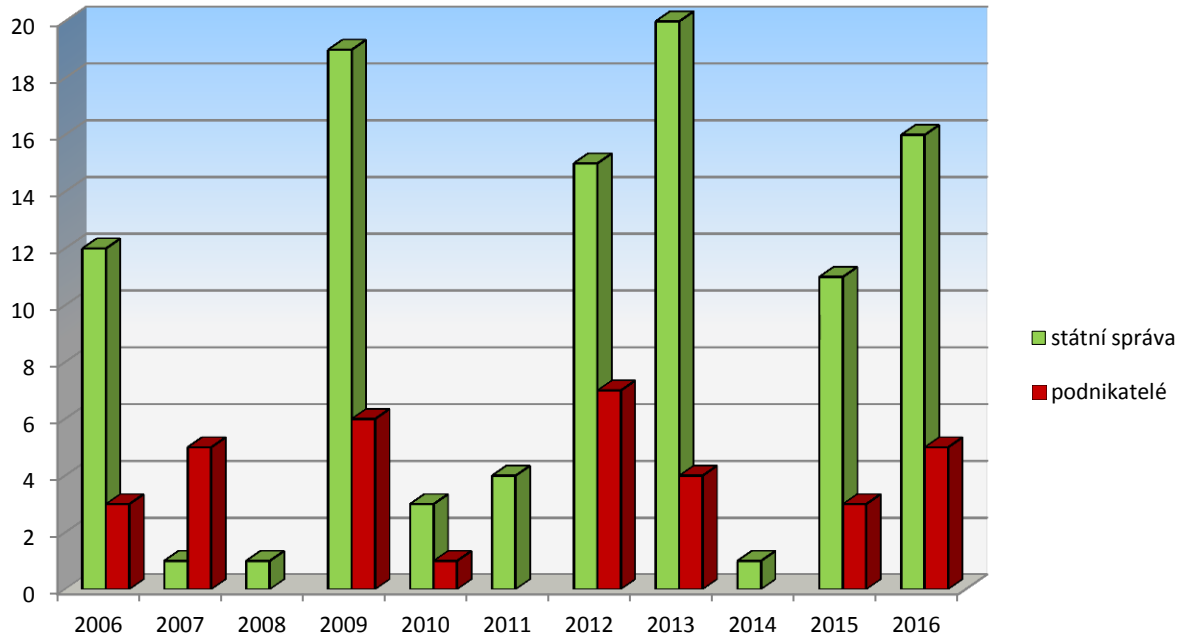
2.6.1.3. Certifikace kryptografických pracovišť

V roce 2016 bylo podáno celkem 21 žádostí o certifikaci kryptografického pracoviště. Většina žádostí o certifikaci spadá do kategorie žádostí o opakovanou certifikaci provozovaných kryptografických pracovišť. Byly podány 2 žádosti o certifikaci nového kryptografického pracoviště, které jsou ve stadiu 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 schválených činností jednotlivých pracovišť, navýšení o další kryptografické prostředky a systémy a ke změnám jejich umístění. Všechny změny musí být předem posouzeny a schváleny Úřadem. Stav řízení je shrnut v následující tabulce.

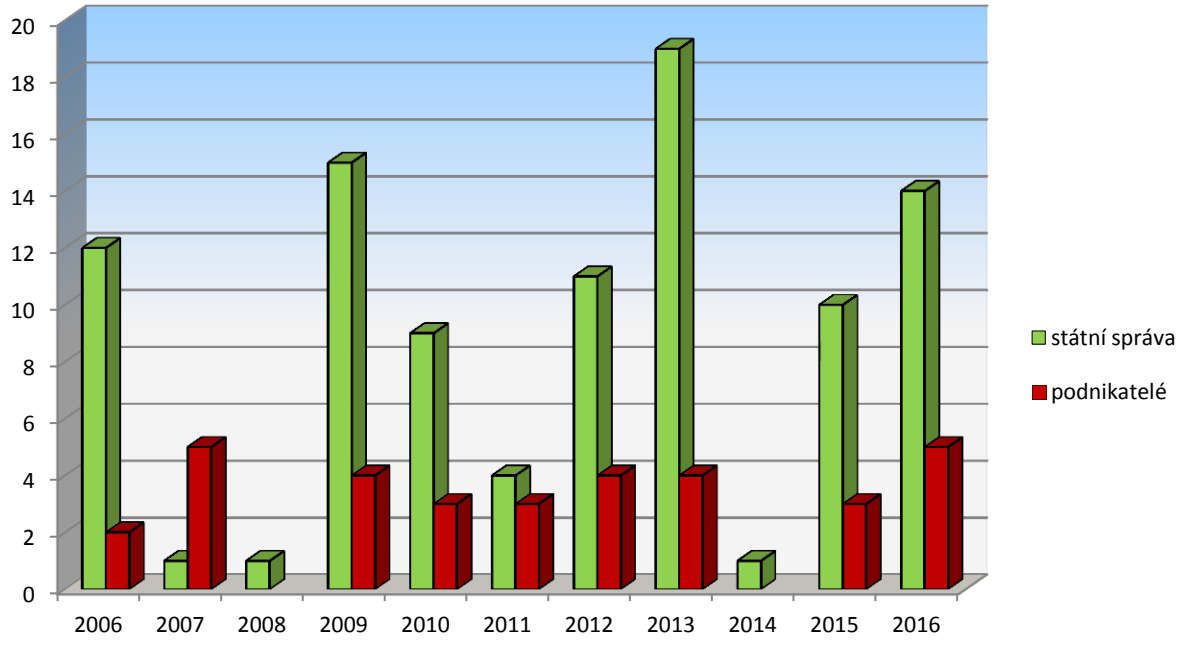
Certifikace kryptografických pracovišť v roce 2016

	Přijaté žádosti	Rozpracováno	Certifikováno	Zamítnuto
Státní správa	16	2	14	0
Podnikatelé	5	0	5	0
Celkem	**21**	**2**	**19**	**0**

Přijaté žádosti o certifikaci kryptografického pracoviště v letech 2006 až 2016



Vydané certifikáty kryptografických pracovišť v letech 2006 až 2016



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 na zastupitelských úřadech v zahraničí. Díky tomu, že příslušné pracoviště Úřadu bylo vybaveno další technikou, bylo možné plnit požadavky Ministerstva zahraničních věcí v přiměřených lhůtách. Celkem bylo vydáno 19 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 2016 bylo v Úřadu vygenerováno celkem 97 971 kryptografických klíčů a hesel uložených na 8 286 nosičích různých typů a dalších 681 ks jiného kryptografického materiálu (procesory, paměti, kryptografická dokumentace, instalační a šifrovací SW).

Úřad vzal do evidence a provedl distribuci celkem 936 ks nového kryptografického a CCI materiálu a dále zajistil servis a opravy na území ČR u 99 ks kryptografických prostředků a mimo ČR u 16 ks kryptografických prostředků.

V průběhu roku 2016 byla zahájena nová výroba klíčového materiálu pro kryptografický prostředek PCA.

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 2016 TEMPEST měření podle standardů NATO řady SDIP, EU řady IASG 7 a podle metodiky CISPR 17. 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 2016 hodnoceno více než 20 typů zařízení. Z toho bylo prováděno TEMPEST měření více než 10 ks zařízení EUROTEMPEST, STEP a Siltec, a to jako samostatného zařízení nebo v kombinaci s kryptografickým prostředkem KRYDEC a PCS. Dále bylo provedeno měření inovovaných systémů s kryptografickým prostředkem TCE 621 a PCA. Tato měření byla prováděna podle metodiky standardu SDIP-27/2. 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 (např. 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. Prováděno bylo rovněž zónové hodnocení prostorů na základě podkladů dodaných akreditovanými pracovišti Ministerstva obrany a Vojenského zpravodajství.

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

V roce 2016 byly provedeny obranné prohlídky v několika objektech jak v ČR, tak mimo ČR 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 2016, je uveden v následující tabulce.

Měřená zařízení a objekty v roce 2016

Typ měření[9)]	**Počet**
Zónové měření	23 objektů
Kryptografické prostředky	3 typy
PC sestavy	8 sestav – třída 0; přes 20 typů – třída 1 a 2
Audiotechnika	2 typy zařízení
Obranné prohlídky i v rámci certifikace IS	14 objektů
Mobilní systémy	2 systémy
Instalační záznamy	6 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 2016 nebyla podána žádná žádost o schválení projektu bezpečnosti nového komunikačního systému.

[9)] 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 nebo Úřad. U instalačních záznamů se jedná o systémy, které mohou mít několik instalací v rámci ČR i mimo ČR.

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

Podporu pro provoz 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 2016 nadále zajišťoval Úřad.

Komunikační systém Panthon pro mobilní komunikaci informací stupně utajení Vyhrazené, který využívá certifikovaného kryptografického prostředku Panthon 3, je rovněž provozován za podpory 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 2016 organizačně zajistil a provedl, v souladu se zákonem, celkem 22 školení skupin pracovníků kryptografické ochrany a po následující zkoušce odborné způsobilosti vydal 114 osvědčení o zvláštní odborné způsobilosti pracovníka kryptografické ochrany. Dále provedl zaškolení pracovníků provozní obsluhy kryptografického prostředku a vydal 4 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 2016 schvaloval aktualizaci osnov a obsahu některých kurzů.

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

Zákonem stanovené činnosti Úřadu v oblasti kryptografické ochrany a bezpečnosti informačních systémů nakládajících s utajovanými informacemi byly v roce 2016 zajištěny.

- 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 certifikace informačních systémů, kryptografických prostředků a pracovišť jsou pracovní místa v Úřadu aktuálně přidělená pro tyto činnosti kvalitně obsazena, avšak celkově je tato oblast personálně poddimenzována. Vzhledem k malému počtu pracovníků, kteří řeší jednotlivá certifikační řízení, má výpadek každého pracovníka (mateřská dovolená, dlouhodobé onemocnění, odchod pracovníka) poznatelný vliv na již tak vysoké pracovní vytížení odborných pracovníků. Nová pracovní místa jsou potřebná rovněž pro testování bezpečnostních technologií a analýzu rizik pro informační a komunikační systémy.

- V oblasti kryptologie došlo v Úřadu v roce 2016 k reálnému úbytku odborných pracovníků. Získání nových odborníků je obtížné, neboť se jedná o specializované činnosti, které jsou v soukromé sféře vyhledávané. Pro tyto pozice v Úřadu je vyžadována bezpečnostní prověrka pro přístup k utajovaným informacím stupně utajení Tajné nebo Přísně tajné. Přitom i tato oblast je personálně poddimenzována.

- 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 potřebné také personální posílení pracoviště Úřadu, zajišťujícího výrobu, evidenci a distribuci kryptografického materiálu národního a EU v ČR. V rámci rezortů 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 certifikovaných informačních systémů.

2.7. ADMINISTRATIVNÍ A FYZICKÁ BEZPEČNOST, ÚSTŘEDNÍ REGISTR

2.7.1. Administrativní bezpečnost

Pracoviště koncepce administrativní bezpečnosti pokračovalo v řešení úkolu implementace utajovaných dokumentů v digitální podobě do stávající legislativy. Úřad zřídil počátkem roku 2015 mezirezortní odbornou pracovní skupinu složenou z odborníků na problematiku správy dokumentů v digitální podobě a se znalostí principů administrativní bezpečnosti. Ve skupině působí zástupci Ministerstva vnitra, Ministerstva obrany, IRMS (Information and Records Management Society – Czech Republic Group, o.s.), Jihočeské univerzity, Národního archivu a dalších úřadů zabývajících se bezpečností státu.

Výsledkem dvouleté práce skupiny bylo vytvoření modelu komplexního datového kontejneru utajovaného dokumentu v digitální podobě, který obsahuje jak ztvárnění obsahu utajovaného dokumentu, tak i patřičná metadata vztahující se k tomuto obsahu s popisem vzájemných vztahů jednotlivých entit a popisu přístupových politik (včetně rolí a oprávnění vizualizovat obsah kontejneru).

Skupina vypracovala čtyřstavový model utajovaného dokumentu v digitální podobě definující změnu stavů a popisných údajů mezi tak zvaným podkladem, konceptem, utajovaným dokumentem

a datovou zásilkou. Datový kontejner utajovaného dokumentu v digitální podobě i čtyřstavový model utajovaného dokumentu tvoří základní stavební prvky potřebné pro implementaci správy utajovaných dokumentů v digitální podobě v průběhu celého životního cyklu utajovaného dokumentu do příslušných legislativních norem.

Následně byl zpracován návrh algoritmu životního cyklu utajovaného dokumentu, na jehož základě byl sestaven elementární výčet procesů a vypracovány karty jednotlivých procesů uvedených v elementárním výčtu. Tyto karty byly použity jako vstup pro vytvoření procesních modelů správy utajovaných dokumentů v digitální podobě.

Dále byla zpracována zadávací dokumentace výzkumného projektu Úřadu „Tvorba standardu pro datový kontejner utajovaného dokumentu v digitální podobě a vývoj programového nástroje pro práci s datovým kontejnerem utajovaného dokumentu v digitální podobě“. Cílem realizace výzkumného projektu Úřadu je:

- zabezpečit jednotnost ve správě utajovaných dokumentů v digitální podobě v rámci celé ČR, a to s využitím vytvořeného standardu, jako direktivy závazné pro všechny původce, kteří budou pracovat s utajovanými dokumenty v digitální podobě,

- poskytnout původcům utajovaných dokumentů v digitální podobě v rámci ČR jednotný certifikovaný nástroj pro práci s těmito utajovanými dokumenty, a to jak původcům, kteří budou používat pouze certifikovaný informační systém, tak i původcům, kteří budou používat systém elektronické spisové služby.

Předpokládané ukončení výzkumného projektu Úřadu je v roce 2020 a implementace do příslušných legislativních norem je plánována na rok 2021, s účinností od 1. ledna 2022.

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 9 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 (Státní pokladna Centrum sdílených služeb s.p., Úřad vlády ČR, Ministerstvo financí, O2 Czech Republic a.s., CSC Computer sciences s.r.o.),

- rozsáhlou odbornou metodickou podporu realizace II. etapy rekonstrukce budovy GSA HQ Prague (Galileo), připomínkování projektu fyzické bezpečnosti této etapy a posouzení skutečného stavu instalovaných technických prostředků a stanovených režimových opatření fyzické bezpečnosti,

- metodickou podporu a odborné posouzení opatření fyzické bezpečnosti v souvislosti s plánovaným stěhováním do nového HQ NATO Stálé delegace ČR při NATO v Bruselu,

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

2.7.2.1. Certifikace technických prostředků

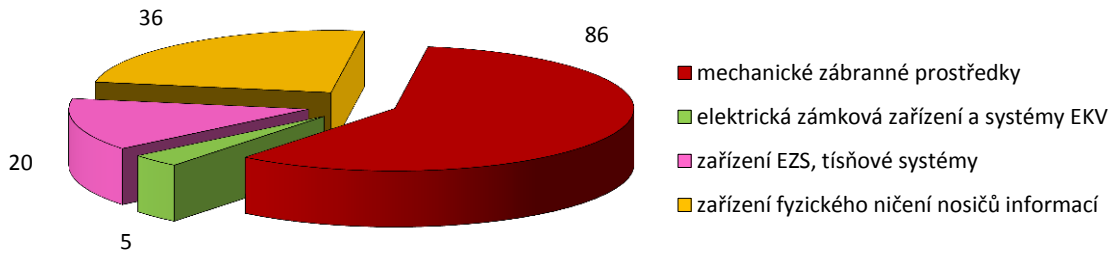
Nezbytnou zákonnou podmínkou pro používání technických prostředků k ochraně utajovaných informací je mj. i jejich certifikace. Úřad v roce 2016 přijal celkem 87 žádostí o certifikaci pro 156 technických prostředků. V rámci posuzovaní a vyhodnocování podkladů pro certifikaci bylo u 18 % žádostí vyžádáno jejich doplnění a upřesnění. Ve 3 případech byl certifikační proces ukončen bez vydání certifikátu, neboť byly zkoušeny podle jiných nebo již neplatných evropských technických norem.

Úřad vydal celkem 147 certifikátů technických prostředků. Počty vydaných certifikátů technických prostředků podle jednotlivých skupin definovaných zákonem jsou uvedeny v následující tabulce.

Vydané certifikáty technických prostředků v roce 2016

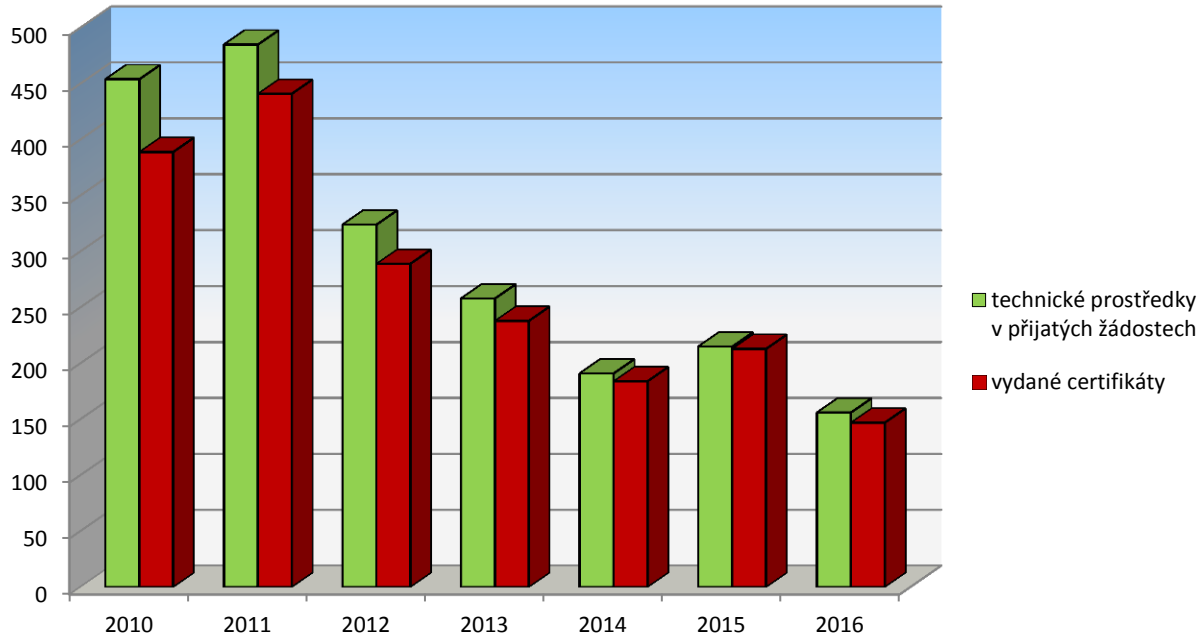
Mechanické zábranné prostředky[10)]	86
Elektrická zámková zařízení, systémy pro kontrolu vstupu[11)]	5
Zařízení elektrické zabezpečovací signalizace a tísňové systémy[12)]	20
Zařízení fyzického ničení nosičů informací[13)]	36
Celkem	**147**

Certifikáty technických prostředků v roce 2016



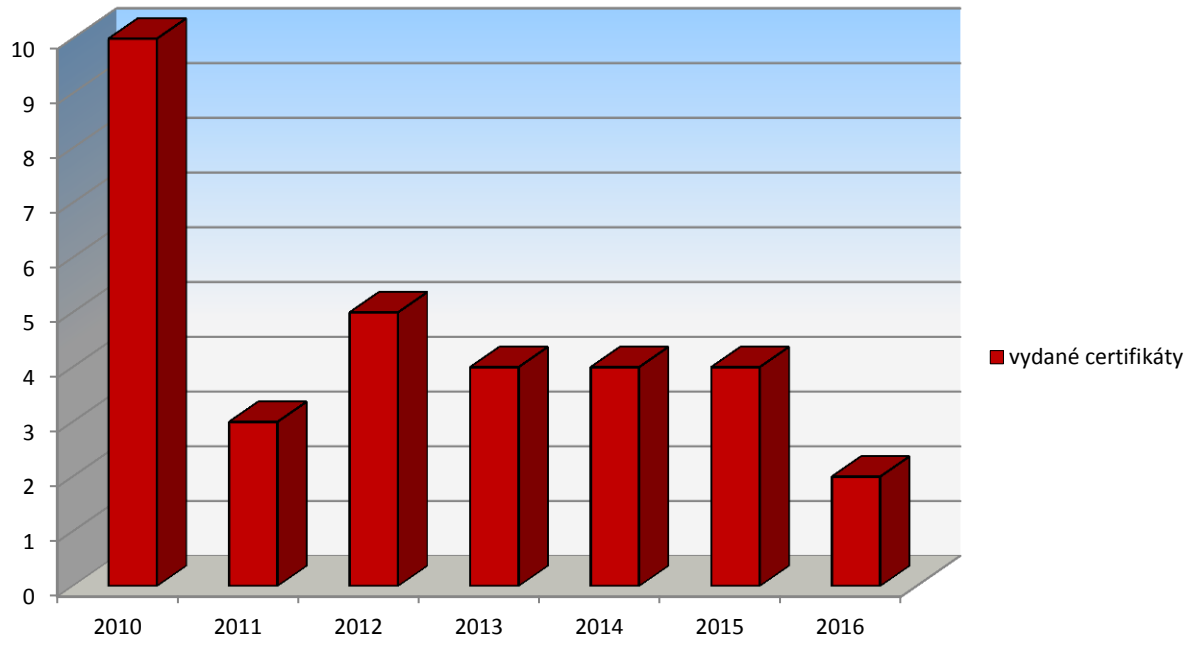
[10)] § 30 odst. 1 písm. a) zákona.
[11)] § 30 odst. 1 písm. b) zákona.
[12)] § 30 odst. 1 písm. c) a e) zákona.
[13)] § 30 odst. 1 písm. h) zákona.

Certifikace technických prostředků v letech 2010 až 2016



Kromě certifikátů uvedených v předchozí tabulce a grafech byly v roce 2016, na základě podaných žádostí, vydány 2 certifikáty pro jednotlivé technické prostředky – uživatelské certifikáty. Jednalo se o 2 kusy bezpečnostních dveří. 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 2010 až 2016



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. V oblasti právních předpisů upravujících certifikaci technických prostředků byla iniciována novelizace a následně zajišťována odborná podpora změn vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů, kterou vyvolaly nové technické normy pro systémy kontroly vstupů v systémových požadavcích a pokynech pro aplikace.

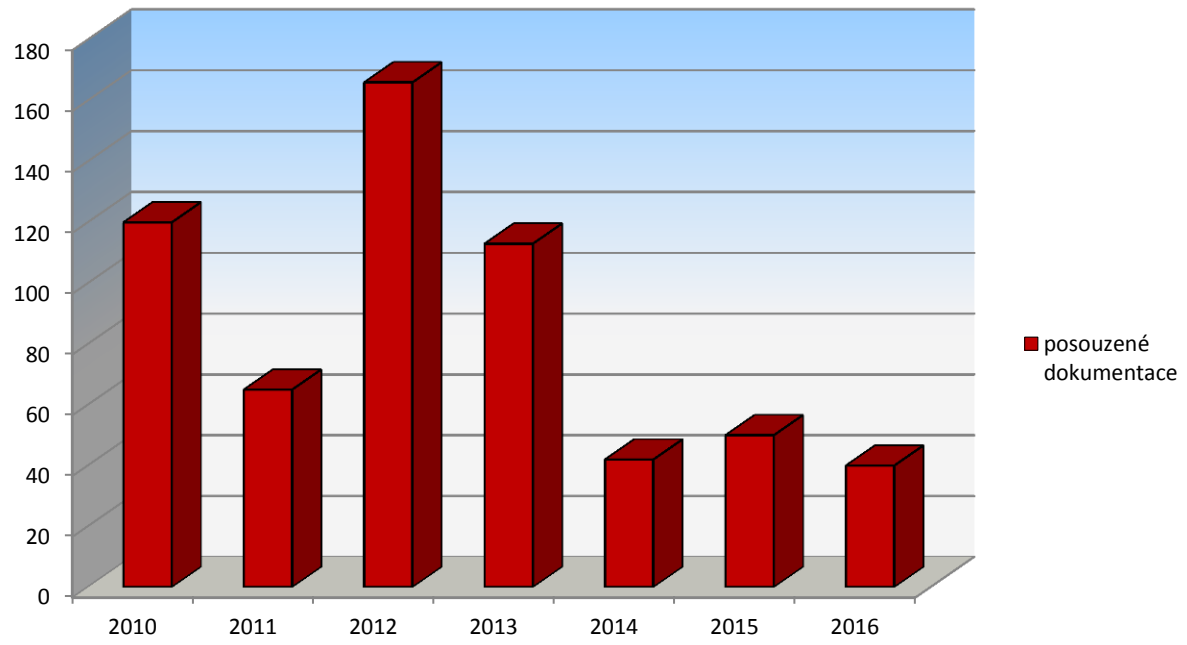
2.7.2.2. Posuzování bezpečnostní dokumentace podnikatele z hlediska fyzické bezpečnosti

V rámci vedených bezpečnostních řízení o vydání osvědčení podnikatele nebo při aktualizaci bezpečnostní dokumentace podnikatele, který je držitelem osvědčení podnikatele, bylo v roce 2016 přijato celkem 43 žádostí o stanovisko k bezpečnostní dokumentaci podnikatele z hlediska zajištění ochrany utajovaných informací fyzickou bezpečností. Při posuzování dokumentací byla ve 33 % případů provedena konzultace s podnikatelem v Úřadu nebo přímo v sídle podnikatele. Bylo posouzeno 40 bezpečnostních dokumentací podnikatele a bylo provedeno 25 tzv. dohlídek, při kterých byla v sídle podnikatele ověřena jeho schopnost zabezpečit ochranu utajovaných informací z hlediska fyzické bezpečnosti. Nebyla vrácena žádná bezpečnostní dokumentace podnikatele z důvodu zastavení řízení. K 31. prosinci 2016 zbývalo posoudit 3 bezpečnostní dokumentace podnikatele. Přehled přijatých žádostí, členěný podle kategorií zabezpečených oblastí, je uveden v následující tabulce.

Přijaté žádosti a posouzené bezpečnostní dokumentace podnikatele v roce 2016

	Důvěrné	Tajné	Přísně tajné	Celkem
Přijaté žádosti	32	11	0	**43**
Posouzené dokumentace	29	11	0	**40**

Posouzené bezpečnostní dokumentace podnikatele v letech 2010 až 2016



2.7.2.3. Problémové oblasti fyzické bezpečnosti

Certifikace technických prostředků:

- nedostatečné podkladové dokumenty k žádosti o certifikaci technického prostředku a posouzení technických prostředků podle neplatné technické normy.

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

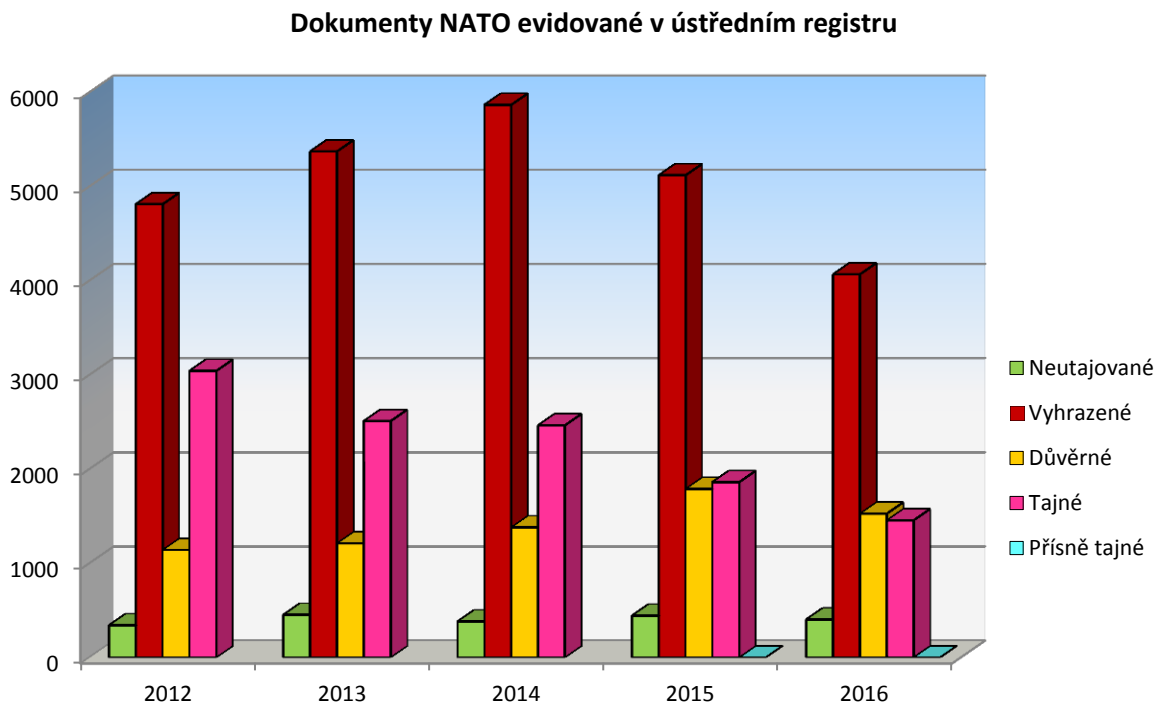
- nízká odborná znalost problematiky ochrany utajovaných informací osob odpovědných za realizaci této oblasti u podnikatelů,
- nedostatky ve zpracování projektů fyzické bezpečnosti (nedostatečný popis rozmístění technických prostředků),
- nekompletní popis režimových opatření fyzické bezpečnosti (nedostatky v evidenci přístupových prvků a označování klíčů, neaktualizované seznamy oprávněných osob),
- nedostatky při instalaci technických prostředků (chybné umístění jednotlivých prvků, nesprávná funkčnost přístupového systému, nesoulad skutečného stavu se stavem deklarovaným).

2.7.3. Ústřední registr

Prostřednictvím ústředního registru je realizováno poskytování utajovaných informací v rámci mezinárodního styku. V roce 2016 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	2012	2013	2014	2015	2016	Celkem
Neutajované	434	454	384	445	405	**2 122**
Vyhrazené	4 814	5 374	5 869	5 121	4 069	**25 247**
Důvěrné	1 143	1 213	1 383	1 719	1 528	**6 986**
Tajné	3 044	2 511	2 466	1 863	1 457	**11 341**
Přísně tajné	0	0	0	1	1	**2**
Celkem	**9 435**	**9 552**	**10 102**	**9 149**	**7 460**	**45 698**



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 24 kontrol podřízených registrů utajovaných informací. Zároveň se pracovníci ústředního registru účastnili 9 kontrol v rámci výkonu státního dozoru u orgánů státu a podnikatelů, které mají zřízeny registry utajovaných informací. Kontroly byly zaměřeny zejména na změny v oblasti administrativní bezpečnosti. Zjištěné nedostatky se týkaly zejména povinných náležitostí jednacích protokolů a seznamů zaměstnanců, kterým lze umožnit přístup k utajovaným informacím cizí moci.

V rámci metodického řízení bylo v roce 2016 provedeno školení vedoucích podřízených ATOMAL registrů a jejich zástupců. Školení bylo zaměřeno na bezpečnost utajovaných informací ATOMAL a prezentaci zkušeností získaných při cvičení ATOMAL, kterého se v roce 2016 zúčastnili společně s pracovníky Ministerstva obrany i zástupci ústředního registru. V souvislosti s novelizací vyhlášky č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací, ve znění pozdějších předpisů, bylo dále provedeno školení pro zaměstnance rezortu Ministerstva obrany.

Ústřední registr ověřoval splnění podmínek nezbytných pro zřízení registru utajovaných informací u 2 subjektů, které podaly žádost o souhlas ke zřízení registru utajovaných informací cizí moci. V seznamu všech registrů zřízených na území ČR bylo ke konci roku 2016 evidováno celkem 46 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. Průběžně byly 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 2016

Stupeň utajení	Počet čísel jednacích
Neutajované	686
Vyhrazené	3 056
Důvěrné	2 750
Tajné	8 814
Celkem	**15 306**

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.

Ve dnech 27. – 29. dubna 2016 byla v ČR provedena Generálním sekretariátem Rady EU hodnotící návštěva EU, která se zabývala kontrolou zabezpečení ochrany utajovaných informací EU. Hodnotící návštěva byla provedena ve 4 Přísně tajných a Tajných registrech utajovaných informací, a to v oblasti administrativní, fyzické a personální bezpečnosti a v oblasti utajovaných informací v rámci informačních systémů. Zpráva o výsledku hodnotící návštěvy zatím nebyla Úřadu doručena.

2.8. KYBERNETICKÁ BEZPEČNOST

Rok 2016 potvrdil, že zajištění kybernetické bezpečnosti patří ke klíčovým výzvám státu, na které ČR musí reagovat. Přelomovou událostí v tomto ohledu bylo listopadové usnesení vlády ČR č. 1049, ve kterém byl schválen rozvoj kapacit a schopností NCKB do roku 2025. Vláda následně rozhodla ve schváleném usnesení č. 1178 o oddělení NCKB ze struktur Úřadu a vytvoření samostatného Národního úřadu pro kybernetickou a informační bezpečnost ve druhé polovině roku 2017.

Dalším z milníků v posilování kybernetické bezpečnosti v ČR bylo zahájení kontrol prvků kritické informační infrastruktury a významných informačních systémů. Ochrana těchto prvků je jedním z hlavních úkolů NCKB a započaté kontroly jsou zásadním krokem směrem k posílení odolnosti systémů KII a VIS. Neméně důležitým úkolem byla příprava novelizace zákona o kybernetické bezpečnosti, která vyplývá z potřeby nastolení souladu se směrnicí NIS.

2.8.1. Budování NCKB/GovCERT.CZ

NCKB prošlo v roce 2016 zásadní organizační změnou. S platností od 1. listopadu došlo ke zrušení pozice ředitele NCKB a povýšení dvou stávajících oddělení ve struktuře NCKB na odbory. Nově se NCKB člení na odbor vládní CERT (bývalé oddělení vládní CERT) a odbor kybernetických bezpečnostních politik (bývalé oddělení teoretické podpory, vzdělaní a výzkumu). Vládní CERT (GovCERT.CZ) řeší kybernetické bezpečnostní incidenty po technické stránce, provádí penetrační testy, analýzu malware a zajišťuje sdílení informací o incidentech, zranitelnostech a trendech v kybernetické bezpečnosti s IT komunitou i veřejností. Odbor kybernetických bezpečnostních politik se soustředí na netechnické aspekty kybernetické bezpečnosti, zejména na tvorbu a implementaci kybernetické bezpečnostní politiky ČR, určování KII a posuzování VIS podle zákona o kybernetické bezpečnosti a prováděcích předpisů, mezinárodní spolupráci, osvětu a vzdělávání nebo publikační činnost. Nově zřízené oddělení strategických informací a analýz posílí analytické kapacity národního centra.

Zásadní událostí pro rozvoj NCKB bylo usnesení vlády ČR č. 1178 ze dne 19. prosince 2016, ve kterém vláda rozhodla o oddělení NCKB ze struktury Úřadu a vytvoření Národního úřadu pro kybernetickou a informační bezpečnost ve druhé polovině roku 2017. Neméně důležité bylo usnesení vlády ČR č. 1049 ze dne 28. listopadu, kterým byl schválen návrh rozvoje kapacit a schopností NCKB do roku 2025. Plán rozšíření předpokládá navýšení personální kapacity na 300-400 zaměstnanců do roku 2025 a výstavbu nové budovy v Brně – Černých polích.

NCKB pokračovalo v roce 2016 ve zvyšování kvalifikace svých pracovníků formou specializovaných školení, stáží a kurzů. Pracovníci GovCERT.CZ získali certifikace společnosti SANS, pracovníci odboru kybernetických bezpečnostních politik se účastnili celé řady školení a kurzů zaměřených na kybernetickou bezpečnost v kontextu mezinárodního práva, terorismu či metod analýzy z otevřených zdrojů.

V průběhu roku byla spuštěna nová verze veřejné části webových stránek sloužící jako informační portál širší a odborné veřejnosti. Neveřejná část je téměř dokončena a k jejímu předání a spuštění by mělo dojít na začátku roku 2017. Tento nový systém usnadní správu stránek a jejich plnění obsahem. Neveřejná část s kontrolou přístupu pak umožní ve větší míře sdílení informací směrem ke správcům systémů KII a VIS a také ke spolupracujícím bezpečnostním týmům. Jedná se zejména o informace, které není možné sdílet zcela veřejně, aby k nim nezískal přístup potenciální útočník.

2.8.2. Vývoj legislativy a koncepčních dokumentů

V roce 2016 pokračoval Úřad v naplňování Akčního plánu, který vychází z hlavních cílů Národní strategie kybernetické bezpečnosti na období let 2015-2020 a na příštích 5 let definuje konkrétní úkoly k jejímu naplnění. 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 ČR nebo Český telekomunikační úřad.

Snahy o zavedení minimálních bezpečnostních standardů pro důležité informační a komunikační systémy a o lepší koordinaci při zajišťování kybernetické bezpečnosti, které na vnitrostátní úrovni vedly k přijetí zákona o kybernetické bezpečnosti, nalezly v roce 2016 konkrétní vyústění i na evropské úrovni v podobě směrnice NIS.

Směrnice NIS upravuje dvě obecné kategorie subjektů, tzv. operátory základních služeb a poskytovatele digitálních služeb, kteří budou v různé míře muset zavádět bezpečnostní opatření a hlásit bezpečnostní incidenty způsobilé narušit klíčové společenské a ekonomické činnosti zajišťované jimi provozovanými službami, resp. kontinuitu poskytování svých služeb. Tyto subjekty coby nové kategorie doplní stávající povinné osoby podle § 3 zákona o kybernetické bezpečnosti, tj. orgány a osoby zajišťující provoz sítí elektronických komunikací, poskytování služeb elektronických komunikací, provozovatele významných sítí, správce prvků KII a správce VIS.

Směrnice NIS kromě identifikace provozovatelů základních služeb a stanovení požadavků na bezpečnostní opatření, na detekci incidentů a na jejich hlášení ukládá členským státům také povinnost zpracovat národní strategii kybernetické bezpečnosti, určit vnitrostátní příslušné orgány, jednotná kontaktní místa pro styk se zahraničními protějšky a pro regulovaná odvětví zřídit bezpečnostní týmy CSIRT a zajistit jejich fungování. ČR řadu těchto opatření zavedla již v souvislosti s přijetím zákona o kybernetické bezpečnosti. Členské státy rovněž budou spolupracovat v rámci 2 směrnicí zřizovaných platforem – Skupiny pro spolupráci pro otázky strategické povahy a Sítě CSIRT pro spolupráci technickou.

V roce 2016 byla rovněž novelizována vyhláška č. 317/2014 Sb., o významných informačních systémech, jejíž příloha stanoví seznam těchto systémů a musela být v souvislosti s pokračující identifikací nových systémů aktualizována.

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 v roce 2016 proces kontroly prvků KII, jejichž správcům, stejně jako správcům VIS vznikly zákonné povinnosti ve vztahu k bezpečnostním opatřením a specifické povinnosti vůči Úřadu.

KII je určována Úřadem podle kritérií stanovených nařízením vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, ve znění nařízení vlády č. 315/2014 Sb. Proces určování, resp. posuzování, zda systémy naplňují stanovená kritéria, probíhá ve spolupráci s daným správcem systému s využitím analýz dopadu incidentů a dalších podkladů. Obecně se jedná o takové informační a komunikační systémy, jejichž narušení by mohlo mít závažný dopad na zabezpečení základních životních potřeb, zdraví osob, bezpečnost nebo ekonomiku státu.

VIS je definován v § 2 písm. d) zákona o kybernetické bezpečnosti jako informační systém spravovaný orgánem veřejné moci, který není KII a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci. Z definice lze dovodit, že jako VIS může být identifikován pouze systém ve správě subjektu státní sféry. Soukromý sektor je tedy z této úpravy vyloučen. Pokud by systém naplnil kritéria pro KII i VIS, určí se jako KII, neboť přísnější regulace má přednost. Z regulace VIS jsou dále vyloučeny obce. Rozdíl oproti KII je u VIS také v procesu určení. Naplnění kritérií VIS musí posoudit sám správce systémů. Pokud kritéria naplní, vzniká mu povinnost nahlásit kontaktní údaje Úřadu a začít se řídit zákonem o kybernetické bezpečnosti. NCKB v této oblasti poskytuje metodickou podporu a konzultace.

K 31. prosinci 2016 NCKB evidovalo 48 KII a 158 VIS ve správě 80 orgánů veřejné moci a 51 KII a 20 správců v soukromém sektoru.

Začátkem roku 2016 byly u povinných osob zahájeny kontroly dodržování zákona o kybernetické bezpečnosti. Výkonem kontrol je na základě tohoto zákona pověřen Úřad a provádí je NCKB. Kontroly byly u správců vždy prováděny po uplynutí tzv. přechodné lhůty (roční lhůta na zavedení požadovaných bezpečnostních opatření). Většina z kontrol vykonaných v roce 2016 byla

zaměřena na VIS. Menší podíl kontrol se zaměřoval na KII. Úřad provedl kontrolu u celkem 15 povinných subjektů (správců). Předmětem proběhlých kontrol bylo celkem 24 systémů.

Hlavním kritériem kontroly je zákon o kybernetické bezpečnosti a jeho prováděcí právní předpis vyhláška č. 316/2014 Sb., o kybernetické bezpečnosti. Kontroly probíhají v souladu se zákonem č. 255/2012 Sb., o kontrole (Kontrolní řád). Proces kontroly se principiálně blíží procesu auditu dle ISO 19 011 a norem řady ISO 27k. Kontroly v roce 2016 byly až na výjimku tzv. metodické. V případě identifikování neshody (porušení některého z požadavků zákona) u metodických kontrol nebylo zahajováno správní řízení. Důvodem k tomuto opatření je snaha pracovat s povinnými subjekty na nápravě a ohled na krátkou platnost zákona o kybernetické bezpečnosti.

Z celkového počtu 15 provedených kontrol byl ve 3 případech zjištěn celkový soulad. V ostatních 12 případech byl shledán nesoulad, tj. 12 kontrolovaných subjektů se dopustilo porušení zákona o kybernetické bezpečnosti.

2.8.4. Spolupráce Úřadu v oblasti kybernetické bezpečnosti

Stejně jako v předchozích letech, i v roce 2016 pokračoval Úřad v navazování a rozvíjení bilaterální a multilaterální mezinárodní spolupráce. Přehled mezinárodních aktivit v této oblasti je uveden v kapitole 2.2.3.

Úřad jako národní gestor dané oblasti aktivně spolupracuje s ostatními rezorty státní správy a snaží se tak udržovat jednotný postoj ČR směrem do zahraničí. Spolu s akademickou sférou se podílí na přípravě budoucích odborníků a na navyšování povědomí o kybernetické bezpečnosti. S bezpečnostními týmy CSIRT sdílí informace a zkušenosti se zranitelnostmi a podílí se na vývoji nových technických nástrojů. Vládní tým CERT a národní tým CSIRT.CZ vzájemně tradičně sdílí informace, zkušenosti a know-how týkajících se zranitelností. V rámci českého zapojení v projektu The Honeynet Project také spolupracují na přípravě sdílení informací z honeynetů a společně se účastní mezinárodních cvičení kybernetické bezpečnosti.

Sdružení CZ.NIC, coby provozovatel Národního CERT týmu, v rámci projektu PROKI (Predikce a obrana před kybernetickými hrozbami), který byl podpořen v rámci programu Bezpečnostního výzkumu České republiky 2015-2020, zahájil v roce 2016 pilotní provoz a započal i zasílaní výstupních zpráv subjektům, které se dobrovolně do pilotního provozu nahlásily. V roce 2016 se sdružení CZ.NIC a tým CSIRT.CZ zapojily do projektu Safer Internet a od července začaly provozovat službu Internet Hotline, která slouží pro hlášení nezákonného obsahu na internetu.

Důležitou roli v zajišťování kybernetické bezpečnosti hraje akademická obec. Ta také patří k tradičním partnerům Úřadu. Zástupci obou sfér se spolupodílí na přípravě budoucích odborníků, realizují kybernetická cvičení a sdílí informace a zkušenosti o kybernetických incidentech. Úřad v roce 2016 úzce spolupracoval zejména s Masarykovou univerzitou v Brně. Vedle příprav národních cvičení probíhala spolupráce v technické rovině i mezi týmy CSIRT-MU při Fakultě informatiky a GovCERT.CZ. V právnické rovině byla spolupráce započata již přípravou zákona o kybernetické bezpečnosti a v loňském roce pokračovala konzultacemi o jeho novelizaci. Na půdě Masarykovy univerzity v Brně proběhla i neformální setkání právníků zabývajících se kybernetickou bezpečností, tzv. CyberCake, kterého se účastnili odborníci z akademické obce, Úřadu, justice a dalších složek státní správy. V rámci přípravy budoucích expertů se NCKB podílelo na výuce předmětů na vysokých školách. Na Fakultě sociálních studií Masarykovy univerzity v Brně a na Přírodovědné fakultě Univerzity Palackého v Olomouci zajišťovali jeho zástupci výuku předmětu „Kybernetická bezpečnost“.

V polovině března zorganizovalo NCKB společně s Ústavem výpočetní techniky Masarykovy univerzity v Brně cvičení s názvem Cyber Czech 2015 II. Jednalo se o opakování cvičení, které bylo

poprvé uspořádáno v říjnu předchozího roku. Hlavním cílem bylo ověřit praktické znalosti zvládání kybernetických incidentů v souvislosti s ochranou prvků KII ČR a procvičit postupy podle zákona o kybernetické bezpečnosti včetně komunikace s médii při zvládání nastalé krize. Cvičení se zúčastnili zástupci z řad subjektů státní správy a subjektů KII. Jejich úkolem bylo, stejně jako v říjnu předchozího roku, bránit informační infrastrukturu fiktivní jaderné elektrárny, na kterou útočil tým hackerů, tzv. červený tým, složený ze zaměstnanců Úřadu a Masarykovy univerzity v Brně.

Ve dnech 23. a 24. června 2016 proběhlo cvičení kybernetické bezpečnosti Cyber Czech 2016, které uspořádalo NCKB. Jednalo se o netechnické, tzv. Table-Top cvičení, jehož primárním cílem bylo procvičit rozhodovací procesy na strategické úrovni nezbytné pro efektivní řešení krize v kybernetickém prostoru, což zahrnuje i procvičení komunikace a spolupráce mezi zapojenými subjekty. Cvičení navázalo na strategické cvičení, které bylo pořádáno Úřadem ve spolupráci s European Cyber Security Initiative (ECSI) a European Defence Agency (EDA) v červnu 2015.

Ve druhé polovině října pořádal Úřad, ve spolupráci s Ústavem výpočetní techniky Masarykovy univerzity v Brně, další národní cvičení v oblasti kybernetické bezpečnosti CYBER CZECH 2016. Tentokrát se jednalo o technické cvičení, které navazovalo na předchozí Table-Top cvičení z června 2016 a stalo se tak druhým technickým cvičením kybernetické bezpečnosti. Hlavním cílem cvičení bylo, stejně jako v předchozích cvičeních, ověřit praktické znalosti zvládání kybernetických incidentů v souvislosti s ochranou prvků KII a procvičit postupy podle zákona o kybernetické bezpečnosti včetně komunikace s médii při zvládání nastalé krize.

První ročník národního komunikačního cvičení CommCzech se pod záštitou NCKB konal ve dnech 3. a 4. listopadu 2016. Cvičení bylo zaměřeno na ověření průchodnosti neklasifikovaných komunikačních kanálů a aktuálnosti údajů nahlášených povinnými subjekty podle § 16 zákona o kybernetické bezpečnosti. Cvičení se skládalo ze dvou fází. V první proběhla zkouška elektronického spojení s cílem prověřit e-mailové adresy. Na základě rozeslaného e-mailu měly příslušné subjekty maximálně do 48 hodin reagovat a potvrdit jeho přijetí. Druhá fáze probíhala simultánně a ověřovala telefonické kontakty.

2.8.5. Zvyšování povědomí a osvěta

Osvěta a podpora vzdělávání v oblasti kybernetické bezpečnosti patří mezi hlavní oblasti činnosti NCKB. V roce 2016 centrum navázalo na aktivity z předchozího roku, rozvinulo stávající spolupráci a uvedlo nové projekty.

NCKB organizovalo 13. září 2016 již druhý ročník celodenního semináře k zákonu o kybernetické bezpečnosti. Seminář byl pořádán pod záštitou studentské komory Akademického senátu Fakulty podnikatelské Vysokého učení technického v Brně. Letošní ročník měl za cíl informovat veřejnost o novinkách z oblasti činnosti NCKB, tedy zejména se zaměřením na zákon o kybernetické bezpečnosti a na praktické zkušenosti z oboru kybernetické bezpečnosti. Semináře se zúčastnilo okolo 200 účastníků z řad odborné veřejnosti, zástupců povinných subjektů (zejména správců KII a VIS) a studentů.

V rámci aktivit pro veřejnou správu uspořádalo NCKB řadu školení týkajících se pravidel bezpečného využívání ICT technologií v zaměstnání a v soukromí. Jako první proběhlo celodenní školení pro zaměstnance Úřadu vlády ČR. Školení bylo věnováno zaměstnancům na všech stupních vedení a jeho obsahem byly současné hrozby a rizika, význam digitální hygieny, základní bezpečnostní pravidla a možné následky při jejich nedodržování včetně názorné ukázky, co způsobuje např. ransomware či keylogger. Obdobné školení bylo připraveno i pro vedení Ministerstva pro místní rozvoj. Na toto školení navazovala prohlídka pracoviště NCKB s podrobným výkladem k jeho činnosti.

V Moravskoslezském kraji se konalo dvoudenní školení s názvem „Kybernetická bezpečnost v organizacích“. Bylo zaměřeno na management kybernetické bezpečnosti v organizacích a jeho součástí byl rovněž workshop síťové analýzy. Cílovou skupinou byli manažeři IT bezpečnosti, manažeři kybernetické bezpečnosti, IT administrátoři, bezpečnostní architekti, implementátoři ISMS a další role vyplývající ze zákona o kybernetické bezpečnosti. Přednášejícími byli zástupci odboru kybernetických bezpečnostních politik i zástupci odboru vládní CERT. Školení zaznamenalo pozitivní ohlas a bylo o něj zažádáno i na rok 2017.

V několika městech Moravskoslezského kraje proběhla série workshopů z cyklu „Mediální gramotnost pro učitele“ s názvem „Kybernetická bezpečnost: stát, jednotlivec, škola?!“. Obsahem byla současná rizika a hrozby dnešní společnosti v souvislosti s využíváním moderních technologií, jak se změnilo vnímání kybernetické bezpečnosti z pohledu státu a jak se bránit kybernetickým útokům z pohledu jednotlivce. Zde byla účastníkům také představena činnost NCKB, Akční plán k národní strategii kybernetické bezpečnosti a návrh připravované koncepce vzdělávání v problematice kybernetické bezpečnosti, kde byla vyzdvižena potřeba vzdělávání a osvěty široké veřejnosti. Workshopy byly akreditovány Ministerstvem školství, mládeže a tělovýchovy.

Do pilotní fáze projektu Digitální stopa se zapojilo celkem 8 školských zařízení (6 základních škol, 1 základní škola a víceleté gymnázium a 1 víceleté gymnázium) ze 4 krajů (Jihomoravský, Olomoucký, Moravskoslezský, Středočeský). Cílovou skupinou byli žáci 6. a 7. ročníků a modul vždy postupně absolvovaly všechny třídy. Celkem se jej dosud zúčastnilo přibližně 300 žáků. Aktivita byla zaměřena na problematiku rizikového chování a závadového jednání v online prostředí. Ústředním tématem byla kyberšikana, sexting a dalších přidružené sociálně patologické jevy. Žáci zde pracovali s internetem a vybranými sociálními sítěmi. Mezi hlavní zjištění patří nedostatečná znalost funkcí sociálních sítí, zejména nastavení zabezpečení mezi žáky a studenty.

Seznam některých zkratek a pojmů používaných v kapitole 2.8. je uveden v příloze.

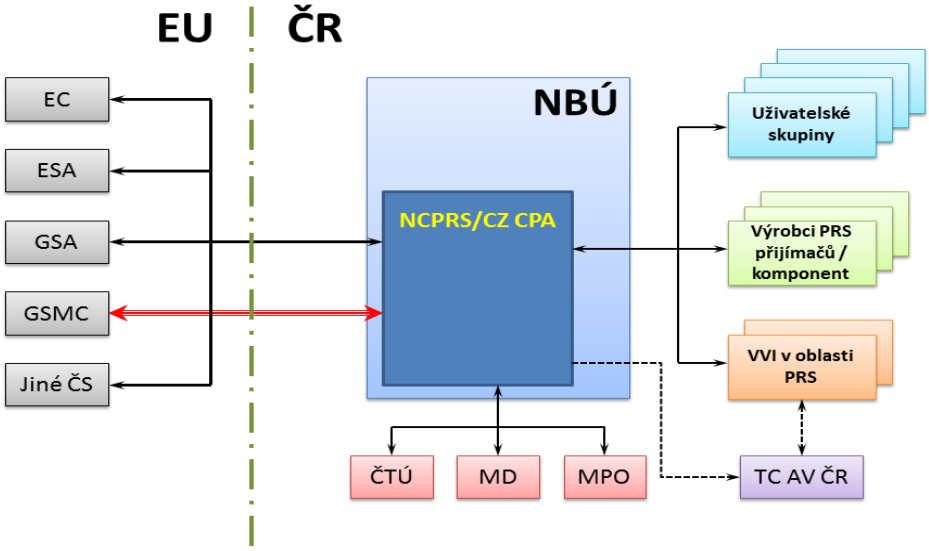
2.9. VÝKON FUNKCE PŘÍSLUŠNÉHO ORGÁNU PRS

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 ke 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 ČR (dále jen „Akční plán PRS“). 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



V roce 2016 probíhala intenzivní mezinárodní příprava společných pilotních projektů pro testování služby PRS v rámci vyhlášeného tendru „Joint Test Activities“, který je v kompetenci Agentury pro evropský GNSS.

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 roce 2015 byl z důvodu zdržení vývoje systému Galileo pozastaven nábor zaměstnanců pro zajištění činnosti NCPRS. Nárůst agendy spojené zejména s řešením problematiky služby PRS na evropské úrovni (akreditace systému pro deklaraci tzv. „Initial Services“, řešení technologických otázek vývoje systému pro dosažení plných operačních schopností a projektů na rozvoj uživatelského segmentu) a zapojení ČR do přípravy a následné realizace pilotních projektů služby PRS, ke kterému došlo v roce 2016, vedl k požadavku na rozšíření pracovního týmu NCPRS.

Personální obsazení bylo řešeno v součinnosti s oddělením personálním a v roce 2016 bylo vyhlášeno výběrové řízení na obsazení dalšího místa, tak aby mohly být efektivně plněny úkoly v kompetenci 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 projektu PRS. Plánovaná realizace tohoto projektu bude uskutečněna v závislosti na dostupné technologii (přijímačů PRS) pravděpodobně až v roce 2018.

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. Na rok 2017 je naplánováno dotazníkové šetření v rámci řešeného projektu FRAME (pilotní projekt GSA pro vývoj a rozšíření uživatelského segmentu PRS).

2.10. OPRAVNÉ PROSTŘEDKY

2.10.1. Bezpečnostní řízení

V roce 2016 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 2016. 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.

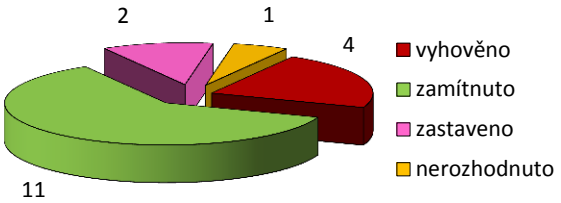
2.10.1.1. Statistické přehledy

2.10.1.1.1. Rozklady

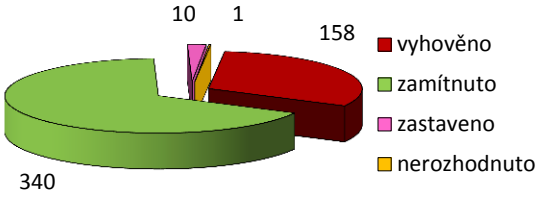
Rozklady proti rozhodnutím Úřadu v oblasti bezpečnostního řízení
(rozhoduje ředitel Úřadu)

Rok	Dosud nerozhodnuto	Vyhověno	Zamítnuto	Zastaveno	Celkem
2015	0	2	29	0	**31**
2016	1	4	11	2	**18**

Řízení o rozkladu v roce 2016



Řízení o rozkladu v letech 2006 až 2016



2.10.1.1.2. Žaloby správní

Žaloby proti rozhodnutím ředitele Úřadu o rozkladu podle zákona v letech 2006 až 2016
(rozhoduje Městský soud v Praze)

Celkem	Dosud nerozhodnuto	Řízení zastaveno	Vyhověno	Zamítnuto	Odmítnuto
106	24	18	13	49	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 2016 *(rozhoduje Nejvyšší správní soud v Brně)*

Celkem	Dosud nerozhodnuto	Řízení zastaveno	Vyhověno	Zamítnuto	Odmítnuto
26	1	0	6	17	2

Kasační stížnosti podané Úřadem proti rozhodnutím Městského soudu v Praze o vyhovění žalobě v letech 2006 až 2016 *(rozhoduje Nejvyšší správní soud v Brně)*

Celkem	Dosud nerozhodnuto	Řízení zastaveno	Vyhověno	Zamítnuto	Odmítnuto
5	0	0	5	0	0

2.10.1.1.4. Ústavní stížnosti

Ústavní stížnosti podané účastníky řízení v letech 2006 až 2016 *(rozhoduje Ústavní soud v Brně)*

Celkem	Dosud nerozhodnuto	Řízení zastaveno	Vyhověno	Zamítnuto	Odmítnuto
5	0	0	0	0	5

2.10.1.1.5. Stížnosti k Evropskému soudu pro lidská práva

Dne 19. října 2016 se konalo před Velkým senátem Evropského soudu pro lidská práva (dále jen „ESLP“) veřejné projednání stížnosti, která se týká rozhodnutí Úřadu o zrušení platnosti osvědčení fyzické osoby a souvisejícího rozhodnutí ředitele Úřadu o zamítnutí rozkladu. (V této věci již v roce 2015 vydal senát ESLP rozsudek, v němž shledal, že v dané věci nedošlo k porušení práva stěžovatele na spravedlivý proces podle čl. 6 odst. 1 Evropské úmluvy o lidských právech. Tento rozsudek však nenabyl právní moci, neboť soud vyhověl žádosti stěžovatele o předložení věci Velkému senátu ESLP). Rozhodnutí Velkého senátu ESLP v této věci lze očekávat v průběhu roku 2017.

2.10.1.2. Hodnocení rozhodovací praxe Úřadu

Jak vyplývá z výše uvedených údajů, v současné době je rozhodnuto v 82 případech o žalobách proti rozhodnutí ředitele Úřadu o rozkladu, přičemž pouze 13 těchto žalob bylo shledáno důvodnými. „Úspěšnost“ ředitele Úřadu tedy činí 84 %.

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 2016 ředitel Úřadu rozhodoval ve 2 případech o opravných prostředcích – rozkladech – uplatněných ze strany fyzických osob ve správním řízení pro porušení povinností v oblasti ochrany utajovaných informací, přičemž jednomu podání bylo ředitelem Úřadu vyhověno a věc byla vrácena Úřadu k novému projednání a v druhém případě bylo rozhodnutí Úřadu změněno ve výši uložené pokuty. 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 2016 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. VÝZKUM A VÝVOJ

2.11.1. Cíle a organizace výzkumu a vývoje

Základním cílem v oblasti výzkumu a vývoje byl neustálý rozvoj bezpečnostních technologií pro ochranu utajovaných informací v komunikačních a informačních systémech. V důsledku turbulentního 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, případně jednotlivé externí odborníky.

2.11.2. Projekty realizované v roce 2016

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 nutné neustálé monitorování a inovace již vyvinutých produktů.

V tomto roce bylo zahájeno 8 nových projektů, u 2 již bylo úspěšně předáno dílo a počátkem roku 2017 proběhne oponentní řízení. Dále bylo řádně dokončeno 6 projektů zahájených v letech 2014 a 2015. Všechny uvedené projekty byly realizovány ve spolupráci s externími řešiteli.

Projekty se věnovaly oblasti kryptografické ochrany, ochrany proti úniku utajovaných informací kompromitujícím vyzařováním a implementaci PRS globálního navigačního systému Galileo.

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

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

V roce 2016 Úřad dále rozvíjel svoji koncepci výzkumu a vývoje v oblasti kryptografické ochrany a ochrany proti úniku utajovaných informací kompromitujícím vyzařováním tak, aby mimo jiné reflektovala požadavky rezortů státní správy, pro které jsou tyto druhy zajištění ochrany utajovaných informací nezbytné.

2.12. 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 pojednává kapitola 2.7.3. O kontrole v oblasti kybernetické bezpečnosti prováděné Úřadem podle § 23 odst. 1 zákona o kybernetické bezpečnosti pojednává kapitola 2.8.3.

2.12.1. Kontroly provedené v roce 2016

Stejně jako v předchozích letech byly i v tomto roce kontroly prováděny na základě průběžně doplňovaných plánů kontrol zpracovávaných na jednotlivá pololetí kalendářního roku a 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 u kontrolovaných osob realizovány, a dále tematické kontroly v oblasti ochrany utajovaných informací, při kterých byly kontrolovány pouze některé vybrané oblasti.

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

V roce 2016 provedl Úřad celkem 82 kontrol, z toho 11 v orgánech státu a jejich složkách, 1 v obecním úřadu a 70 u podnikatelů. Souhrnné údaje o kontrolách a přehled jednotlivých kontrolních akcí realizovaných v roce 2016 jsou uvedeny v následujících tabulkách.

Kontroly provedené v roce 2016

Kontroly	Komplexní	Tematické	Následné	Celkem
Orgány státu	10	1	0	**11**
Krajské a obecní úřady	1	0	0	**1**
Podnikatelé	67	3	0	**70**
Celkem	**78**	**4**	**0**	**82**

Kontroly v orgánech státu a jejich součástech v roce 2016

Kontrolovaná osoba	Kontrolovaná osoba
Celní správa ČR – Generální ředitelství cel	Český telekomunikační úřad
Kancelář Senátu Parlamentu ČR	Ministerstvo průmyslu a obchodu
Ministerstvo vnitra	Ministerstvo vnitra – Generální ředitelství Hasičského záchranného sboru ČR
Ministerstvo zahraničních věcí – zastupitelský úřad ČR v Abú Dhabí	Ministerstvo zahraničních věcí – zastupitelský úřad ČR v Aténách
Ministerstvo zahraničních věcí – zastupitelský úřad ČR v Moskvě	Ministerstvo zahraničních věcí – zastupitelský úřad ČR v Tiraně
Správa základních registrů	

Kontroly v krajských a obecních úřadech v roce 2016

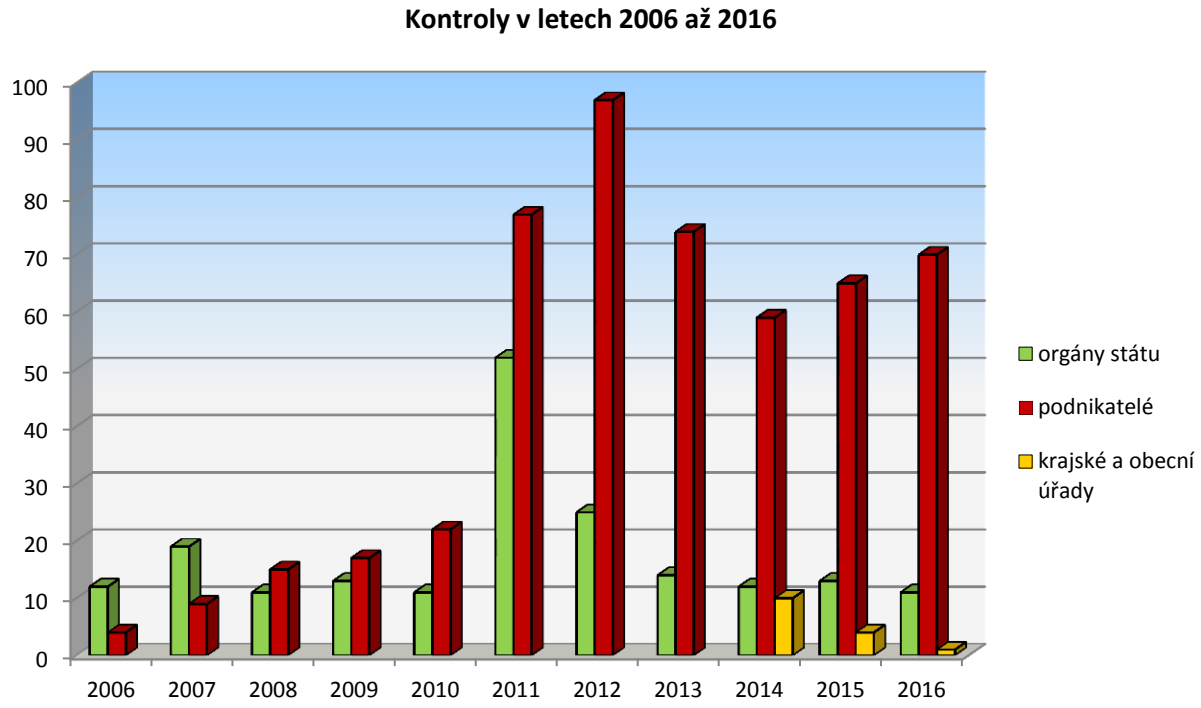
Kontrolovaná osoba
Městský úřad Rokycany

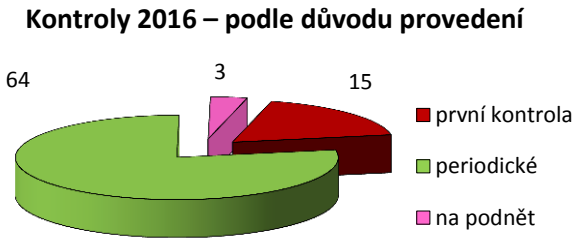
Kontroly u podnikatelů v roce 2016

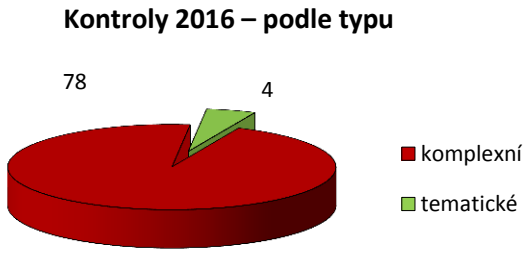
Kontrolovaná osoba	Kontrolovaná osoba
ADASTRA, s.r.o.	ARANEA TECHNOLOGY a.s.
AED project, a.s.	ASD Software, s.r.o.
ALES, s.r.o.	ATELIER PENTA v.o.s.
ALIMEX s.r.o.	AutoCont CZ a.s.

Kontrolovaná osoba	Kontrolovaná osoba
AŽD Praha s.r.o.	PAMÁTKY TÁBOR, s.r.o.
BARA HK spol. s r.o.	PIK s.r.o.
CATEGORY a.s.	PKE ČR s.r.o.
CGI IT Czech Republic s.r.o.	Poličské strojírny a.s.
ComArr, spol. s r.o.	Porr a.s.
COMIMPEX, spol. s r.o.	Pramacom Prague spol. s r.o.
České dráhy, a.s.	PSG-International a.s.
Dálniční stavby Praha, a.s.	RETIA, a.s.
DEFCON s.r.o.	ROGER – security, a.s.
Deloitte Security s.r.o.	S group FACILITY MANAGEMENT, a.s.
Dimension Data Czech Republic s.r.o.	S.ICZ a.s.
ELSO PHILIPS SERVICE spol. s r.o.	Saab Czech s.r.o.
ELTES, s.r.o.	SECURITY TECHNOLOGIES a.s.
ELTODO, a.s.	SEOS CZ s.r.o.
EMV s.r.o.	SOFIM, spol. s r.o.
ERICSSON spol. s r.o.	STAEG Stavby, spol. s r.o.
Explosia a.s.	STREICHER, spol. s r.o. Plzeň
EZH, a.s.	SUDOP Project Plzeň a.s.
F.S.C. BEZPEČNOSTNÍ PORADENSTVÍ, a.s.	TECHNISERV IT, spol. s r.o.
GEFOS a.s.	TECHNISERV, spol. s r.o.
I&C Energo a.s.	TELESPOJ, s.r.o.
ICZ a.s.	TESCO SW a.s.
INGBAU CZ s.r.o.	TESLA, akciová společnost
Ivo Menšík	Trade FIDES, a.s.
LEC s.r.o.	TRIGON PLUS spol. s r.o.
Letiště Praha, a. s.	Triocom s.r.o.
M – SILNICE a.s.	TTC TELEKOMUNIKACE, s.r.o.
MAXPROGRES, s.r.o.	ÚJV Řež, a. s.
MICROSOFT s.r.o.	VCES a.s.
NAM system, a.s.	Vojenský výzkumný ústav, s. p.
ORZO SECURITY, spol. s r.o.	Z.L.D. s.r.o.

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 2016 byly nedostatky zjištěny v 56 případech (68,3 %). Ve 12 případech (14,6 %) 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. Příčinou nedostatků bylo ve většině případů selhání lidského činitele. Při kontrolách provedených v roce 2016 byly zjištěny zejména následující nedostatky:

Obecné nedostatky

- neobsazení funkce bezpečnostního ředitele,
- nesplnění některé z podmínek pro výkon funkce bezpečnostního ředitele,

- nevytvoření podmínek pro zajištění ochrany utajovaných informací,
- nesoulad postupu stanoveného vnitřním předpisem pro manipulaci s utajovanými dokumenty s platnou právní úpravou (neaktuální vnitřní předpisy),
- nevedení evidence neoprávněného nakládání s utajovanou informací,
- neoznámení porušení povinností při ochraně utajovaných informací Úřadu.

Personální bezpečnost

- přístup k utajované informaci zjištěný u fyzické osoby, která nesplňovala některou ze zákonem stanovených podmínek pro tento přístup (neprovedení poučení, absence oznámení o splnění podmínek pro přístup k utajované informaci stupně utajení Vyhrazené nebo osvědčení fyzické osoby, případně dokladu),
- 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 proškolení 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,
- nezpracování přehledu pracovních míst a funkcí, na kterých je nezbytné mít přístup k utajované informaci,
- nevedení nebo 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, 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),
- formální nedostatky vyhotovených písemných dokladů (chybějící nebo nesprávné údaje na výtisku poučení nebo oznámení, poučení nebo oznámení neodpovídalo vzoru stanovenému platnou právní úpravou, prohlášení o způsobilosti k právním úkonům předkládaná místo prohlášení o svéprávnosti).

Průmyslová bezpečnost

- poskytnutí utajované informace podnikateli, který nesplňoval zákonem stanovené podmínky pro tento přístup,
- přístup podnikatele k utajované informaci formou, pro kterou nesplňoval zákonem stanovené podmínky (absence příslušného osvědčení podnikatele),

- nedostatky v bezpečnostní dokumentaci podnikatele (neúplná dokumentace).

Administrativní bezpečnost

- chybějící utajovaný dokument (později byl dohledán),

- 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, nevyhotovení kontrolního listu, neuvedení všech osob, které se seznámily s obsahem utajovaného dokumentu, v kontrolním listu),

- používání administrativních pomůcek, které neodpovídaly požadavkům stanoveným právními předpisy (autentizace, formální a obsahové nedostatky),

- neevidování utajovaného dokumentu,

- nedostatky ve vedení evidence administrativních pomůcek (nedostatečné nebo chybné údaje),

- 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, při ukládání vyřízených utajovaných dokumentů, při přepravě, neuvádění záznamu o odpojení příloh, rozdělovníku a záznamu, nepředání utajovaných dokumentů proti potvrzení, neuvádění údajů o skartaci utajovaných dokumentů).

Činnost registrů utajovaných informací

- nedostatky v evidenci utajovaných dokumentů cizí moci (evidenční označení přidělovaná utajovaným dokumentům, neúplné nebo nesprávné zápisy v jednacím protokolu).

Fyzická bezpečnost

- neplnění povinností stanovených v oblasti fyzické bezpečnosti právními předpisy (nezpracování projektu fyzické bezpečnosti),

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

- nedostatky v realizaci opatření fyzické bezpečnosti (chybná funkce použitých technických prostředků, nesprávná instalace technických prostředků),

- nesoulad skutečného stavu opatření fyzické bezpečnosti se stavem deklarovaným v projektu fyzické bezpečnosti (nesprávné bodové hodnocení jednotlivých opatření a technických prostředků v projektu, režim manipulace s klíči od zabezpečených oblastí a úschovných objektů),

- ukládání utajovaných informací mimo zabezpečené oblasti.

Bezpečnost informačních a komunikačních systémů

- nesplnění požadavků na konfiguraci a provoz informačního systému (nepodporovaný antivirový SW, zastaralý operační systém, nefunkčnost komponent informačního systému nebo SW),

- nesplnění požadavků na instalaci informačního systému z hlediska fyzické bezpečnosti (zabezpečená oblast, ve které je instalován informační systém, nesplňovala minimální požadavky pro danou kategorii),

- nedostatky v evidenci provozních médií informačního systému (zdvojená evidence).

Kryptografická ochrana

- nedostatky v provozu kryptografického prostředku (nesplnění požadavků uvedených v certifikační zprávě),

- nedostatky ve vedení administrativních pomůcek kryptografické ochrany (chybějící údaje v evidenci pracovníků kryptografické ochrany).

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 zpětné vazby, která je využívána například při přípravě novelizací právních předpisů v působnosti Úřadu. V rámci metodické činnosti vůči orgánům státu i podnikatelům majícím přístup k utajovaným informacím se Úřad zaměřuje na identifikované 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 2016 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 2016. 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 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 2016 byla vydána 2 pravidelná čísla.

Ve Věstníku Úřadu jsou 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. Obsahem Věstníku Úřadu jsou rovněž aktuální seznamy podnikatelů, kterým bylo vydáno osvědčení podnikatele, certifikovaných kryptografických prostředků a certifikovaných technických prostředků.

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. Na internetových stránkách jsou dále zveřejňovány 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. Na internetových stránkách jsou dále dostupná jednotlivá čísla Věstníku Úřadu (od roku 2011) a výroční zprávy o činnosti 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 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 2016 bylo Úřadu podáno 14 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 2016 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 2016 prováděla, v rámci plnění dlouhodobých úkolů, činnosti související s výkonem interní kontroly určených oblastí působnosti Úřadu.

V roce 2016 inspekce ředitele Úřadu řešila 2 podání – stížnosti, které byly vyhodnoceny jako nedůvodné.

3. BEZPEČNOSTNÍ, EKONOMICKÉ A PERSONÁLNÍ ZABEZPEČENÍ ÚŘADU

3.1.OCHRANA UTAJOVANÝCH INFORMACÍ A KRIZOVÉ ŘÍZENÍ V ÚŘADU

3.1.1. Vnitřní kontrola ochrany utajovaných informací

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

V roce 2016 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.

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 2016 nebylo zjištěno závažné porušení ochrany utajovaných informací zaměstnanci Úřadu. Rovněž ustanovení provozního řádu byla v roce 2016 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 2016 bylo evidováno 100 žádostí o vydání osvědčení fyzické osoby, vydáno bylo 103 osvědčení fyzické osoby včetně ukončených bezpečnostních řízení zahájených již v roce 2015.

Vydaná osvědčení fyzické osoby v rámci Úřadu v roce 2016

Důvěrné	18
Tajné	68
Přísně tajné	17
Celkem	**103**

Důvody zániku platnosti osvědčení fyzické osoby v rámci Úřadu v roce 2016

Doručení nového osvědčení	68
Změna některého z údajů uvedených v osvědčení	4
Vráceno uživatelem	1
Celkem	**73**

Vydaná osvědčení fyzické osoby pro cizí moc v rámci Úřadu v roce 2016

COSMIC TOP SECRET ATOMAL	1
COSMIC TOP SECRET	11
NATO SECRET	24
Celkem	**36**

V roce 2016 bylo dále vydáno 13 oznámení o splnění podmínek pro přístup k utajované informaci stupně utajení Vyhrazené.

3.1.3. Fyzická bezpečnost v rámci Úřadu

V roce 2016 byla provedena modernizace elektronické kontroly vstupu pro objekty areálu Úřadu v Praze.

3.1.4. Krizové řízení v rámci Úřadu

V roce 2016 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. V listopadu 2016 byla Generálním ředitelstvím Hasičského záchranného sboru provedena v Úřadu kontrola v oblasti krizového řízení.

3.1.5. Ostatní činnosti

Odbor bezpečnostní zajišťuje rovněž evidenční ochranu zaměstnanců Úřadu v případě jejich ohrožení v souvislosti s výkonem povolání. V roce 2016 byla opakovaně prováděna periodická aktualizace seznamu chráněných osob.

V rámci bezpečnostní agendy boje proti korupci byla v roce 2016 vytvořena analýza korupčních rizik, která slouží k aktualizaci Interního protikorupčního programu Úřadu, který byl rovněž aktualizován.

V rámci zajišťování provozu vozového parku v Úřadu nebyl v roce 2016 proveden nákup motorových vozidel. V průběhu roku 2016 byl ukončen 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 2016 bylo provedeno 15 archivních prohlídek. Celkový rozsah archiválií je v bezpečnostním archivu 10,62 běžných metrů a ve specializovaném archivu 18,44 běžných metrů. V roce 2016 navštívil bezpečnostní archiv 1 externí badatel a specializovaný archiv 1 interní badatel.

V roce 2016 byla zpracována analýza současného stavu Archivu a návrh řešení výstavby digitálního archivu. Uvedené dokumenty budou využity při výstavbě specializovaného a bezpečnostního digitálního archivu v roce 2017.

3.3. EKONOMICKÉ ZABEZPEČENÍ ÚŘADU

Úřad je od 1. listopadu 1998 samostatnou kapitolou státního rozpočtu „308“. V roce 2016 byla jeho činnost financována výhradně ze státního rozpočtu. Konečný rozpočet výdajů v tomto roce činil po rozpočtových opatřeních 460 269,9 tis. Kč. Čerpání k 31. prosinci 2016 bylo na úrovni 80,6 %.

Příjmovou část státního rozpočtu naplnila kapitola v roce 2016 ve výši 1 304,5 tis. Kč, a to zejména úhradou správních poplatků ve výši 275 tis. Kč, vybranými pokutami ve výši 159 tis. Kč, příjmem z licenční smlouvy ve výši 380 tis. Kč a nahodilými příjmy, jako jsou přeplatky z minulých let ve výši 388 tis. Kč a prodej hmotného majetku (vyřazené osobní automobily) ve výši 86 tis. Kč a ostatní drobné příjmy ve výši 16,5 tis. Kč.

Rozpočet roku 2016 byl posílen o nároky nespotřebovaných výdajů roku 2015 ve výši 83 028,5 tis. Kč. Důvodem jejich nevyužití v investiční části rozpočtu byl zejména fakt, že z důvodu časově náročného stavebního řízení nedošlo v roce 2016 k realizaci projektu z roku 2014 – přístavba budovy NCKB v Brně. Záměrem bylo rozšíření o zabezpečený jednací sál v hodnotě stavební investice ve výši 18 654,38 tis. Kč. Dále bylo na základě rozhodnutí vlády odloženo plnění úkolů souvisejících s implementací služby PRS, tím nebyly realizovány plánované investiční nákupy ve výši 7 380,6 tis. Kč. Zbývající nároky nespotřebovaných výdajů byly určeny na pokrytí akcí v rámci rozvoje informačních technologií a softwaru, na které byly vypsány veřejné zakázky v roce 2015 a realizace proběhla až následující rok.

Rozpočet roku 2016 byl čerpán ve výši 371 137,4 tis. Kč. Největší objem běžných výdajů tvořily mzdové výdaje a zákonem dané odvody ve výši 224 201,7 tis. Kč. O nevyužité mzdové prostředky z nenaplněných tabulek NCPRS, které není zatím plně funkční, bude požádáno Ministerstvo financí, aby částečně pokryly mzdové náklady v souladu s plněním nových úkolů Úřadu v roce 2017.

Běžné výdaje na provoz, zejména platby v oblasti energií, nezbytných služeb a nákupů k zajištění činnosti Úřadu, NCKB a NCPRS, činily po rozpočtových změnách 107 230,3 tis. Kč a byly čerpány vlivem vývoje cen v rámci veřejných zakázek a úsporných opatření ve výši 87 946,2 tis. Kč, což je na úrovni 81 %.

Kapitálové výdaje byly čerpány v celkové výši 58 989,4 tis. Kč, tj. včetně upotřebených nároků nespotřebovaných výdajů roku 2015. Nejvyšší výdaje byly v rámci budování NCKB, kdy na informační technologie a programové vybavení bylo vyčerpáno 26 095,6 tis. Kč a na projekty výzkumu a vývoje se vydalo 19 171 tis. Kč.

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 24 097,6 tis. Kč včetně NNV. Vyčerpáno bylo 20 398,7 tis. Kč a nejvyšší objem – 19 171,1 tis. Kč činily smluvní závazky s externími řešiteli v rámci výzkumných projektů.

Rozpočet Úřadu lze považovat již po několik let v rámci meziročního nárůstu výdajů za stabilizovaný a k navýšení rozpočtu dochází pouze u financování nově svěřených činností na základě nových usnesení vlády ČR jako bylo usnesení č. 520/2015, o posílení kapacity Národního bezpečnostního úřadu v oblasti kybernetické bezpečnosti v letech 2016 až 2018, a dále usnesení vlády ČR č. 1034/2015, o schválení personálních projektů ministerstev a dalších ústředních správních úřadů, zpracovaných podle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

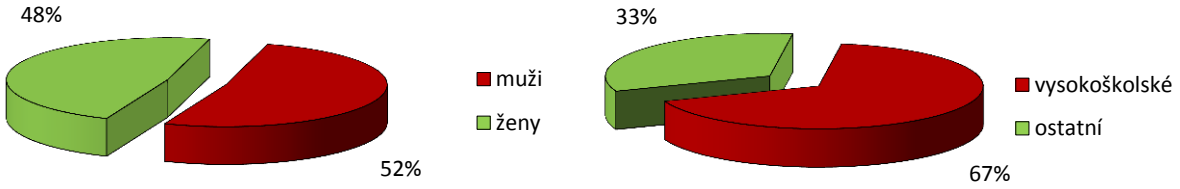
Využívání svěřených finančních prostředků bylo i v roce 2016 v souladu s činnostmi, které jsou Úřadu vymezeny zákonem a zákonem o kybernetické bezpečnosti. Čerpání rozpočtu, rozpočtová opatření a nové záměry projednávala pravidelně i v roce 2016 komise pro hospodaření s finančními prostředky Úřadu. Veškeré výdaje vždy 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

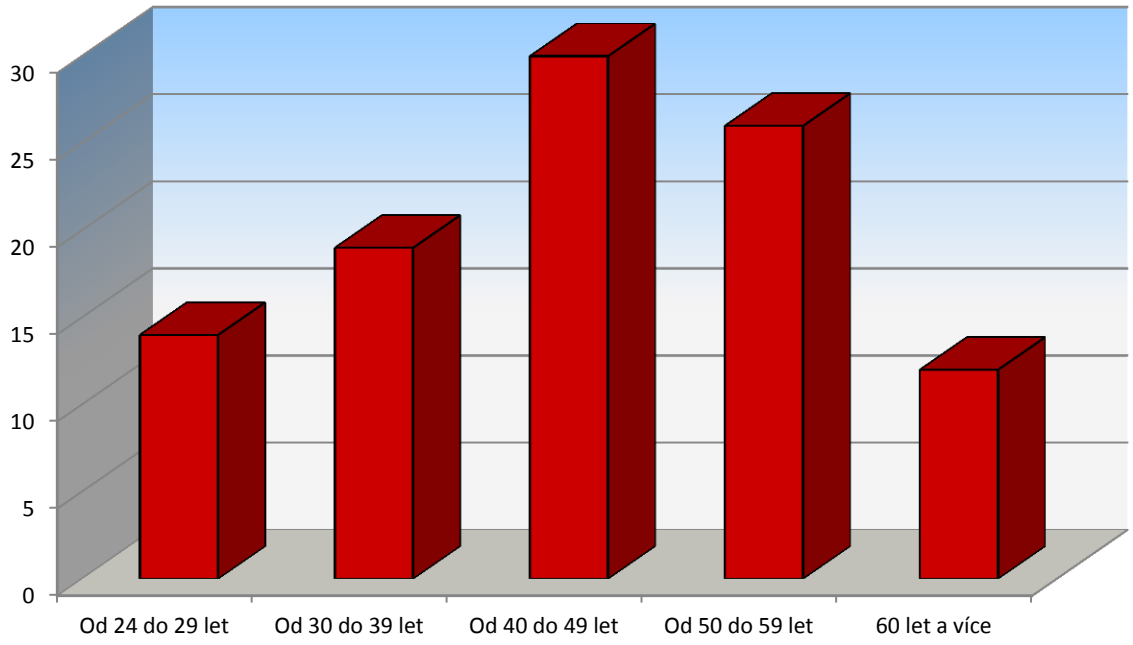
Pro rok 2016 měl Úřad systemizovaných 335 pracovních míst, z tohoto počtu bylo 46 míst určeno pro NCKB, resp. problematiku kybernetické bezpečnosti, a 7 míst pro NCPRS. V průběhu roku byla všechna pracovní místa v NCKB obsazována novými, převážně mladými odborníky. Dále se rozvíjí spolupráce s vysokými školami a dalšími subjekty působícími v této oblasti.

K 31. prosinci 2016 bylo aktuálně obsazeno 319 pracovních míst, z toho bylo 166 mužů a 153 žen. 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 %)



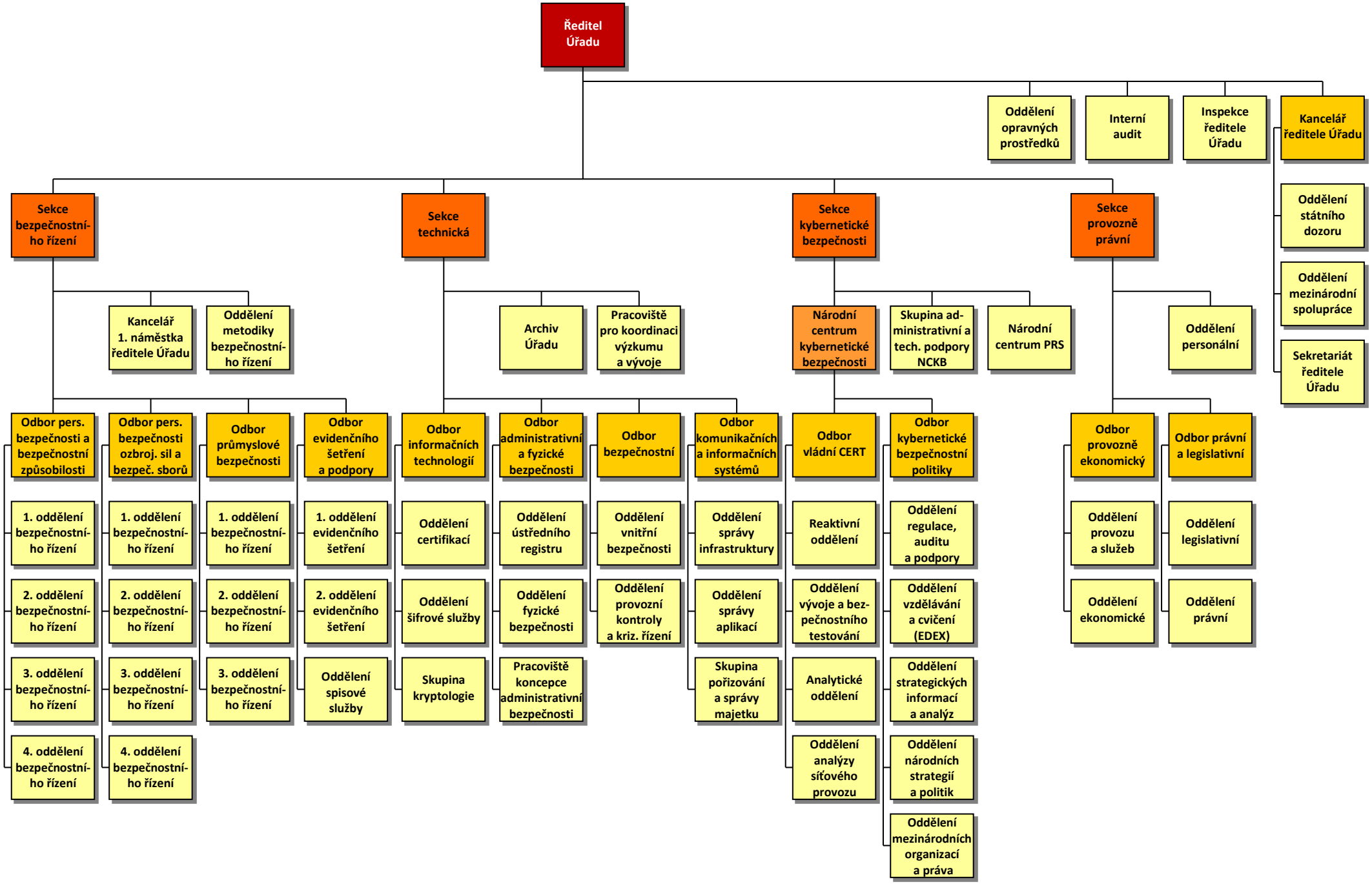
V Úřadu je průběžně realizován systém vzdělávání zaměstnanců. V roce 2016 pokračovalo skupinové i individuální jazykové vzdělávání, kterého se pravidelně účastní více než 80 zaměstnanců.

V roce 2016 byla realizována odborná školení pro technické a odborné specialisty, 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 2016 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.).

Rovněž byla věnována pozornost zdokonalení komunikačních dovedností zaměstnanců, kteří přicházejí do kontaktu s veřejností (podatelna, zaměstnanci zařazení v odboru evidenčního šetření a podpory). Školení byla účastníky hodnocena velmi kladně, s velkým přínosem pro praxi.

Zaměstnanci měli možnost vzdělávat se v oblastech, které bezprostředně souvisejí s jejich pracovními činnostmi, tj. především v oblasti práva soukromého a veřejného, v oblasti účetnictví a auditu. Možnost odborného a jazykového vzdělávání zaměstnanců je jedním z motivačních prvků, které Úřad využívá.

Organizační schéma Úřadu k 31. 12. 2016



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

CCDCoE – Cooperative Cyber Defence Centre of Excellence

CERT – Computer Emergency Response Team

CSIRT – Computer Security Incident Response Team

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

ENISA – European Union Agency for Network and Information Security (Evropská agentura pro bezpečnost sítí a informací)

EU – Evropská unie

GovCERT.CZ – vládní CERT sloužící jako koordinační místo pro okamžitou reakci na kybernetické bezpečnostní incidenty; je organizační složkou Úřadu, resp. specializovaným pracovištěm NCKB

Honeypot – návnada lákající útočníka; po zachycení potencionálně nebezpečného software dochází k jeho automatizované analýze

KII – kritická informační infrastruktura

NATO – North Atlantic Treaty Organization (Organizace Severoatlantické smlouvy)

NIS – Directive on security of network and information systems

NCKB – Národní centrum kybernetické bezpečnosti

OECD – Organisation for Economic Co-operation and Development (Organizace pro hospodářskou spolupráci a rozvoj)

TABLE-TOP – cvičení navržené k testování teoretických schopností cvičících ve skupině reagovat na krizovou situaci; výhodu tohoto druhu cvičení představuje možnost vyzkoušet si jakoukoliv hypotetickou situaci bez rizika způsobení škody a dalších 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 2016	7
2.2.1.2.	Výhled na rok 2017	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	8
2.3.	PERSONÁLNÍ BEZPEČNOST	10
2.3.1.	Bezpečnostní řízení o žádostech fyzických osob	11
2.3.2.	Prověřování splňování podmínek po vydání osvědčení fyzické osoby	11
2.3.3.	Analýza důvodů nevydání nebo zrušení platnosti osvědčení fyzické osoby	12
2.3.4.	Přehled ostatních důvodů zániku platnosti osvědčení fyzické osoby	12
2.3.5.	Statistické přehledy	13
2.3.6.	Personální projekt	17
2.4.	BEZPEČNOSTNÍ ZPŮSOBILOST	18
2.4.1.	Statistické přehledy	18
2.5.	PRŮMYSLOVÁ BEZPEČNOST	19
2.5.1.	Bezpečnostní řízení o žádostech podnikatelů	19
2.5.2.	Prověřování splňování podmínek po vydání osvědčení podnikatele	19
2.5.3.	Analýza důvodů nevydání nebo zrušení platnosti osvědčení podnikatele	20
2.5.4.	Přehled ostatních důvodů zániku platnosti osvědčení podnikatele	20
2.5.5.	Statistické přehledy	20
2.6.	BEZPEČNOST INFORMAČNÍCH A KOMUNIKAČNÍCH SYSTÉMŮ A KRYPTOGRAFICKÁ OCHRANA	22
2.6.1.	Certifikační a akreditační činnost	23
2.6.1.1.	Certifikace a akreditace informačních systémů	23
2.6.1.2.	Certifikace kryptografických prostředků	25
2.6.1.3.	Certifikace kryptografických pracovišť	27
2.6.1.4.	Certifikace stínicích komor	28
2.6.2.	Další odborná činnost	29
2.6.2.1.	Výroba kryptografického materiálu	29
2.6.2.2.	Měření kompromitujícího vyzařování (TEMPEST)	29

2.6.2.2.1. TEMPEST měření elektronických zařízení 29
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 30
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 31
2.7. ADMINISTRATIVNÍ A FYZICKÁ BEZPEČNOST, ÚSTŘEDNÍ REGISTR 32
2.7.1. Administrativní bezpečnost 32
2.7.2. Fyzická bezpečnost 33
2.7.2.1. Certifikace technických prostředků 34
2.7.2.2. Posuzování bezpečnostní dokumentace podnikatele z hlediska fyzické bezpečnosti 36
2.7.2.3. Problémové oblasti fyzické bezpečnosti 37
2.7.3. Ústřední registr 37
2.8. KYBERNETICKÁ BEZPEČNOST 39
2.8.1. Budování NCKB/GovCERT.CZ 40
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 41
2.8.4. Spolupráce Úřadu v oblasti kybernetické bezpečnosti 42
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 45
2.10. OPRAVNÉ PROSTŘEDKY 46
2.10.1. Bezpečnostní řízení 46
2.10.1.1. Statistické přehledy 46
2.10.1.1.1. Rozklady 46
2.10.1.1.2. Žaloby správní 47
2.10.1.1.3. Kasační stížnosti 47
2.10.1.1.4. Ústavní stížnosti 47
2.10.1.1.5. Stížnosti k Evropskému soudu pro lidská práva 47
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. VÝZKUM A VÝVOJ 48
2.11.1. Cíle a organizace výzkumu a vývoje 48
2.11.2. Projekty realizované v roce 2016 48
2.12. STÁTNÍ DOZOR 49
2.12.1. Kontroly provedené v roce 2016 49
2.12.2. Výsledky kontrol 52
2.13. METODICKÁ ČINNOST ÚŘADU 55

2.13.1.	Metodická činnost v oblasti bezpečnostního řízení	56
2.14.	VĚSTNÍK ÚŘADU A INTERNETOVÉ STRÁNKY ÚŘADU	56
2.14.1.	Věstník Úřadu	56
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	58
3.1.	OCHRANA UTAJOVANÝCH INFORMACÍ A KRIZOVÉ ŘÍZENÍ V ÚŘADU	58
3.1.1.	Vnitřní kontrola ochrany utajovaných informací	58
3.1.2.	Personální bezpečnost v rámci Úřadu	59
3.1.3.	Fyzická bezpečnost v rámci Úřadu	59
3.1.4.	Krizové řízení v rámci Úřadu	60
3.1.5.	Ostatní činnosti	60
3.2.	ARCHIV NÁRODNÍHO BEZPEČNOSTNÍHO ÚŘADU	60
3.3.	EKONOMICKÉ ZABEZPEČENÍ ÚŘADU	61
3.4.	PERSONÁLNÍ ZABEZPEČENÍ ÚŘADU	62
Příloha	Seznam některých zkratek a pojmů použitých v textu k oblasti kybernetické bezpečnosti	65