NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

ZPRÁVA

O ČINNOSTI

NÁRODNÍHO ÚŘADU PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST

ZA ROK 2017

Praha 2018

Obsah

1. ÚVOD

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) je ústředním správním orgánem pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany. Dále má na starosti problematiku neveřejné služby v rámci družicového systému Galileo. Vznikl 1. srpna 2017 na základě zákona číslo 205/2017 Sb., kterým se změnil zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).

Hlavní oblasti činnosti NÚKIB:

- provozovat Vládní CERT České republiky (GovCERT.CZ)
- spolupráce s ostatními národními CERT® týmy a CSIRT týmy
- spolupráce s mezinárodními CERT® týmy a CSIRT týmy
- příprava bezpečnostních standardů pro informační systémy KII a VIS
- osvěta a podpora vzdělávání v oblasti kybernetické bezpečnosti
- výzkum a vývoj v oblasti kybernetické bezpečnosti
- ochrana utajovaných informací v oblasti informačních komunikačních systémů
- kryptografická ochrana
- národní kontaktní místo PRS - jedna ze služeb evropského satelitního systému Galileo (NCPRS)

2. ČINNOST ÚŘADU

Tato zpráva popisuje činnost NÚKIB ve všech oblastech s výjimkou kybernetické bezpečnosti, která je obsažena ve Zprávě o stavu kybernetické bezpečnosti České republiky za rok 2017.

2.1. LEGISLATIVNÍ A PRÁVNÍ ČINNOST ÚŘADU

2.1.1. Vnitřní legislativní činnost

Zákonem č. 205/2017 Sb., kterým byl novelizován zákon o kybernetické bezpečnosti a na základě kterého Úřad vznikl, byly do zákona o kybernetické bezpečnosti zavedeny nové povinné subjekty, a to správce a provozovatel informačního systému základní služby, provozovatel základní služby a poskytovatel digitální služby. Tím se rozšířila jak tzv. constituency Úřadu, tak také jeho legislativní pravomoc. Podle § 28 odst. 2 písm. e) zákona o kybernetické bezpečnosti je s účinností uvedené novely úkolem Úřadu stanovit vyhláškou dopadová a odvětvová kritéria pro určení provozovatele základní služby a vymezení významnosti dopadu

narušení základní služby na zabezpečení společenských nebo ekonomických činností. Tento svůj úkol Úřad splnil přijetím vyhlášky č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby. Tato vyhláška stanoví kritéria pro odvětví energetiky, dopravy, bankovnictví, infrastruktury finančních trhů, zdravotnictví, vodního hospodářství, digitální infrastruktury a chemického průmyslu.

Zohlednit zařazení nových povinných subjektů do rozsahu regulace zákona o kybernetické bezpečnosti a také reagovat na požadavky praxe je cílem návrhu nové vyhlášky o kybernetické bezpečnosti. Tato zcela nová vyhláška, která má nahradit vyhlášku č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti), je připravována v úzké spolupráci se zástupci jiných správních úřadů i odborné veřejnosti od poloviny roku 2017.

Úřad v období od srpna do prosince 2017 vyjádřil své stanovisko v rámci mezirezortního připomínkového řízení k několika desítkám návrhů právních předpisů i materiálů nelegislativní povahy předkládaných ministerstvy nebo jinými ústředními správními úřady. V souvislosti s přijetím obecného nařízení o ochraně osobních údajů (GDPR) Úřad v rámci meziresortní spolupráce připravil text novelizace zákona o kybernetické bezpečnosti, který se následně stal součástí návrhu zákona předkládaného vládě Ministerstvem vnitra.

Poskytování informací podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím za rok 2017

Počet podaných žádostí o informace podle zákona č. 106/1999 Sb. a počet vydaných rozhodnutí o odmítnutí žádosti: oblast - počet podaných žádostí/počet vydaných rozhodnutí

- Kybernetická bezpečnost - 2/1
- Všeobecné - 1/0
- Celkem - 3/1

Počet podaných odvolání proti rozhodnutím Úřadu podle zákona č. 106/1999 Sb.

- 0 odvolání

Počet podaných stížností na postup při vyřizování žádosti podle zákona č. 106/1999 Sb.:

- 0 stížností

Rozsudky soudu ve vztahu k Úřadu v oblasti poskytování informací:

- Žádný rozsudek.

Výsledky řízení o sankcích za nedodržování zákona č. 106/1999 Sb.:

- Nebylo vedeno žádné řízení.

Výčet poskytnutých výhradních licencí:

- Nebyla poskytnuta žádná výhradní licence.

2.1.2. Správní řízení

Jednou z působností Úřadu je ukládání správních trestů za nedodržení povinností stanovených zákonem o kybernetické bezpečnosti. Do působnosti Úřadu přitom spadá nejen projednávání přestupků podle § 25 a násl. zákona o kybernetické bezpečnosti, ale zároveň i vybírání pokut, jenž Úřad v rozhodnutí o spáchání přestupku povinnému subjektu uloží. Vybírání pokut je přitom samostatným úkonem nad rámec vlastního správního řízení o přestupku, které může v případě nezaplacení sankce vyústit až v exekuční řízení. Úřad v roce 2017 nevedl žádné správní řízení na porušení povinností dle zákona o kybernetické bezpečnosti.

Úřad rovněž projednává přestupky podle části osmé zákona o ochraně utajovaných informací, avšak to pouze dílem, neboť řada přestupků podle jmenovaného zákona zůstala v gesci Národního bezpečnostního úřadu. I podle zákona o ochraně utajovaných informací platí, že Úřad pokuty nejen ukládá, ale tyto zároveň i vybírá.

V druhé polovině roku 2017 bylo Úřadu v rámci delimitace z Národního bezpečnostního úřadu postoupeno 6 podnětů k prošetření, z nichž se všechny dotýkaly zákona o ochraně utajovaných informací. Z hlediska konkrétního údajného pochybení, které má Úřad posoudit, se pak především jednalo o nevhodné nakládání s utajovanou informací. Prošetřování důvodnosti těchto podnětů nebylo do konce roku 2017 ukončeno.

2.2. BEZPEČNOST INFORMAČNÍCH A KOMUNIKAČNÍCH SYSTÉMŮ A KRYPTOGRAFICKÁ OCHRANA

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

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

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

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

Od 1. 8. 2017 došlo k oddělení Národního úřadu pro kybernetickou a informační bezpečnost. V rámci tohoto oddělení došlo ke spisové odluce, v rámci které bylo předáno více než 18 tisíc čísel jednacích listinných dokumentů, více než 5 tisíc čísel jednacích elektronických dokumentů a více než 750 čísel jednacích dokumentů KRYPTO.

2.2.1. 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.

2.2.1.1. Certifikace a akreditace informačních systémů

V roce 2017 probíhalo řízení o certifikaci 170 informačních systémů. K 50 žádostem o certifikaci informačního systému, jejichž zpracování bylo zahájeno v předchozím roce, přibylo v roce 2017 dalších 120 žádostí, a to 50 ze státní správy nebo samosprávy a 70 ze soukromé sféry. Ve většině případů se jednalo o žádosti o opakovanou certifikaci již provozovaných informačních systémů. Ve 41 případech byla podána žádost o certifikaci nově budovaného informačního systému, přičemž pouze 8 z těchto žádostí pochází ze státní správy.

V uvedeném roce bylo vydáno celkem 111 certifikátů informačních systémů, z toho 53 pro žadatele ze státní správy nebo samosprávy a 58 ze soukromé sféry.

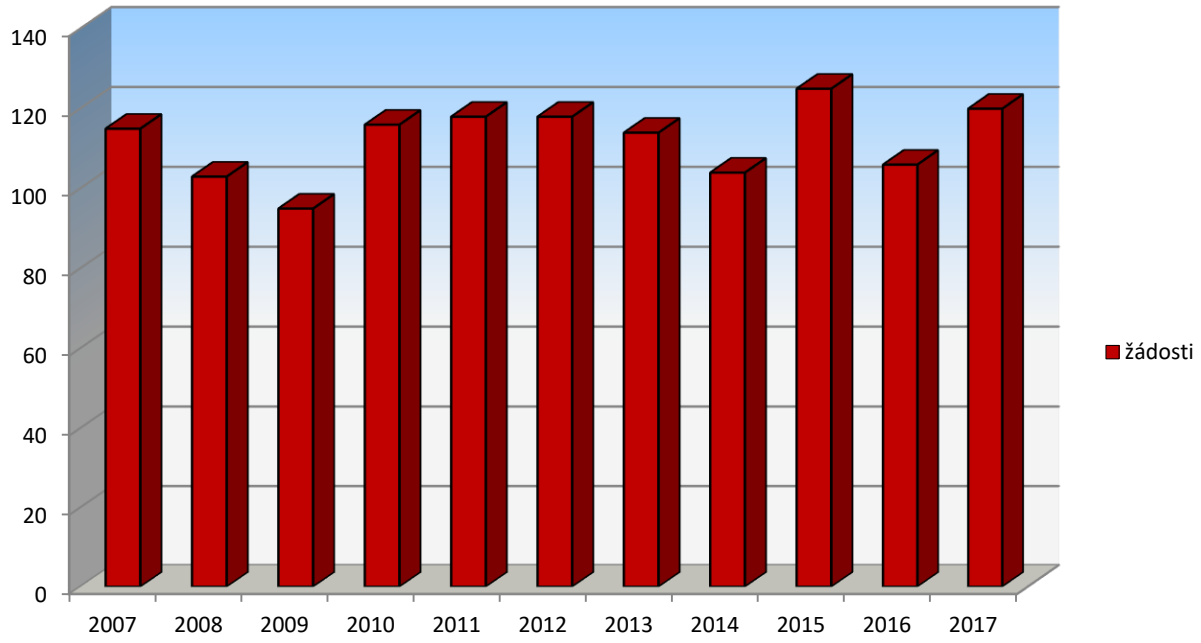
Celkem 69 certifikátů informačních systémů bylo vydáno na žádost podanou v roce 2017.

V 11 případech provozovatel informačního systému s certifikátem platným do data spadajícího do roku 2017 nepožádal o opakovanou certifikaci a platnost certifikátu automaticky skončila.

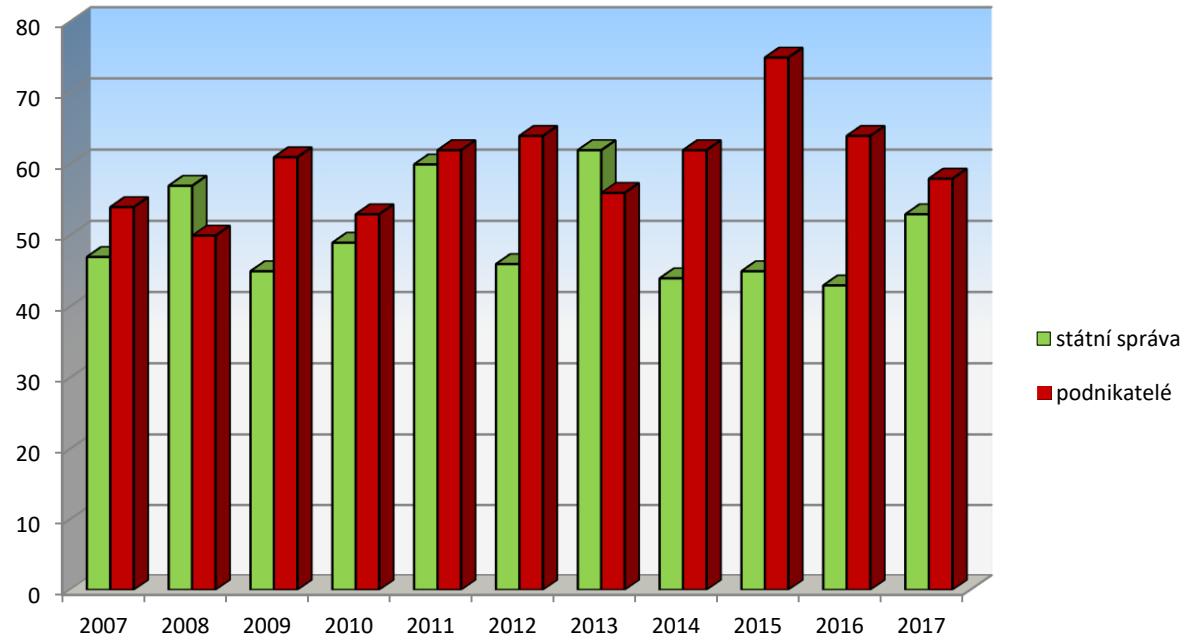
Certifikace informačních systémů v roce 2017

Řešené žádosti v roce 2017	Vydané certifikáty podle stupně utajení				Vydané certifikáty	
	Vyhrazené	Důvěrné	Tajné	Přísně tajné	státní správa	Podnikatelé
170	24,8 %	41,3 %	31,4 %	2,5 %	53	58

Přijaté žádosti o certifikaci informačního systému v letech 2007 až 2017



Vydané certifikáty informačních systémů v letech 2007 až 2017



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 2017 přibylo 8 žádostí o certifikaci nově budovaného informačního systému ze státní správy a 33 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 2017, 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 2017 Úřad provedl pro rezorty Ministerstva obrany, Ministerstva vnitra, Ministerstva zahraničních věcí a Bezpečnostní informační služby národní akreditaci 11 součinnostních systémů NATO a 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.

V roce 2017 byla na území ČR zahájena výstavba 3 nových součinnostních systémů.

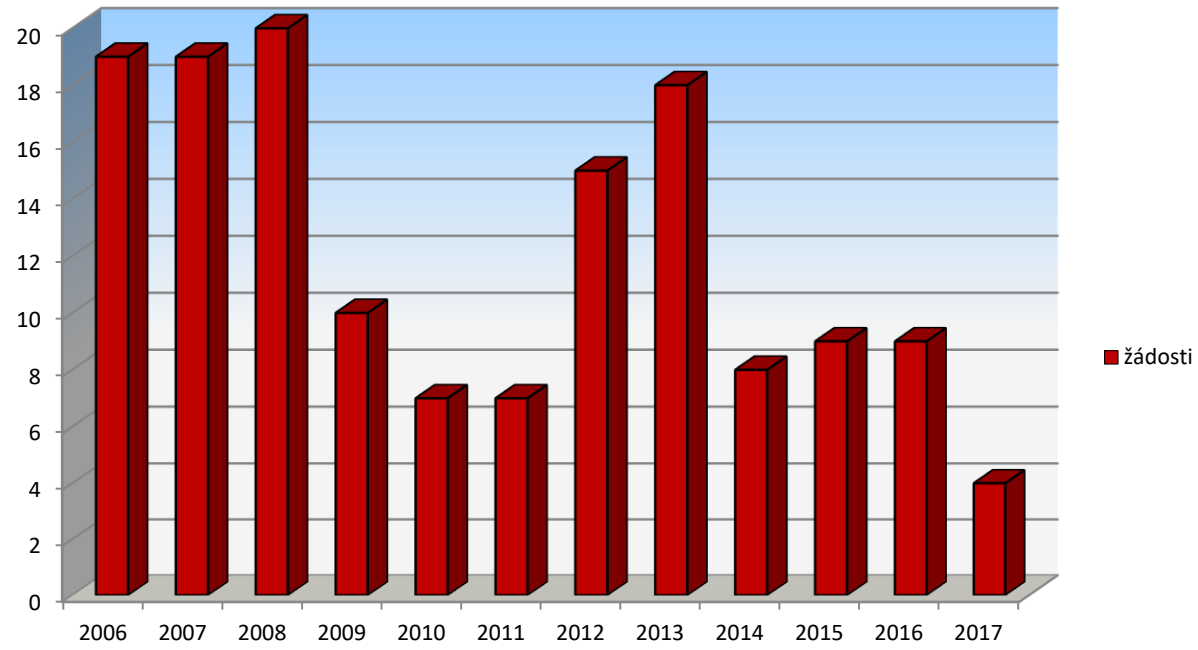
2.2.1.2. Certifikace kryptografických prostředků

V roce 2017 byly Úřadu podány celkem 4 žádosti o certifikaci kryptografického prostředku, z toho 3 na nový kryptografický prostředek. V řízeních k certifikaci kryptografického prostředku byly vydány 4 certifikáty, žádné řízení nebylo ukončeno bez vydání certifikátu. Stav řízení je shrnut v následující tabulce.

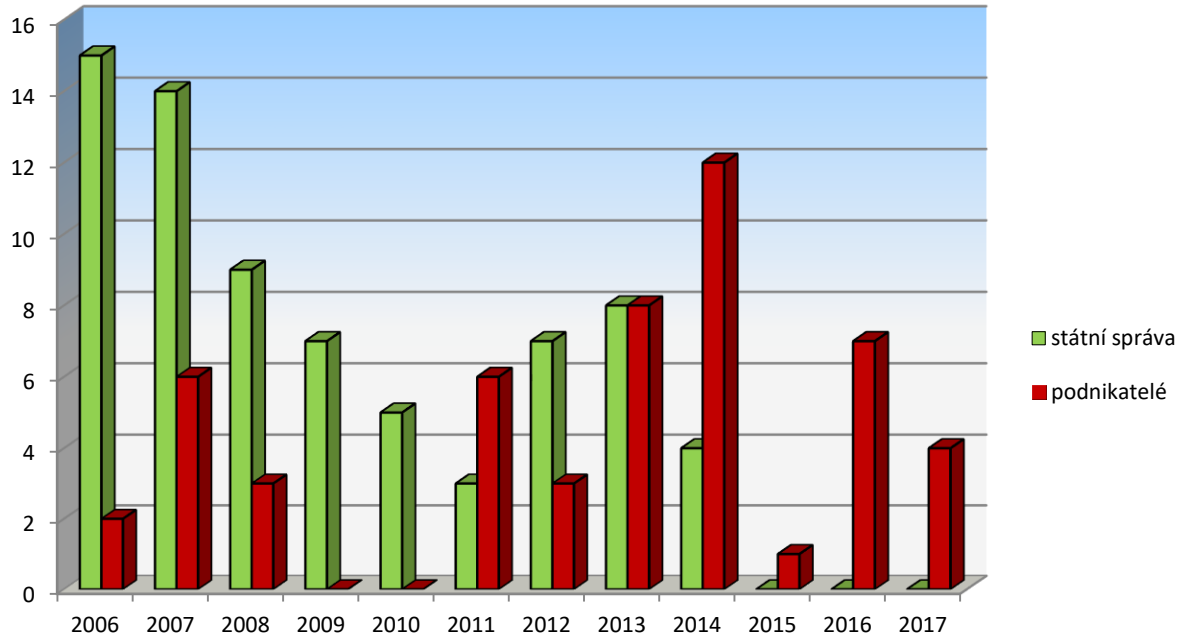
Certifikace kryptografických prostředků v roce 2017

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
4	8	3	0	0	0	4	4	2

Přijaté žádosti o certifikaci kryptografického prostředku v letech 2006 až 2017



Vydané certifikáty kryptografických prostředků v letech 2006 až 2017



Nově byly certifikovány kryptografické prostředky SECTRA Tiger/R a LANPCS-RG2, ostatní 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. SECTRA Tiger/R, RES a prostředky třídy LANPCS. Nezanedbatelné byly také činnosti související s „duálním" hodnocením kryptografického prostředku LANPCSe-AES jako prostředku schváleného EU. 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 přípravné práce na vytvoření expozice v prostorách Úřadu, zabývající se historií kryptografických prostředků používaných v ČR.

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 NBÚ.

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

Do seznamu Úřadu materiálu „kontrolovaná kryptografická položka" byly nově zařazeny dva kryptografické prostředky.

2.2.1.3.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 2017 nebyla podána žádná žádost o schválení projektu bezpečnosti nového komunikačního systému RETIS.

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 2017 nadále zajišťoval Úřad.

Komunikační systém Panthon pro mobilní komunikaci informací stupně utajení Vyhrazené, který využívá certifikovaného kryptografického prostředku Panthon 3, byl rovněž provozován za podpory Úřadu. Provoz tohoto systému byl ukončen 16. února 2018.

Jako náhrada komunikačního systému Panthon byl po schválení projektu bezpečnosti v roce 2017 uveden do provozu komunikační systém RETIS, který pro mobilní komunikaci informací stupně utajení Vyhrazené využívá certifikovaný kryptografický prostředek SECTRA Tiger/R (nová generace KP SECTRA Panthon 3). Provoz tohoto systému nadále zajišťuje Úřad.

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.

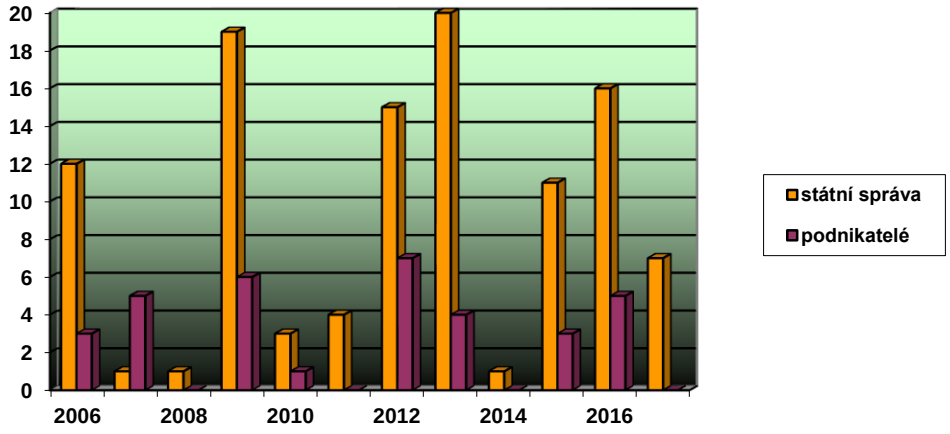
2.2.1.4.Certifikace kryptografických pracovišť

V roce 2017 bylo podáno celkem 7 žádostí o certifikaci kryptografického pracoviště. Většina žádostí o certifikaci spadá do kategorie opakovaných žádostí. Byla podána jedna žádost o certifikaci nového kryptografického pracoviště, a dále jsou ještě další dvě žádosti ve stádiu posuzování. Jedno řízení o opakované certifikaci bylo na základě oznámení žadatele zastaveno. 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:

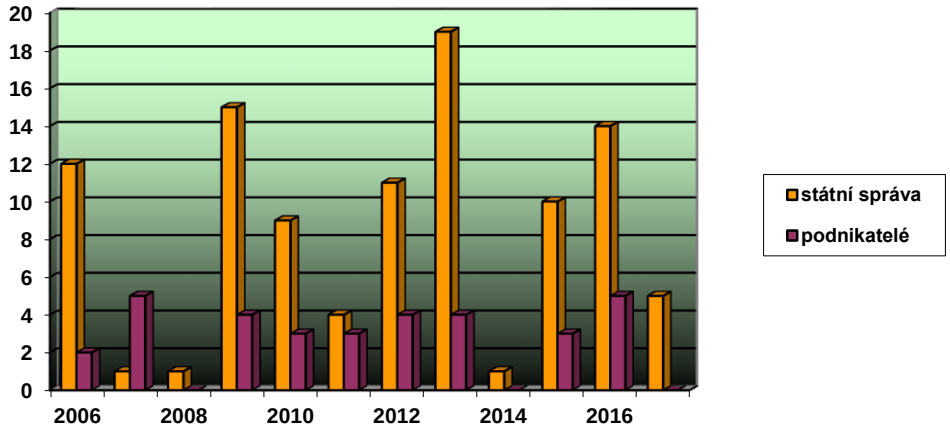
Certifikace kryptografických pracovišť v roce 2017

	Přijaté žádosti	Rozpracováno	Certifikováno	Zamítnuto	Zastaveno
Státní správa	7	3	5	0	1
Podnikatelé	0	0	0	0	0
Celkem	**7**	**3**	**5**	**0**	**1**

Přijaté žádosti o certifikaci kryptografického pracoviště v letech 2006 až 2017



Vydané certifikáty kryptografických pracovišť v letech 2006 až 2017



2.2.1.5.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 29 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.

2.2.2. Další odborná činnost

2.2.2.1.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.

V roce 2017 bylo v Úřadu vygenerováno celkem 90 922 kryptografických klíčů a hesel uložených na 7 121 nosičích různých typů a dalších 83 ks jiného kryptografického materiálu (procesory, paměti, kryptografická dokumentace, instalační a šifrovací SW).

Úřad vzal do evidence a provedl distribuci celkem 709 ks nového kryptografického a CCI materiálu a dále zajistil servis a opravy na území ČR u 102 ks kryptografických prostředků a mimo ČR u 19 ks kryptografických prostředků.

Úřad zajistil výrobu, vzal do evidence a provedl distribuci celkem 13 ks kryptografického materiálu EU.

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.

2.2.2.2.Měření kompromitujícího vyzařování (TEMPEST)

2.2.2.2.1. TEMPEST měření elektronických zařízení

Úřad prováděl v roce 2017 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 2017 provedeno více než 59 měření různých typů zařízení. Z toho bylo prováděno TEMPEST měření samostatných zařízení nebo v kombinaci s kryptografickým prostředkem KRYDEC a PCS1 a dále bylo provedeno měření národních kryptografických prostředků Slovinska na jejich žádost. 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.

2.2.2.2.2. 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 Důvěrné a Tajné a v rámci certifikace těchto systémů byly zpracovány instalační záznamy z 19 lokalit.

V roce 2017 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.

2.2.2.2.3. Přehled provedených měření

Přehled měření v oblasti kompromitujícího vyzařování, provedených v roce 2017, je uveden v následující tabulce.

Měřená zařízení a objekty v roce 2017

Typ měření[9)]	**Počet**
Zónové měření	20 objektů
Kryptografické prostředky	3 typy
Komponenty ICT	59 měření
Audiotechnika	2 typy zařízení
Obranné prohlídky i v rámci certifikace IS	16 objektů
Mobilní systémy	3 systémy
Instalační záznamy	19 lokalit

2.2.2.3.Školení pracovníků kryptografické ochrany a zkoušky odborné způsobilosti

Úřad v roce 2017 organizačně zajistil a provedl, v souladu se zákonem, celkem 15 školení skupin pracovníků kryptografické ochrany a po následující zkoušce odborné způsobilosti vydal 62 osvědčení o zvláštní odborné způsobilosti pracovníka kryptografické ochrany. Dále provedl zaškolení pracovníků provozní obsluhy kryptografického prostředku a vydal 37 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 2017 schválil nový kurz pro zařízení TCE 114 a aktualizace osnov a obsahu dříve schváleních kurzů.

2.2.2.4.Kontroly ochrany utajovaných informací (státní dozor)

V roce 2017 provedl Úřad ve smyslu §143 odst. 6 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti 22 kontrol za oblast bezpečnosti informačních nebo komunikačních

[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.

systémů, případně kryptografické ochrany. Z tohoto počtu bylo 9 kontrol provedeno v rámci státní správy a 13 kontrol u podnikatelů.

2.2.3. 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 2017 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 2017 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.

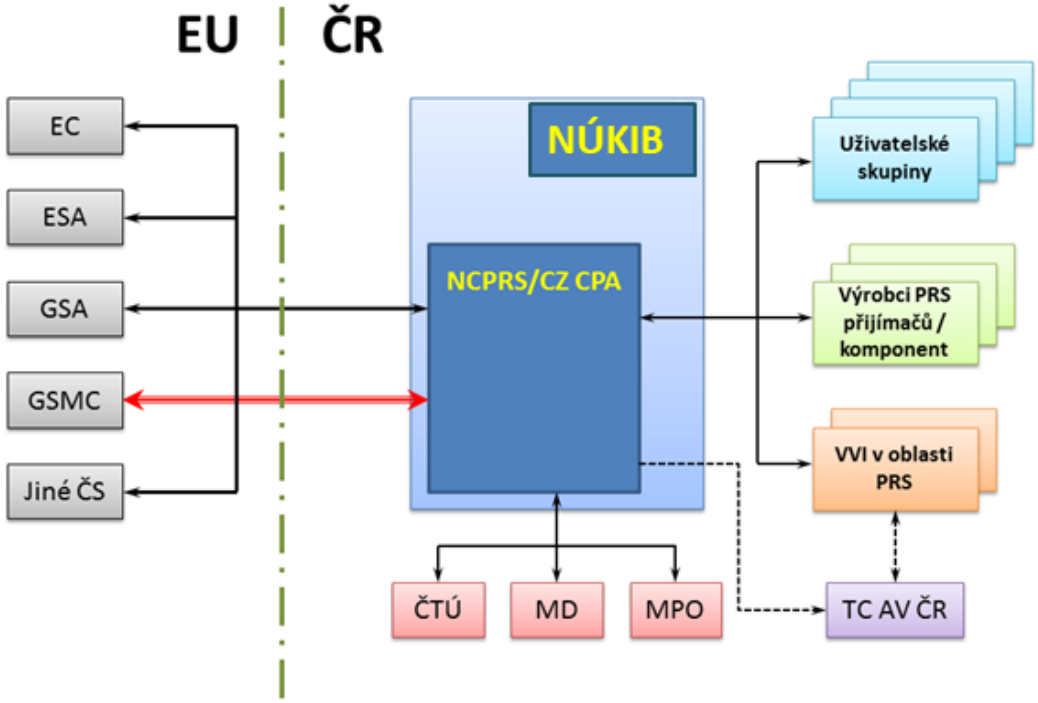
2.3. VÝKON FUNKCE PŘÍSLUŠNÉHO ORGÁNU PRS

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“).

2.3.1. 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.

2.3.2. 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.

2.3.3. 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 2018 je naplánováno dotazníkové šetření v rámci řešeného projektu FRAME (pilotní projekt GSA pro vývoj a rozšíření uživatelského segmentu PRS).

2.4. VÝZKUM A VÝVOJ

2.4.1. 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.

2.4.2. Projekty realizované v roce 2017

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 proběhlo 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 2017 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.

2.5. STÁTNÍ DOZOR

2.5.1. Kontroly provedené v roce 2017

Pokud jde o výkon státního dozoru v oblasti ochrany utajovaných informací, pracovníci NÚKIB jsou členy kontrolních skupin NBÚ. Veškeré statistické údaje jsou tedy obsaženy ve Zprávě o činnosti Národního bezpečnostního úřadu za rok 2017.

3. EKONOMICKÉ A PERSONÁLNÍ ZABEZPEČENÍ ÚŘADU

3.1. EKONOMICKÉ ZABEZPEČENÍ ÚŘADU

Úřad je od 1. 8. 2017 samostatnou kapitolou státního rozpočtu pod číslem 378.

Rozpočet Úřadu k datu jeho vzniku jako nového správního úřadu, tedy ke **dni 1. 8. 2017 činil 210 062 511,- Kč a byl dále upravován** v pořadí sedmi rozpočtovými opatřeními, ve kterých se promítají změny ve vazbě na Delimitační protokol a dohodu o přechodu práv a povinností uzavřený mezi Národním

bezpečnostním úřadem a novým Úřadem s účinností od 1. 8. 2017, včetně dodatku č. 1 ze dne 31. 10. 2017 dodatku č. 2 ze dne 14. 11. 2017, z nichž nejvýznamnější jsou:

- **rozpočtové opatření MF RO č. 4** v celkovém objemu 16 934 901,- Kč (z toho 6 569 780,- Kč na pokrytí platů a 2 365 121,- Kč pro příslušenství), na provozní výdaje, platy, příslušenství, tedy zajištění výdajů k zabezpečení plnění úkolů Úřadu
- **rozpočtové opatření MF RO č. 5** v celkovém objemu 33 590 000,- Kč (z toho navýšení běžných výdajů 7 390 000,- Kč a navýšení kapitálových výdajů o 26 200 000,- Kč) – jednalo se o pokrytí běžných a kapitálových výdajů v souladu s usnesením vlády č. 1178/2016

Konečný rozpočet Úřadu činil 260 174 100,- Kč a bylo vyčerpáno 90 234 714,38 Kč, což představuje 34,68 % z konečného rozpočtu.

Z celkových výdajů byl nejvyšší podíl vynaložen na výdaje platové, spolu s příslušenstvím a náhradami platů v době nemoci, které vedeme rozpočtově společně pro všechny výdajové bloky Úřadu.

Běžné výdaje

Konečný rozpočet běžných výdajů, včetně platových výdajů a příslušenství, ve výši 102 356 658,- Kč byl vyčerpán v objemu 69 296 256,55 Kč, což představuje 67,70 %.

Prostředky na platy zaměstnanců po navýšení od 1. 11. 2017 dle nařízení vlády jsou vykázány v objemu 31 896 316,- Kč, skutečné čerpání platových prostředků činí 30 714 531,- Kč, což je **96,34 %**.

Kapitálové výdaje

Ke dni vzniku Úřadu byl delimitovaný rozpočet programového financování celkem včetně běžných výdajů 133 075 977,- Kč. Na základě souhlasu ministra financí byly navýšeny kapitálové výdaje o 26 200 000,- Kč. Delimitované a navýšené finanční prostředky nebyly z legislativních důvodů vyčerpány, zejména s ohledem na nemožnost dodržení lhůt vyplývajících ze zákona č. 134/2016 Sb., o zadávání veřejných zakázek, v platném znění.

Čerpání v porovnání skutečnosti v objemu 20 938 458,- Kč ke konečnému rozpočtu v objemu 159 275 977,- Kč k datu 31. 12. 2017 činí 13,14 %.

Kapitálové výdaje jsou evidovány v Informačním systému programového financování v programu EDS/SVMS ve výdajovém titulu „Rozvoj a obnova materiálně-technické základny Národního úřadu pro kybernetickou a informační bezpečnost“ pod č. 378V01, který se dělí na subtituly.

V rámci rozvoje a obnovy majetku ICT

činil konečný rozpočet 139 698 342,- Kč a byl vyčerpán v objemu 13 616 397,- Kč, což představuje plnění **9,75 %.** Důvodem pro nízké čerpání je nerealizování projektů v r. 2017. Finanční objemy budou přesunuty do nároků z nespotřebovaných výdajů do následujícího roku.

Pro rozvoj a obnovu movitého majetku

činil konečný rozpočet 13 076 505,- Kč a byl vyčerpán v objemu 4 780 226,- Kč, což představuje plnění **36,56 %.**

Rozvoj a obnova nemovitého majetku

byl konečný rozpočet v objemu 6 501 129,- Kč s čerpáním 2 541 834,- Kč, tj. **39,10 %.** Delimitovaný rozpočet byl navýšen v souladu s usnesením vlády č. 1178.

Nároky z nespotřebovaných výdajů nebylo možno delimitovat z Národního bezpečnostního úřadu. Úřadu poprvé vznikly nároky z nespotřebovaných výdajů nedočerpáním rozpočtu z roku 2017.
Ke 1. 1. 2018 Úřad eviduje **nároky z nespotřebovaných výdajů ve výši 169 939 385,62 Kč.**

Převážnou část nespotřebovaných výdajů roku 2017 tvoří kapitálové výdaje určené k financování projektu z EU a nákup SW. Nespotřebované výdaje budou v roce 2018 použity na pokrytí nerealizovaných smluvních závazků roku 2017, na neplánované výdaje roku 2018, zejména pak na dokončení a zrealizování veřejných zakázek souvisejících s budováním nových pracovišť.

Řídící a kontrolní mechanismy jsou pro jednotlivé oblasti činností Úřadu nastaveny prostřednictvím interních aktů řízení v souladu s ustanovením § 3 odst. 4 zákona o finanční kontrole. Interní akty řízení Úřadu tvoří základ jeho vnitřního kontrolního systému.

Od zřízení Úřadu byl zajišťován výkon řídící kontroly jednotlivými příkazci operací, hlavní účetní a správcem rozpočtu. V rámci své působnosti prováděli jmenované osoby finanční řídící kontroly při hospodaření s finančními prostředky na příslušných rozpočtových položkách Úřadu v rámci jeho rozpočtové skladby.

Mimo výkon řídící kontroly probíhala kontrolní činnost vedoucích zaměstnanců jednotlivých organizačních celků Úřadu, zaměřená na vyhodnocování již vyúčtovaných operací v jejich kompetenci z pohledu dosažení plánovaných cílů.
Při uskutečněných řídících kontrolách nebyly zjištěny skutečnosti, které by nasvědčovaly neoprávněnému nakládání s finančními prostředky, ani podezření na podvodné či korupční jednání. Finanční operace byly realizovány účelně, hospodárně a v souladu s naplňováním cílů a posláním Úřadu.
Místo interního auditora Úřad plánuje obsadit v roce 2018, tedy auditní činnost za období od zřízení Úřadu do konce roku 2017 nebyla vykonávána.

3.2. PERSONÁLNÍ ZABEZPEČENÍ ÚŘADU

V souladu s Delimitačním protokolem a Dohodou o přechodu práv a povinností s účinností od 1. 8. 2017 bylo delimitováno z Národního bezpečnostního úřadu 129 pracovních míst na Národní úřad pro kybernetickou a informační bezpečnost. K uvedenému datu došlo k přechodu výkonu práv a povinností z pracovně právních vztahů u 118 vybraných zaměstnanců, z tohoto počtu byli 3 zaměstnanci mimo evidenční stav - (1 zaměstnankyně na rodičovské dovolené a 2 zaměstnanci na neplaceném volnu).

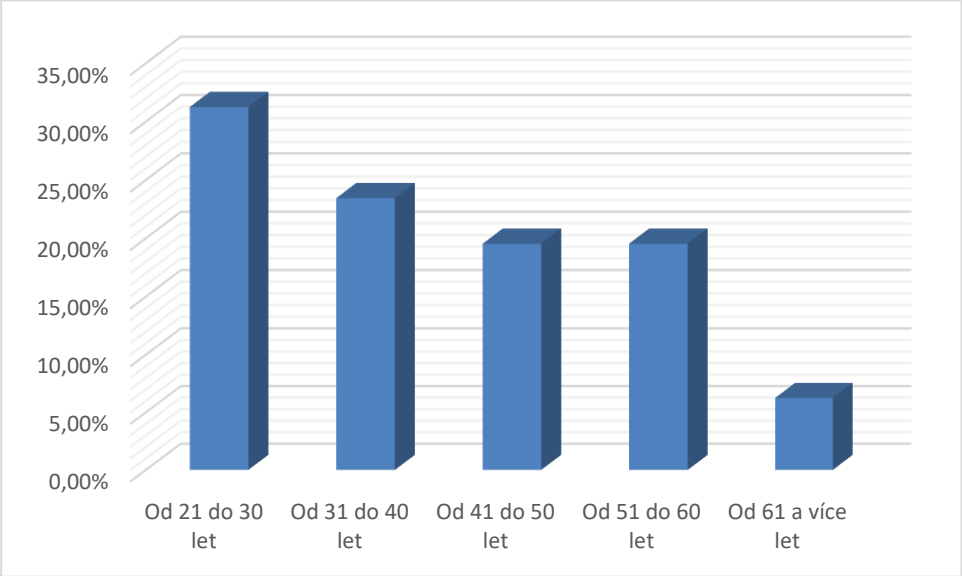
Pro zabezpečování činností nově vzniklého ústředního správního úřadu byla vytvořena ke dni jeho vzniku současně organizační struktura, do které byla začleněna delimitovaná pracovní místa.

Do konce roku 2017 byla pracovní místa postupně obsazována novými zaměstnanci. Do pracovního poměru v období od 1. 8. 2017 do 31. 12. 2017 bylo přijato 13 nových zaměstnanců. Dalších 12 zaměstnanců vykonávalo činnost na základě uzavřených dohod o pracích konaných mimo pracovní poměr.

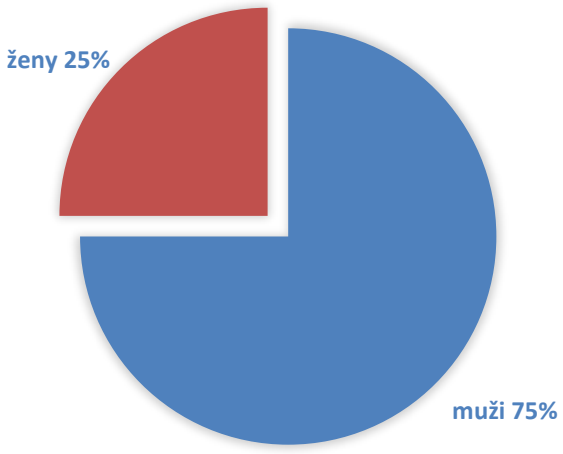
Do konce roku 2017 ukončilo 5 zaměstnanců pracovní poměr, tj. 3,9% z celkového počtu zaměstnanců. Z tohoto počtu 2 zaměstnanci ukončili pracovní poměr ve zkušební době a 3 delimitovaní zaměstnanci z Národního bezpečnostního úřadu podali výpověď v souladu se zákoníkem práce.

K 31. 12. 2017 bylo v evidenčním stavu celkem 128 zaměstnanců, z toho 75% mužů a 25% žen. Průměrný věk zaměstnanců úřadu je 44 let.

Struktura zaměstnanců Úřadu podle věku (%)

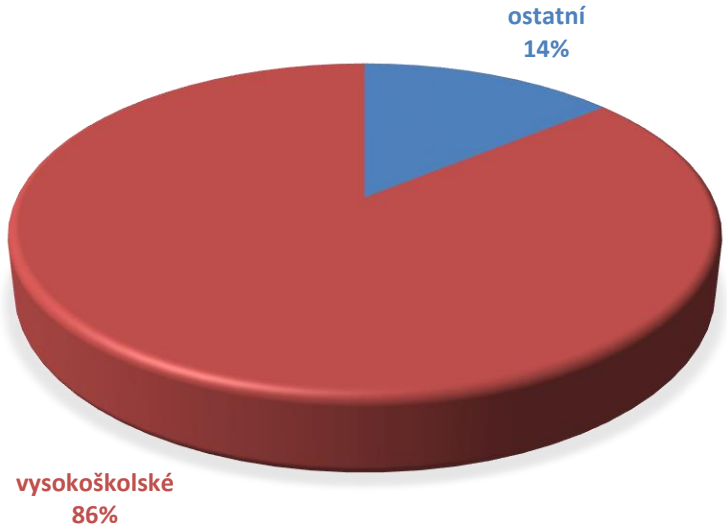


Struktura zaměstnanců Úřadu – ženy/muži



V rámci organizační struktury Úřadu je na jednotlivých pracovních místech stanoven předpoklad potřebného vzdělání, vysokoškolské vzdělání je stanoveno na 90% těchto pracovních míst. Z celkového počtu zaměstnanců k 31. 12. 2017 mělo 86% zaměstnanců vysokoškolské vzdělání.

Struktura zaměstnanců Úřadu podle vzdělání



Od vzniku Úřadu rozvíjíme znalosti a dovednosti našich zaměstnanců a uvědomujeme si přínos jednotlivce a týmu ke kvalitnímu plnění činností Úřadu. Osobnostní a profesní rozvoj zaměstnanců prostřednictvím soustavného rozvíjení a prohlubování dovedností, znalostí a schopností znamenají udržení profesionality Úřadu. Zabezpečujeme odborný rozvoj zaměstnanců, zajišťujeme prohlubování jejich odborné kvalifikace a umožňujeme zaměstnancům skupinové i individuální jazykové vzdělávání.

V roce 2017 byla realizována školení převážně v oblasti kybernetické bezpečnosti a informačních technologií jak v ČR, tak i v zahraničí. Převážná část školení byla zakončena certifikační zkouškou. V rámci spolupráce se společností SANS Institute se zaměstnanci NCKB zúčastnili školení v oblasti předcházení, detekce a reakce na kybernetické útoky.

Rovněž byla věnována pozornost i dalšímu odbornému vzdělávání zaměstnanců v oblastech souvisejících s jejich pracovní činností, především v oblasti ekonomické a právní.

I v roce 2017 se Úřad prezentoval na veletrhu JobChallenge, který je pořádán Masarykovou univerzitou, Mendelovou univerzitou a Vysokým učením technickým v Brně. Veletrh je jedním z největších veletrhů práce v České republice. Každý rok jej navštíví až na 3 000 studentů a představuje se na něm až 90 zaměstnavatelů. Úřad na veletrhu prezentoval svou činnost a využil této příležitosti k přiblížení jeho aktivit potenciálním uchazečům o pracovní pozice.

Vedle pracovních příležitostí Úřad rovněž poskytuje za účelem přípravy na budoucí povolání praktické stáže pro vysokoškolské studenty. V roce 2017 absolvovalo stáž 7 studentů. Stáže byly jak technického, tak právního a politicko-bezpečnostního zaměření. Součástí spolupráce se studenty jsou také pravidelné odborné konzultace diplomových a seminárních prací.

Pracovněprávní, platové a jiné nároky zaměstnanců byly realizovány v souladu s platnou Kolektivní smlouvou.

Spokojení a motivovaní zaměstnanci jsou základní podmínkou pro zvyšování kvality výstupů Úřadu, odpovědnosti za svou práci a dobré spolupráce v rámci jednotlivých organizačních celků. Proto se snažíme

pečovat o své zaměstnance, udržovat s nimi dobré vztahy a i přes problémy spojené s budováním pracovišť Úřadu vytvářet dobré pracovní podmínky a zázemí.