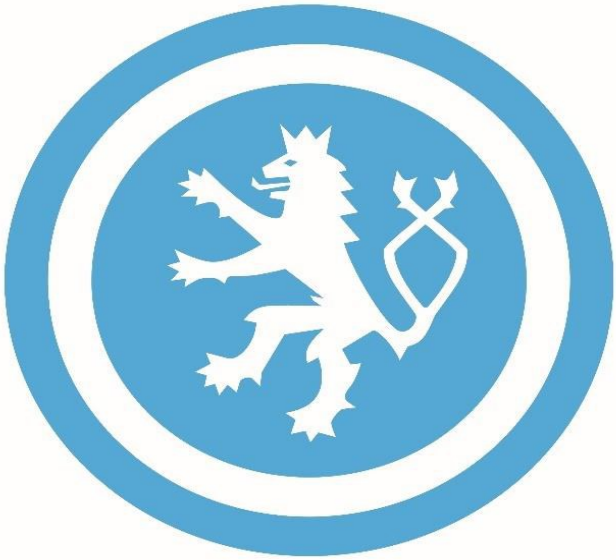
NÚKIB



Národní úřad pro kybernetickou a informační bezpečnost

Z P R Á V A

O ČINNOSTI

NÁRODNÍHO ÚŘADU
PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST

ZA ROK 2018

Praha 2019

Obsah

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 č. 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:

- provoz Vládního CERT České republiky (GovCERT.CZ)
- spolupráce s ostatními národními CERT® týmy a CSIRT týmy
- spolupráce s mezinárodními CERT® týmy a CSIRT týmy
- stanovení kritérií pro určení klíčových informačních systémů z hlediska České republiky a jejich autoritativní určování v konkrétních případech
- stanovení bezpečnostních standardů pro informační systémy kritické informační infrastruktury, provozovatelů základních služeb a významných informačních systémů formou vyhlášek
- kontrola dodržování stanovených standardů u informačních systémů KII, PZS a VIS
- osvěta a podpora vzdělávání v oblasti kybernetické bezpečnosti
- výzkum a vývoj v oblasti kybernetické bezpečnosti
- ochrana utajovaných informací v oblasti informačních a komunikačních systémů
- kryptografická ochrana
- národní kontaktní místo PRS - jedna ze služeb evropského satelitního systému Galileo (NCPRS)

Legislativa a Vládní agenda úřadu

NÚKIB je gestorem zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, vybraných částí zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů, a samozřejmě také prováděcích předpisů k uvedeným zákonům. Cílem regulace podle těchto zákonů a jejich prováděcích předpisů je zajištění kybernetické bezpečnosti jak v informačních systémech kritické informační infrastruktury, významných informačních systémech, informačních systémech provozovatelů základních služeb a dalších systémech, ve kterých jsou zpracovávány neutajované informace, tak také kybernetické bezpečnosti informačních a komunikačních systémů nakládajících s utajovanými informacemi.

V roce 2018 nabyla účinnosti vyhláška NÚKIB č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby, a byla přijata zcela nová vyhláška NÚKIB č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti). V témže roce NÚKIB také zahájil práce na přípravě novelizace vyhlášky NÚKIB č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, ve znění pozdějších předpisů, a na přípravě zcela nové vyhlášky o způsobu likvidace kopií dat a provozních údajů informačního systému veřejné správy a o náležitostech protokolu o průběhu jejich likvidace. V roce 2018 se NÚKIB podílel také na přípravě novelizace zákona č. 412/2005 Sb., která má být v následujícím roce předložena vládě ke schválení a k dalšímu projednání v Parlamentu České republiky.

Vedle přijetí výše uvedených vlastních právních předpisů NÚKIB v roce 2018 posoudil v meziresortním připomínkovém řízení více než 100 materiálů legislativní i nelegislativní povahy, přičemž k více než pětině z nich uplatnil z hlediska své působnosti připomínky.

Příslušné pracoviště NÚKIB vedle výše uvedeného zajišťuje také činnosti v oblasti vládní agendy, a to předkládání vlastních materiálů NÚKIB vládě, Bezpečnostní radě státu či Výboru pro kybernetickou bezpečnost, aktualizaci výkaznictví souladu právních předpisů v gesci NÚKIB s právními předpisy Evropské unie, řízení gescí úřadu k dokumentům legislativní i nelegislativní povahy Evropské unie apod.

Interní audit

Výkon interního auditu Úřadu je zajišťován jedním zaměstnancem pověřeným zajištěním interního auditu ve smyslu § 28 odst. 1 zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (dále jen „zákon o finanční kontrole“). Postavení interního auditu je nezávislé na organizační struktuře Úřadu a interní audit je administrativně a funkčně podřízen řediteli Úřadu.

V první polovině roku 2018 byl vydán interní normativní akt Vnitřní kontrolní systém, který upravuje organizaci a fungování vnitřního kontrolního systému Úřadu ve smyslu zákona o finanční kontrole. Součástí tohoto interního normativního aktu je Statut interního auditu vymezující činnost interního auditu.

Finanční kontrolu vykonávanou podle zákona o finanční kontrole tvoří u Úřadu tyto složky:

- vnitřní kontrolní systém zahrnující:
  - finanční kontrolu zajišťovanou odpovědnými vedoucími zaměstnanci jako součást vnitřního řízení Úřadu (řídící kontrola),
  - **interní audit**
- veřejnosprávní kontrola vykonávaná státními kontrolními orgány vůči Úřadu.

Ve spolupráci interní auditorky a vedoucích zaměstnanců byla identifikována a vyhodnocena rizika vyskytující se na Úřadě. Výsledkem byla zpracovaná Mapa rizik obsahující rozdělení rizik dle jejich významnosti, vymezení nositele rizika, oblastí rizika, popis rizika, důsledek, projev rizika, RPN (Risk Priority Number – kritické rizikové číslo dané násobkem pravděpodobnosti výskytu a velikosti dopadu, vyjadřuje závažnost rizika) a doporučení ke snížení či eliminaci rizik.

Ve spolupráci interní auditorky a příkazců operací byla zpracována zpráva o výsledcích následných řídících kontrol provedených v průběhu roku v jimi řízeném organizačním celku. Interní auditorka také namátkově provedla průběžnou kontrolu realizace následných kontrol v pololetí a předložila o ní zprávu řediteli.

V průběhu roku byl taktéž vypracován Střednědobý plán pro období 2019-2021 a Plán auditu pro rok 2018, ve kterém byl naplánován 1 interní audit.

Jednalo se o audit veřejných zakázek s ohledem na jejich legalitu, dodržování principů transparentnosti, přiměřenosti, rovného zacházení či nediskriminace. Z provedeného auditu vyplynula doporučení pro zkvalitnění vnitřního kontrolního systému a fungování Úřadu. Veškerá auditní zjištění byla projednána s ředitelem auditovaného útvaru tak, aby byla zajištěna smysluplnost auditních doporučení, jejich implementace a následná zpětná vazba. Je zavedena evidence těchto doporučení.

Ke konci roku byla řediteli Úřadu předána Zpráva o kvalitě a účinnosti vnitřního systému. Její součástí byly:

- Mapa rizik,
- Zprávy o provedené kontrole realizace následných kontrol v pololetí a za celý rok 2018,
- Zprávu o činnosti interního auditu v průběhu roku včetně zjištění z vykonaného auditu.

Mimo auditní činnost byla náplní práce interní auditorky také průběžná konzultační a poradenská činnost, a dále připomínkování a spolupráce při tvorbě interních normativních aktů.

Odbor právní

Oblast správního 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, jež 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 rovněž projednává přestupky podle části osmé zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů (dále jen „zákon 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 roce 2018 Úřad evidoval šest podnětů k prošetření, z nichž se všechny dotýkaly zákona o ochraně utajovaných informací. Z hlediska konkrétního údajného pochybení fyzických osob, které má Úřad posoudit, se pak především jednalo o nevhodné nakládání s utajovanou informací. Prošetřování důvodnosti těchto podnětů nebylo do konce roku 2018 ukončeno.

Významnou část činnosti odboru právního tvoří agenda obchodních smluv uzavíraných na plnění jednotlivých veřejných zakázek a agenda dalších smluvních ujednání uzavíraných v souvislosti se zabezpečením výkonu působnosti Úřadu, kdy se jedná převážně o smlouvy a zápisy uzavírané s dalšími organizačními složkami státu, orgány státní správy nebo jinými subjekty a agenda pracovně právní.

Odbor právní v rámci Úřadu zabezpečuje též agendu zadávání veřejných zakázek. V souvislosti s povinnou elektronizací procesu zadávání všech veřejných zakázek zavedenou zákonem č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, Úřad využívá Elektronický nástroj E-ZAK a Národní elektronický nástroj, kdy používání tohoto nástroje je pro Úřad povinné. Mezi veřejné zakázky největšího významu realizované na Úřadě v roce 2018 lze zařadit nadlimitní veřejné zakázky na Servery, Technologie ochrany síťového perimetru a Odborné vzdělávání zaměstnanců Úřadu v oblasti kybernetické bezpečnosti.

Odbor právní rovněž zajišťuje uveřejnění smluv v registru smluv splněním zákonné povinnosti dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv a o registru smluv, ve znění pozdějších předpisů.

Současně odbor právní plní povinnosti vyplývající pro Úřad ze zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, zákona č. 101/2000 Sb., ochraně osobních údajů a o změně některých zákonů, a nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů, GDPR).

Odbor právní se dále podílí na zpracování stanovisek z oblasti kybernetické bezpečnosti a vybraných oblastí ochrany utajovaných informací, poskytuje metodickou pomoc ostatním organizačním celkům a vykonává další činnosti.

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

Úřadu bylo v roce 2018 adresováno celkem 9 žádostí o poskytnutí informací vztahujících se k jeho působnosti. V plném rozsahu byla informace poskytnuta v 9 případech. Poskytnuté informace byly zveřejňovány v souladu s § 5 odst. 3 zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů

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

Poskytování informací dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, podle oblastí v roce 2018	počet podaných žádostí	počet vydaných rozhodnutí o odmítnutí žádosti
Kybernetická bezpečnost	5	0
Vzdělávání	1	0
Všeobecné	3	0
Celkem	9	0

2. Počet podaných odvolání proti rozhodnutím Úřadu podle zákona č. 106/1999 Sb.: 0 odvolání
3. Počet podaných stížností na postup při vyřizování žádosti podle § 16 zákona č. 106/1999 Sb.: 0 stížnosti
4. Rozsudky soudu ve vztahu k Úřadu v oblasti poskytování informací: Žádný rozsudek.
5. Výsledky řízení o sankcích za nedodržování zákona č. 106/1999 Sb.: Nebylo vedeno žádné řízení.
6. Výčet poskytnutých výhradních licencí: Nebyla poskytnuta žádná výhradní licence.

Ekonomické zabezpečení úřadu

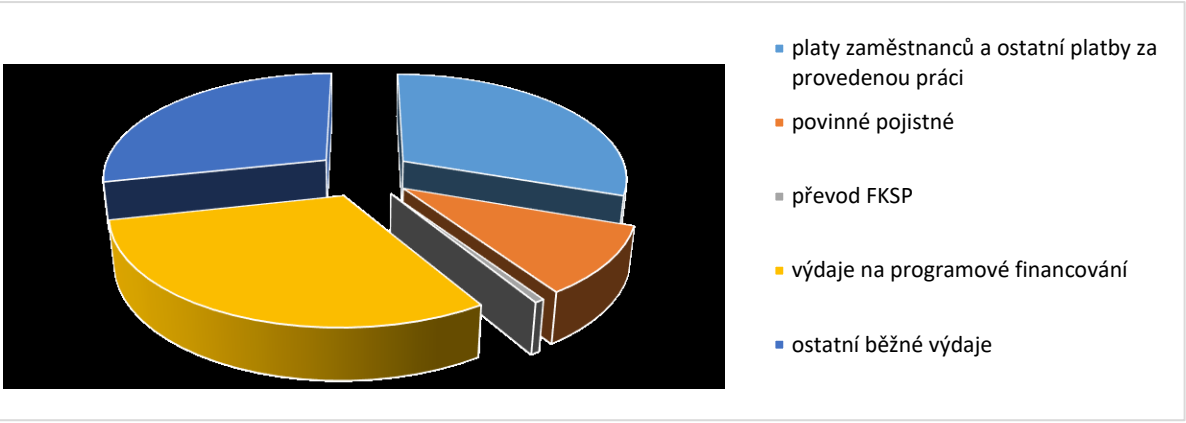
Úřad je od 01. 08. 2017 samostatnou kapitolou státního rozpočtu pod číslem 378.

Plánovaný rozpočet Úřadu byl v roce 2018 ve výši 363 026 559 Kč a byl upravován celkem jedenácti rozpočtovými opatřeními Ministerstva financí ČR (dále jen „MF“) na celkovou částku **378 349 618 Kč.** K 31. 12. 2018 bylo vyčerpáno z upraveného rozpočtu **348 735 246** Kč, tj**. 92,17 %. Čerpání konečného rozpočtu ve výši 548 289 003,62 Kč představuje 63,60 %**. Jedná se o upravený rozpočet, který byl navýšen o nároky z nespotřebovaných výdajů (dále jen „NNV“) roku 2017 ve výši **169 939 385,62 Kč.**

Celkové platové výdaje byly rozpočtovány ve výši 142 372 198 Kč, rozpočtovými opatřeními byly upraveny na 143 677 798 Kč a zapojením nároků z nespotřebovaných výdajů (dále jen „NNV“) byly upraveny na konečný rozpočet ve výši 146 162 471 Kč, který byl čerpán ve výši **143 753 936 Kč.**

V návaznosti na výše uvedené bylo provedeno jedenáct rozpočtových opatření MF.

Podíl čerpání jednotlivých průřezových ukazatelů na celkovém čerpání rozpočtu NÚKIB za rok 2018



Běžné výdaje

Konečný rozpočet běžných výdajů celkem včetně platových výdajů a příslušenství ve výši **284 441 914,45 Kč** byl **vyčerpán v objemu 242 792 469,48 Kč,** což představuje **85,36 %.**

Schválený rozpočet na platy činil **104 114 528 Kč pro 177 zaměstnanců** (v objemu je zahrnut nadpožadavek Úřadu na platy a příslušenství pro 3 kyber odborníky). Pro ostatní platby za práce na základě uzavřených dohod o provedení práce a o pracovní činnosti byl schválen objem **579 433 Kč.** Rozpočet platů byl upraven na objem 105 074 528 Kč, což činí 99,48 % upraveného rozpočtu a konečné čerpání bylo v objemu 104 524 309 Kč, tj. 99,27 %. V konečném rozpočtu platů ve výši 105 298 207 Kč jsou promítnuté i nároky z nespotřebovaných výdajů roku 2017 ve výši 223 679 Kč.

Příděl do fondu kulturních a sociálních potřeb na základě platné právní úpravy byl propočten pro rok 2018 ve výši 2 082 290 Kč, tj. 2 % z celkového objemu prostředků na platy zaměstnanců Úřadu. Rozpočtovým opatřením byl navýšen na 2 101 490 Kč a dále byl navýšen o NNV roku 2017 na konečných 2 123 995 Kč. Vyčerpáno bylo 2 095 307 Kč, tj. 98,65 %. Prostředky fondu byly použity na stravování, rekreaci, kulturní a sportovní akce a penzijní připojištění.

Kapitálové výdaje

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.

Čerpání za všechny programy SMVS **v porovnání skutečnosti v objemu 106 175 920,12 Kč ke konečnému rozpočtu v objemu 265 767 104,17 Kč** k datu 31. 12. 2018 **činí 39,95 %.**

V rámci rozvoje a obnovy majetku IT

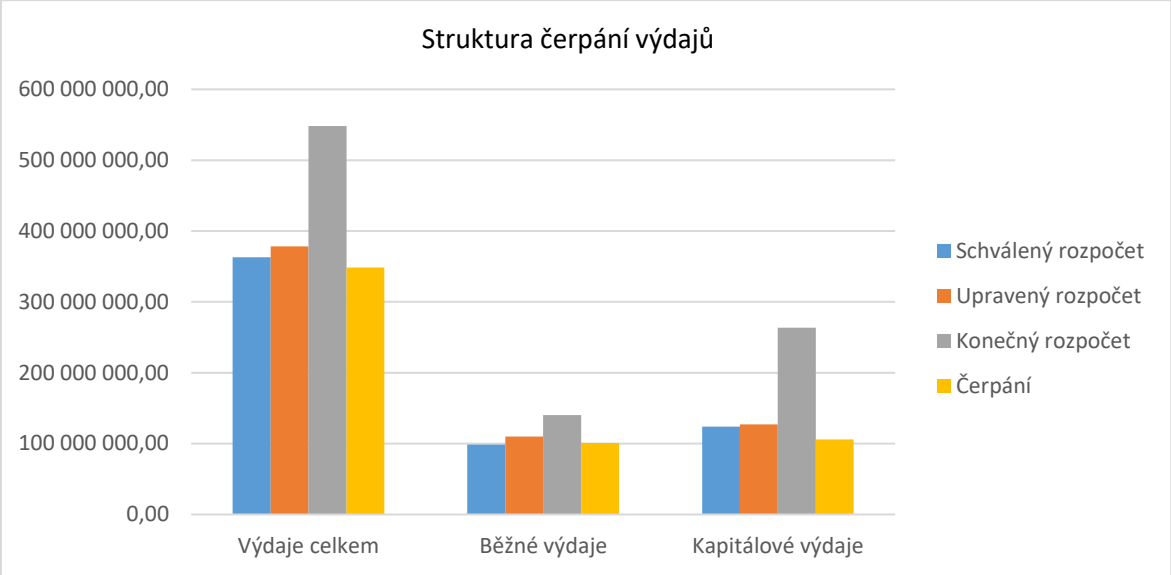
činil **konečný rozpočet 217 118 139,70 Kč** a byl **vyčerpán** v objemu **90 623 733,98 Kč,** což představuje **plnění 41,74 %**. Nejvyšší objem byl vynaložen realizováním projektu Systém detekce kybernetických incidentů.

Pro rozvoj a obnovu movitého majetku

činil **konečný rozpočet 23 524 387 Kč** a byl **vyčerpán** v objemu **12 679 173,61 Kč**, což představuje **plnění 53,90 %.**

Rozvoj a obnova nemovitého majetku

konečný rozpočet v objemu **25 124 577,47 Kč** byl čerpán částkou **2 873 12,53 Kč** tj. **11,44 %.**



Nároky z nespotřebovaných výdajů

Úřadu poprvé vznikly nároky z nespotřebovaných výdajů nedočerpáním rozpočtu z roku 2017.
Ke dni 1. lednu 2018 Úřad evidoval nároky z nespotřebovaných výdajů ve výši **169 939 385,62 Kč.**

Celkem za rok 2018 bylo vyčerpáno z nároků z nespotřebovaných výdajů 113 745 970,37 Kč.

Nespotřebované výdaje k 01. 01. 2019 jsou ve výši 199 533 757,62 Kč. V tomto objemu se promítá neprofinancovaný objem roku 2017 ve výši 56 193 415,25 Kč. Z tohoto objemu činí prostředky k zajištění financování projektu Systém detekce kybernetických incidentů částku 39 533 951,06 Kč, která bude vrácena do státního rozpočtu.

Převážnou část nespotřebovaných výdajů tvoří kapitálové výdaje určené k financování projektu z EU a prostředky určené k nákupům IT. Nespotřebované výdaje budou v roce 2019 použity na pokrytí nerealizovaných smluvních závazků roku 2018, na neplánované výdaje roku 2019, zejména pak na dokončení a zrealizování veřejných zakázek souvisejících s rozšiřováním pracovišť Úřadu. Čerpání NNV je u akcí IT ovlivněno podmínkami při budování síťové infrastruktury pro všechna pracoviště Úřadu a i časovými podmínkami při realizování veřejných zakázek k nákupům technologických celků a speciální techniky IT.

Řídící a kontrolní mechanismy jsou pro jednotlivé oblasti činností Úřadu nastaveny prostřednictvím interních normativních aktů řízení v souladu s ustanovením § 3 odst. 4 zákona o finanční kontrole. Interní akty řízení Úřadu tvoří základ jeho vnitřního kontrolního systému, na začátku roku 2018 bylo obsazeno místo interní auditorky, která již plně provádí auditní činnost a byla vydána směrnice Vnitřní kontrolní systém.

Výkon řídící kontroly byl prováděn 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.

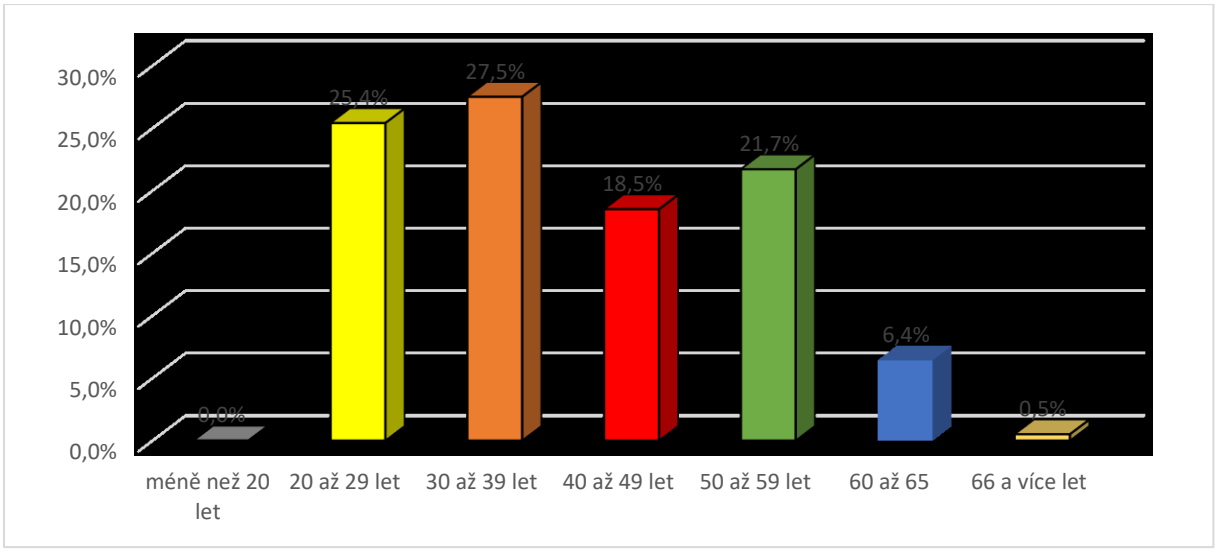
Personální zabezpečení úřadu

Také v roce 2018 byla pracovní místa postupně obsazována novými zaměstnanci. Do pracovního poměru v období od 1. 1. 2018 do 31. 12. 2018 bylo přijato 79 nových zaměstnanců. Dalších 26 zaměstnanců vykonávalo činnost na základě uzavřených dohod o pracích konaných mimo pracovní poměr.

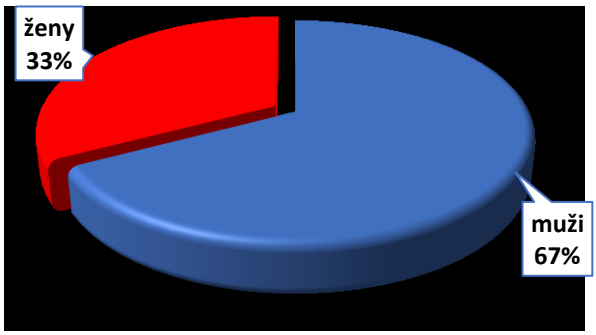
Do konce roku 2018 ukončilo 13 zaměstnanců pracovní poměr, tj. 6,8% z celkového počtu zaměstnanců. Z tohoto počtu 1 zaměstnanec ukončil pracovní poměr ve zkušební době, 2 zaměstnanci ukončili pracovní poměr uplynutím doby určité a 10 zaměstnanců rozvázalo pracovní poměr výpovědí.

K 31. 12. 2018 bylo v evidenčním stavu celkem 189 zaměstnanců z toho 66,6% mužů a 33,3% žen. Průměrný věk zaměstnanců úřadu je 39,9 let.

Struktura zaměstnanců Úřadu podle věku (%)



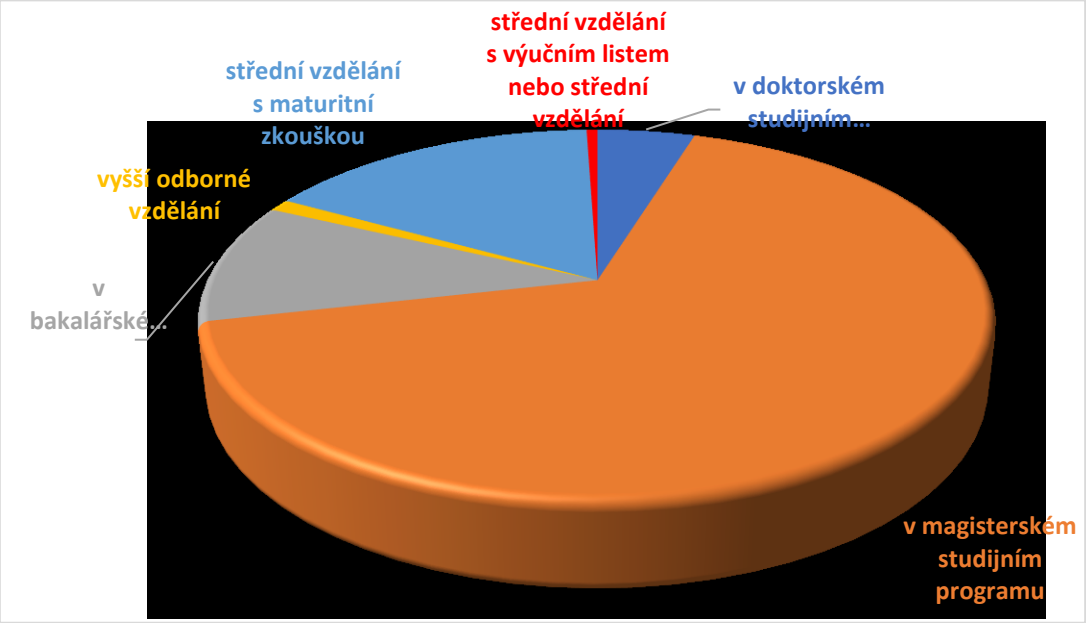
Struktura zaměstnanců Úřadu – ženy/muži



Na všechna pracovní místa jsou ve specifikacích pracovních míst stanoveny kvalifikační předpoklady a požadavky. Plnění potřebného vzdělání se pak projevuje v kvalifikační struktuře zaměstnanců Úřadu.

Dosažené vzdělání k 31. 12. 2018	**Počet zaměstnanců k 31. 12. 2018**	**Procentní struktura**
v doktorském studijním programu	9	4,8%
v magisterském studijním programu	126	67%
v bakalářském studijním programu	20	10,1%
vyšší odborné vzdělání	2	1,1%
střední vzdělání s maturitní zkouškou	31	16,4%
střední vzdělání s výučním listem nebo střední vzdělání	1	0,6%
základní vzdělání		
Celkem	**189**	**100%**

Struktura zaměstnanců 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 2018 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 GOPAS se zaměstnanci sekce Národního centra kybernetické bezpečnosti 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 2018 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. Dále se zaměstnankyně oddělení personálních věcí a vzdělávání zúčastnily Profesia days Praha a Dnů NATO v Ostravě.

Vedle pracovních příležitostí Úřad rovněž poskytuje za účelem přípravy na budoucí povolání praktické stáže pro vysokoškolské studenty. V roce 2018 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 vytvářet zaměstnancům Úřadu dobré pracovní podmínky a zázemí.

Oddělení investic a rozvoje

V roce 2018 proběhla další etapa opravy kancelářských prostor objektu Cejl v Brně. Dále, v rámci objektu Cejl, se zrealizovalo zázemí pro Ochrannou službu Policie ČR, která vykonává pro NÚKIB kontrolu a ostrahu tohoto objektu po dobu 24 hodin denně.

Z důvodu nedostatku kancelářských prostor pro nově nastupující zaměstnance Úřadu došlo k uzavření nájemní smlouvy na kancelářské prostory v objektu Fakulty podnikatelské VUT v Brně. Následně se realizovala rekonstrukce vyhrazených kanceláří a v prosinci 2018 proběhlo stěhování zaměstnanců Úřadu.

Nová administrativní budova NÚKIB

Během roku 2018 dále pokračovaly práce na vytvoření nové administrativní budovy v Brně – Černých Polích. V měsíci květnu byla přípravným projektovým týmem sestavena podrobná specifikace a seznam požadavků na novou budovu Úřadu. V měsících srpnu a září probíhalo (jakožto veřejná zakázka malého rozsahu) výběrové řízení ve smyslu zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, za účelem výběru administrátora soutěže o návrh na vybudování nového sídla úřadu v Černých Polích v Brně, a v říjnu byla vybrána ekonomicky nejvýhodnější nabídka. Administrátor poté zahájil přípravu podkladů pro soutěž. V měsících listopadu a prosinci se zpracovávaly podklady a průzkumy (inženýrsko-geologický průzkum, geodetické zaměření, identifikace inženýrských sítí atd.), které budou součástí soutěžních podmínek pro mezinárodní architektonickou soutěž.

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 obranných 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.

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.

Certifikace a akreditace informačních systémů

V roce 2018 probíhalo řízení o certifikaci 183 informačních systémů. K 39 žádostem o certifikaci informačního systému, jejichž zpracování bylo zahájeno v přechozím roce (2017), přibylo v roce 2018 dalších 144 žádostí, a to 55 ze státní správy nebo samosprávy a 89 ze soukromé sféry. Ve většině případů se jednalo o žádosti o opakovanou certifikaci již provozovaných informačních systémů. Ve 31 případech byla podána žádost o certifikaci nově budovaného informačního systému, přičemž pouze 8 z těchto žádostí pocházejí ze státní správy.

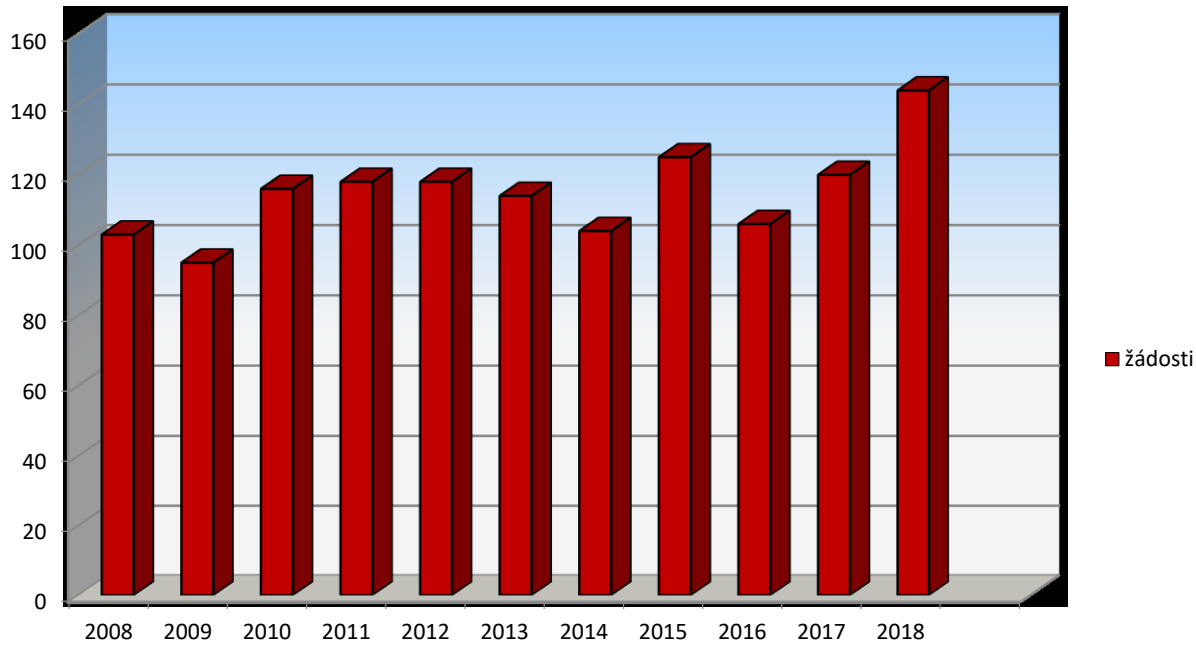
V uvedeném roce bylo vydáno celkem 111 certifikátů informačních systémů, z toho 40 pro žadatele ze státní správy nebo samosprávy a 71 ze soukromé sféry.

Celkem 67 certifikátů informačních systémů bylo vydáno na žádost podanou v roce 2018.

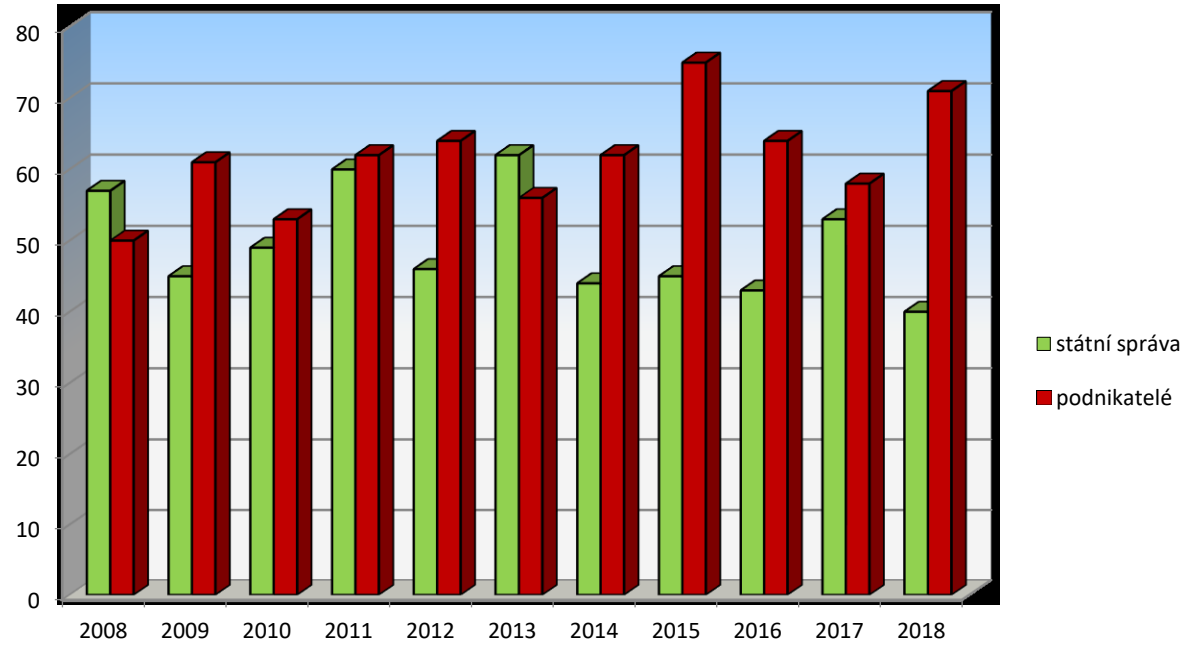
V 8 případech provozovatel informačního systému s certifikátem platným do data spadajícího do roku 2018 nepožádal o opakovanou certifikaci a platnost certifikátu automaticky skončila.

Řešené žádosti v roce 2018	Vydané certifikáty podle stupně utajení				Vydané certifikáty	
	Vyhrazené	Důvěrné	Tajné	Přísně tajné	státní správa	Podnikatelé
183	22,5 %	49,6 %	27,0 %	0,9 %	40	71

Přijaté žádosti o certifikaci informačního systému v letech 2008 až 2018



Vydané certifikáty informačních systémů v letech 2008 až 2018



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 2018 přibylo 8 žádostí o certifikaci nově budovaného informačního systému ze státní správy a 23 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 2018, kromě certifikace menších informačních systémů podnikatelů, několika ministerstev a úřadů (Ministerstvo práce a sociálních věcí, Ministerstvo průmyslu a obchodu, Ministerstvo zemědělství, Ministerstvo dopravy, Ministerstvo pro místní rozvoj, Úřad vlády ČR, Ústavní soud, Generální inspekce bezpečnostních sborů, Česká obchodní inspekce, Vězeňská služba, 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 a Bezpečnostní informační služby.

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 2018 Úřad provedl pro rezorty Ministerstva obrany, Ministerstva vnitra, Ministerstva zahraničních věcí a Bezpečnostní informační služby národní akreditaci 4 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 2018 byla na území ČR zahájena akreditace 8 součinnostních systémů, dokončení se předpokládá v roce 2019.

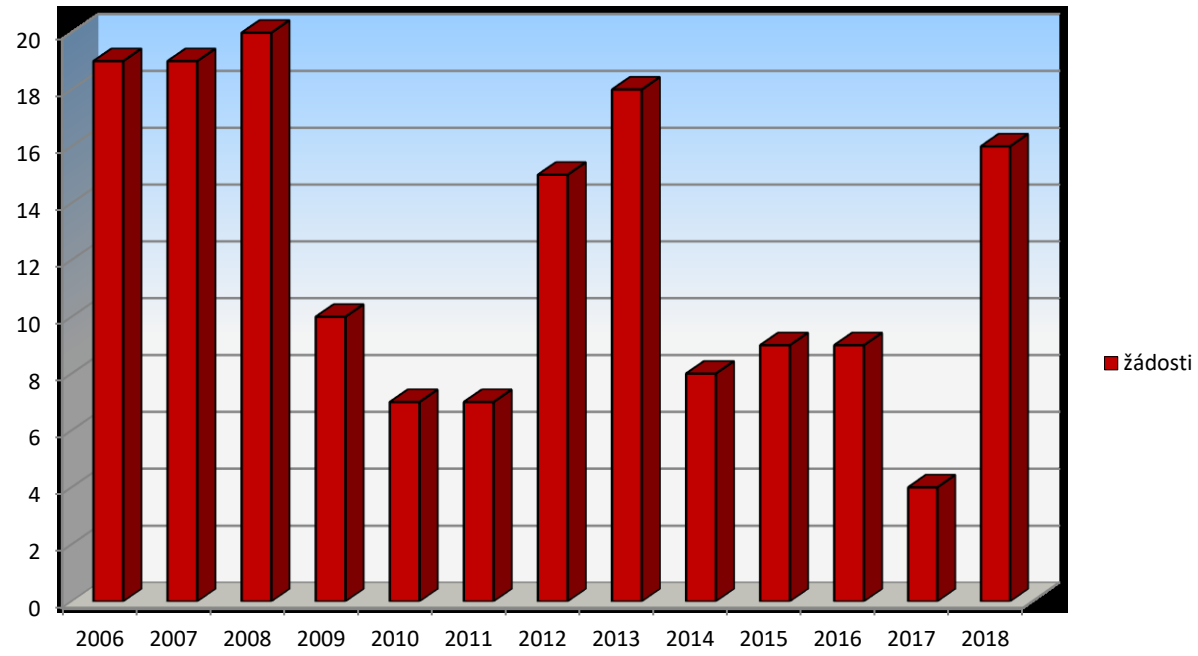
Certifikace kryptografických prostředků

V roce 2018 bylo Úřadu podáno celkem 16 žádostí o certifikaci kryptografického prostředku, z toho 6 na nový kryptografický prostředek. V řízeních k certifikaci kryptografického prostředku bylo vydáno 11 certifikátů, žádné řízení nebylo ukončeno bez vydání certifikátu. Stav řízení je shrnut v následující tabulce.

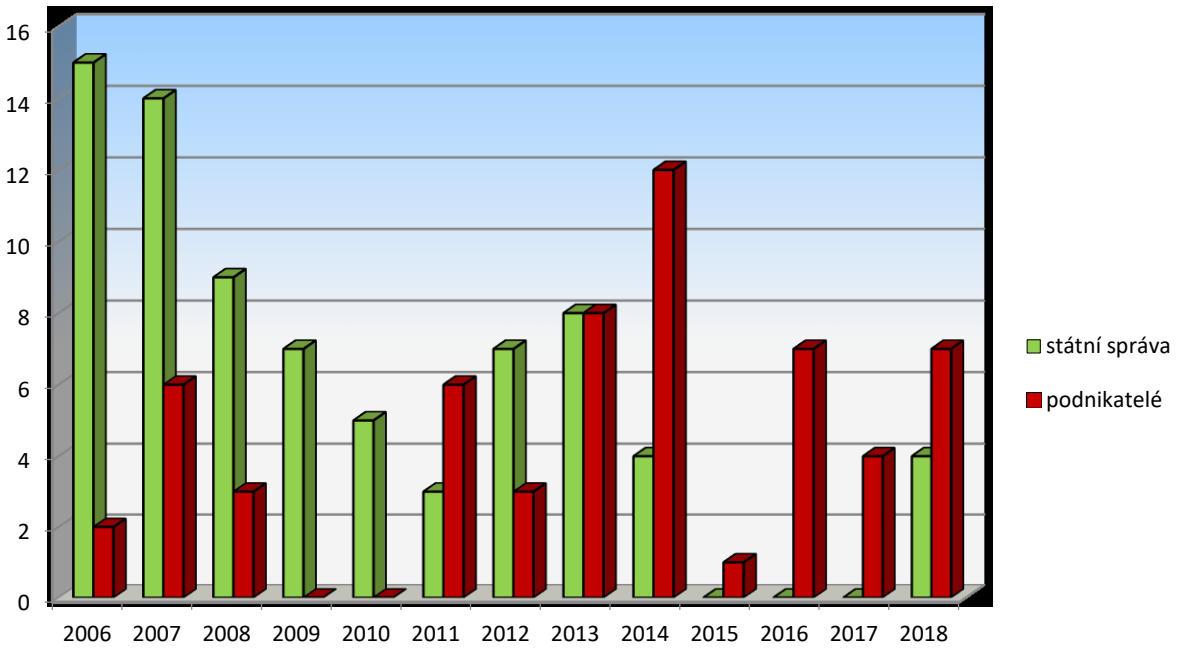
Certifikace kryptografických prostředků v roce 2018

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
16	8	8	0	0	4	7	10	10

Přijaté žádosti o certifikaci kryptografického prostředku v letech 2006 až 2018



Vydané certifikáty kryptografických prostředků v letech 2006 až 2018



Nově byly certifikovány kryptografické prostředky SINA L2 Box S, SINA L3 Box H a SECTRA Tiger/S XS, 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. pro systém SINA, LANPCS a PCS1. Nadále pokračovaly přípravné 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 SINA) a hlasové komunikace (systém SECTRA). Přehled aktuálně certifikovaných kryptografických prostředků je pravidelně zveřejňován ve Věstníku NÚKIB.

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 „Kontrolovaná kryptografická položka“ byly nově zařazeny dva kryptografické prostředky.

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 byla 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 2018 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. 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.

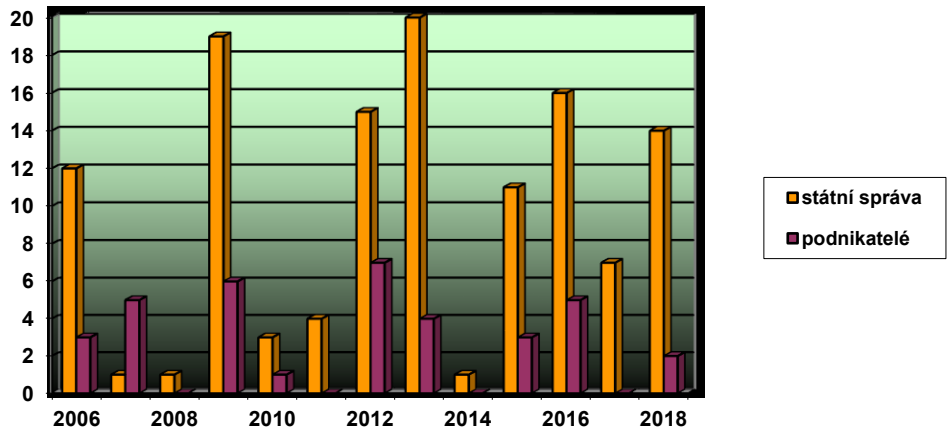
Certifikace kryptografických pracovišť

V roce 2018 bylo podáno celkem 16 žádostí o certifikaci kryptografického pracoviště. Většina žádostí o certifikaci spadá do kategorie opakovaných žádostí. Byly podány dvě žádosti o certifikaci nového kryptografického pracoviště, a dále jsou ještě další dvě žádosti ve stádiu posuzování. Z provedené certifikace vyplynulo, že umístění kryptografických pracovišť a provoz na nich je v souladu s reálnými potřebami příslušných organizací. V tomto rámci ovšem dochází k rozšiřování 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:

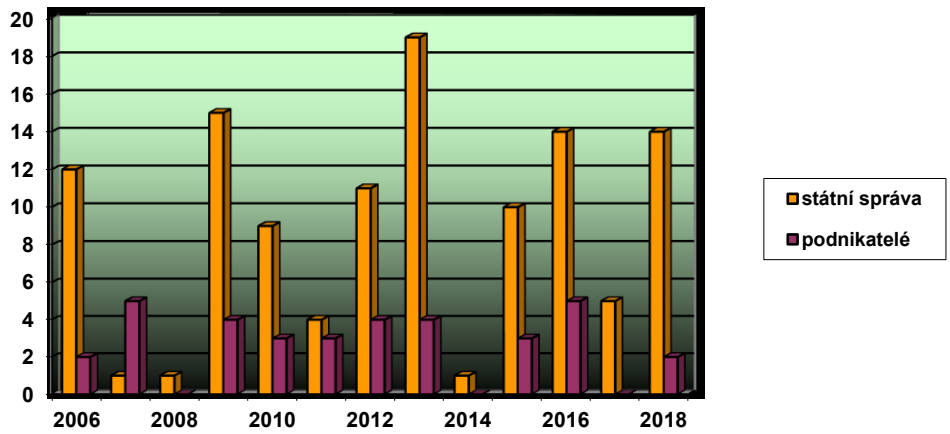
Certifikace kryptografických pracovišť v roce 2018

	Přijaté žádosti	Rozpracováno	Certifikováno	Zamítnuto	Zastaveno
Státní správa	14	2	14	0	0
Podnikatelé	2	0	2	0	0
Celkem	**16**	**2**	**16**	**0**	**0**

Přijaté žádosti o certifikaci kryptografického pracoviště v letech 2006 až 2018



Vydané certifikáty kryptografických pracovišť v letech 2006 až 2018



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 21 certifikátů stínicích komor, přičemž bylo využíváno i podkladů z měření provedených pracovníky Ministerstva zahraničních věcí na základě smlouvy o zajištění činnosti.

Další odborná činnost

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 2018 bylo v Úřadu vygenerováno celkem 96 342 kryptografických klíčů a hesel uložených na 7931 nosičích různých typů a dalších 73 ks jiného kryptografického materiálu (procesory, paměti, kryptografická dokumentace, instalační a šifrovací SW a FW).

Úřad vzal do evidence a provedl distribuci celkem 3885 ks nového kryptografického a CCI materiálu a dále zajistil servis a opravy na území ČR u 107 ks kryptografických prostředků a mimo ČR u 23 ks kryptografických prostředků.

Úřad zajistil výrobu, vzal do evidence a provedl distribuci celkem 83 ks kryptografického materiálu EU.

Pro zajištění výroby materiálu k zajištění funkce kryptografického prostředku HCrypt bylo v roce 2018 na pracovišti oddělení šifrové služby úspěšně otestováno nové středisko pro výrobu heslového materiálu.

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.

Měření kompromitujícího vyzařování (TEMPEST)

TEMPEST měření elektronických zařízení

Úřad prováděl v roce 2018 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 2018 provedeno více než 50 měření různých typů zařízení. Z toho bylo prováděno TEMPEST měření samostatných zařízení nebo v kombinaci s kryptografickým prostředkem 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 většina vyžádána Ministerstvem obrany.

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 10 lokalit.

V roce 2018 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.

Přehled provedených měření

Přehled měření v oblasti kompromitujícího vyzařování, provedených v roce 2018, je uveden v následující tabulce.

Měřená zařízení a objekty v roce 2017

Typ měření[9)]	Počet
Zónové měření	26 objektů
Kryptografické prostředky	2 typy
Komponenty ICT	více než 50 měření
Audiotechnika	2 typy zařízení
Obranné prohlídky i v rámci certifikace IS	14objektů
Mobilní systémy	2 systémy
Instalační záznamy	10 lokalit

Měření kompromitujícího vyzařování (TEMPEST)

TEMPEST měření elektronických zařízení

Úřad prováděl v roce 2018 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 2018 provedeno více než 50 měření různých typů zařízení. Z toho bylo prováděno TEMPEST měření samostatných zařízení nebo v kombinaci s kryptografickým prostředkem 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 většina vyžádána Ministerstvem obrany.

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.

[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.

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 10 lokalit.

V roce 2018 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.

Školení pracovníků kryptografické ochrany a zkoušky odborné způsobilosti

Úřad v roce 2018 organizačně zajistil a provedl, v souladu se zákonem, celkem 18 školení skupin pracovníků kryptografické ochrany a po následující zkoušce odborné způsobilosti vydal 90 osvědčení o zvláštní odborné způsobilosti pracovníka kryptografické ochrany. Kromě toho probíhají další školení a zkoušky odborné způsobilosti na Ministerstvu vnitra, Ministerstvu obrany a Ministerstvu zahraničních věcí na základě smluv uzavřených mezi Úřadem a uvedenými ministerstvy.

Kontroly ochrany utajovaných informací (státní dozor)

V roce 2018 provedl Úřad ve smyslu §143 odst. 6 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti 19 kontrol za oblast bezpečnosti informačních nebo komunikačních systémů, případně kryptografické ochrany. Z tohoto počtu bylo 9 kontrol provedeno v rámci státní správy a 10 kontrol u podnikatelů.

Problémové oblasti bezpečnosti informačních a komunikačních systémů a kryptografické ochrany

Zákonem stanovené činnosti Úřadu v oblasti bezpečnosti informačních systémů nakládajících s utajovanými informacemi a kryptografické ochrany byly v roce 2018 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 je získání nových odborníků 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 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.

Výzkumná a vývojová činnost Úřadu v oblasti ochrany utajovaných informací

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.

Projekty realizované v roce 2018

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 řádně dokončeno devět projektů zahájených v letech 2016 a 2017. Zahájen byl jeden nový projekt a pokračuje řešení dvou projektů započatých v roce 2017. Všechny uvedené projekty byly realizovány ve spolupráci s externími řešiteli.

Projekty se věnovaly oblasti kryptografické ochrany, ochrany proti úniku utajovaných informací kompromitujícím vyzařováním, hodnocení informačních a komunikačních systémů a implementaci veřejně regulované služby globálního navigačního systému Galileo.

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

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

V roce 2018 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 resortů státní správy, pro které jsou tyto druhy zajištění ochrany utajovaných informací nezbytné.

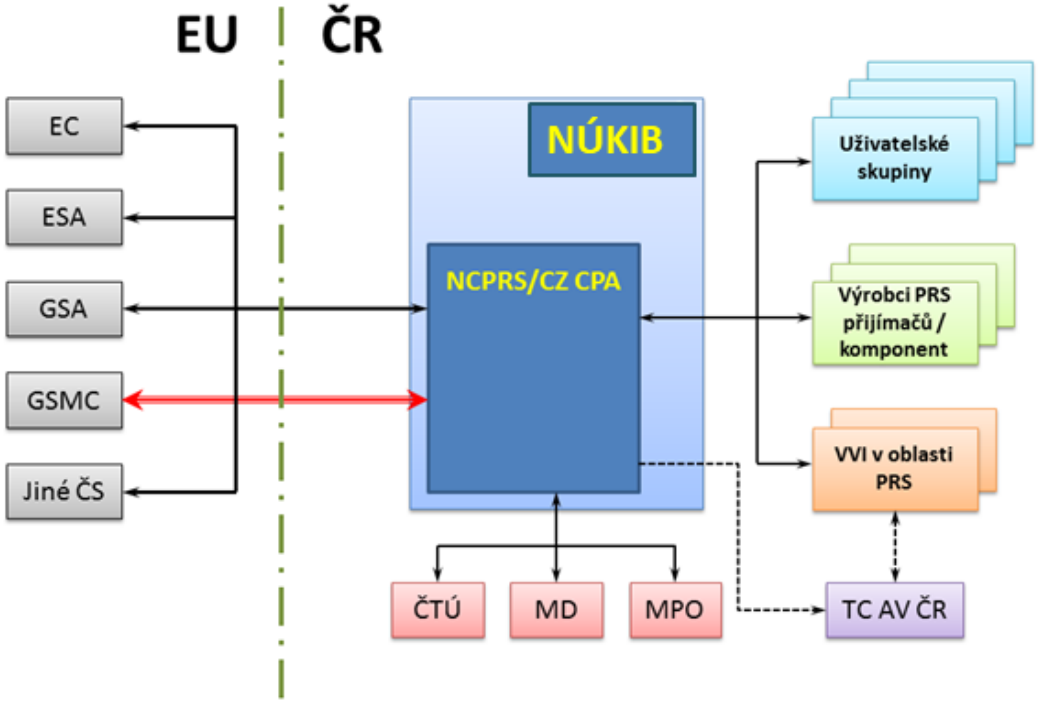
Výkon funkce příslušného orgánu PRS

Usnesením vlády ČR ze dne 30. ledna 2013 č. 71 k Akčnímu plánu implementace veřejně regulované služby programu Galileo (Public Regulated Service, dále jen „PRS“) v České republice byla převedena problematika služby PRS z kompetence rezortu Ministerstva dopravy na Úřad. 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“).

Budování národního centra PRS

Implementace služby PRS v ČR probíhá na základě schváleného Akčního plánu implementace PRS v ČR. V souladu se schváleným finančním rámcem a personálními opatřeními Úřad pokračuje v budování Národního centra 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 schématu:

Organizační schéma zabezpečení služby PRS v ČR



Součástí povinností, kterými je NCPRS pověřeno, je mimo jiné též reprezentace Úřadu, resp. ČR v pracovních skupinách programu Galileo (EU) řešících problematiku bezpečnosti programu Galileo a PRS. Tato aktivita přirozeně pokračovala i v roce 2018. Dalším důležitým úkolem NCPRS je koordinace aktivit spojených s přístupem k informacím a technologiím služby PRS. NCPRS v souladu se stanovenými podmínkami zajišťuje, aby subjekty se sídlem v ČR, které se chtějí podílet na výrobě nebo vývoji přijímačů PRS, bezpečnostních modulů či technologií s integrovanou službou PRS, splňovaly požadavky fyzické a administrativní bezpečnosti a byla jim udělena bezpečnostní akreditace.

NCPRS bylo také aktivní v oblasti propagace a osvěty služby PRS mezi jejími potenciálními uživateli. Zorganizovalo či se podílelo na organizaci několika událostí zaměřených na tematiku rozvoje uživatelského segmentu.

V daném roce též pokračovala intenzivní příprava pro testování služby PRS v rámci projektu společného testování „Joint Test Activities“, vyhlášeného Agenturou pro evropský GNSS. Vzhledem k tomu, že se jedná o projekt s mezinárodní účastí, proběhla řada jednání jak se zahraničními partnery projektu, tak se samotnou Agenturou pro evropský GNSS. Ke konci roku 2018 byl zahájen proces nákupu technologií potřebných pro úspěšné provedení projektu. Samotná realizace bude uskutečněna v závislosti na dostupnosti speciálních přijímačů PRS pravděpodobně v roce 2019.

V souladu s výstupy z projektů výzkumu a vývoje a na základě postupně uvolňovaných informací ze strany Evropské komise a ESA byly realizovány některé nákupy techniky a technologií nezbytných pro zabezpečení chodu NCPRS.

Personální obsazení NCPRS

Nárůst agendy spojené zejména s řešením problematiky služby PRS na evropské úrovni (řešení technologických otázek vývoje systému pro dosažení plných operačních schopností a řešení projektů na rozvoj uživatelského segmentu) a zapojení ČR do přípravy a následné realizace pilotních projektů služby PRS vedl k požadavku na rozšíření pracovního týmu NCPRS. Na tomto základě bylo vypsáno výběrové řízení na obsazení dalších dvou pracovních míst. Personální obsazení bylo řešeno v součinnosti s Oddělením personálním a na konci roku 2018 byla obsazena jedna nová pozice s výhledem na obsazení další pozice na začátku roku 2019.

Spolupráce s ostatními subjekty při implementaci služby PRS

Při řešení problematiky služby PRS NCPRS úzce spolupracuje zejména s Ministerstvem dopravy coby národním koordinátorem pro správu a řízení evropských systémů družicové navigace. V roce 2018 byla též prohloubena spolupráce s Ministerstvem obrany, a to jak z důvodu zapojení do projektu společného testování PRS, tak z důvodu potenciálního využití služby PRS Armádou ČR.