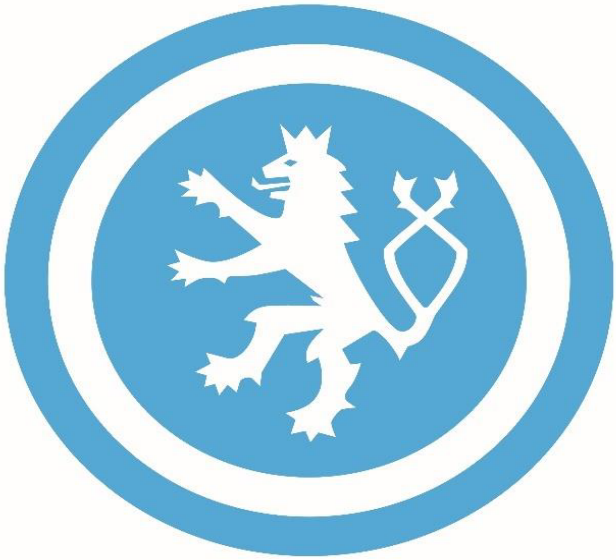
NÚKIB



Národní úřad pro kybernetickou a informační bezpečnost

Z P R Á V A

O ČINNOSTI

NÁRODNÍHO ÚŘADU PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST

ZA ROK 2019

Praha 2020

Obsah

Úvod

Národní úřad pro kybernetickou a informační bezpečnost (dále jen „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 KII, PZS a VIS 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 (dále jen „zákon o kybernetické bezpečnosti“), vybraných částí zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů (dále jen „zákon o ochraně utajovaných informací“), a samozřejmě také prováděcích předpisů k uvedeným zákonům. Cílem regulace podle těchto zákonů a jejich prováděcích předpisů je zajištění kybernetické bezpečnosti v informačních systémech KII, VIS, informačních systémech PZS a dalších systémech, ve kterých jsou zpracovávány neutajované informace, a kybernetické bezpečnosti informačních a komunikačních systémů nakládajících s utajovanými informacemi.

V roce 2019 NÚKIB připravil novelizaci zákona o kybernetické bezpečnosti, přijaté zákonem č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů, kterou byl zejména kompletně upraven katalog přestupků a precizováno ustanovení o bezpečnostních opatřeních, a podílel se také na přípravě novelizace zákona o ochraně utajovaných informací.

Velmi významnou oblast z hlediska kybernetické bezpečnosti představuje v současnosti cloud computing. V roce 2019 se uskutečnilo mnoho zákonodárných aktivit týkajících se využívání služeb cloud computingu orgány veřejné moci. NÚKIB k těmto aktivitám přispíval kvalifikovanou oponenturou, popřípadě přípravou vlastních návrhů legislativních řešení. Do konce roku však nebyla zákonná právní úprava stabilizována. Legislativní činnost bude pokračovat v roce 2020.

V daném roce pokračovaly také legislativní 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.

Vedle přijetí výše uvedených vlastních právních předpisů NÚKIB v roce 2018 posoudil v meziresortním připomínkovém řízení více než 120 materiálů legislativní i nelegislativní povahy, přičemž více než ke čtvrtině 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 NÚKIB 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 (zákon o finanční kontrole), ve znění pozdějších předpisů (dále jen „zákon o finanční kontrole“). Postavení interního auditu je nezávislé na organizační struktuře NÚKIB a interní audit je administrativně a funkčně podřízen řediteli NÚKIB.

Začátkem roku 2019 byly vydány interní normativní akty Manuál interního auditu, který stanoví zásady a postupy výkonu interního auditu a Program pro zabezpečení a zvyšování kvality interního auditu ke zdokonalování jeho procesů.

Výkon interního auditu probíhal taktéž v souladu s interním normativním aktem Vnitřní kontrolní systém, který upravuje organizaci a fungování vnitřního kontrolního systému NÚKIB 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 NÚKIB tyto složky:

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

Ve spolupráci interní auditorky a vedoucích zaměstnanců byla identifikována a vyhodnocena

rizika vyskytující se na NÚKIB. 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.

Interní auditorka spolu s příkazci operací zpracovala zprávu 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.

Začátkem roku byl taktéž vypracován Plán auditu pro rok 2019, ve kterém byly naplánovány 3 interní audity a 1 následný audit zaměřený na prověření realizace doporučení a úkolů z vykonaného auditu veřejných zakázek v roce 2018.

V roce 2019 byl proveden interní audit pokladny, interní audit spisové služby a byl zahájen audit cestovních náhrad.

Interní audit pokladny byl zaměřen na prověření hotovostního platebního styku a kontrolu vybraných operací s ohledem na jejich legalitu, účelnost, hospodárnost a efektivitu. Interní audit spisové služby se věnoval oblasti řízení dokumentů, záznamů a aplikací požadavků zákona č. 499/2004 Sb., o archivnictví, ve znění pozdějších předpisů včetně souvisejících vyhlášek. Pozornost interního auditu cestovních náhrad byla upřena na kontrolu postupu při vysílání zaměstnance na pracovní cestu a poskytování náhrad výdajů zaměstnanci při pracovní cestě, kontrola vybraných operací s ohledem na jejich legalitu, účelnost, hospodárnost a efektivitu.

Veškerá auditní zjištění byla projednána s řediteli auditovaných útvarů tak, aby byla zajištěna smysluplnost auditních doporučení, jejich implementace a následná zpětná vazba. Je zavedena evidence těchto doporučení.

Mimo auditní činnost byla náplní 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 NÚKIB je projednávání přestupků stanovených zákonem o kybernetické bezpečnosti a ukládání správních trestů za jejich spáchání. Do působnosti NÚKIB přitom spadá nejen projednávání přestupků podle § 25 a násl. zákona o kybernetické bezpečnosti, ale zároveň i vybírání pokut, jež NÚKIB v rozhodnutí o spáchání přestupku pachateli uloží.

V roce 2019 zahájil NÚKIB jedno přestupkové řízení pro podezření ze spáchání přestupku stanoveného zákonem o kybernetické bezpečnosti. Toto řízení nebylo do konce roku 2019 pravomocně skončeno.

NÚKIB rovněž projednává některé přestupky podle části osmé zákona o ochraně utajovaných informací. Jedná se o přestupky proti bezpečnosti utajovaných informací v informačních a komunikačních systémech a proti bezpečnosti utajovaných informací při kryptografické ochraně. I

podle zákona o ochraně utajovaných informací platí, že NÚKIB pokuty nejen ukládá, ale tyto zároveň i vybírá.

V roce 2019 NÚKIB prošetřoval 5 nových podnětů, podle nichž mohlo dojít ke spáchání přestupků upravených zákonem o ochraně utajovaných informací, a to především z důvodu nakládání s utajovanou informací v necertifikovaném informačním systému. Prošetřování důvodnosti těchto podnětů nebylo do konce roku 2019 ukončeno.

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

NÚKIB bylo v roce 2019 doručeno celkem 13 žádostí o poskytnutí informací podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů (dále jen „zákon č. 106/1999 Sb.“). V plném rozsahu byly informace poskytnuty v 9 případech. Ve 3 případech byla žádost částečné odmítnuta za současného částečného poskytnutí požadovaných informací. V plném rozsahu byla žádost odmítnuta v 1 případě.

Poskytnuté informace byly zveřejňovány v souladu s § 5 odst. 3 zákona č. 106/1999 Sb..

Statistiky k poskytování informací podle zákona č. 106/1999 Sb. ve vztahu k NÚKIB:

1. Počet podaných žádostí o informace podle zákona č. 106/1999 Sb. a počet vydaných rozhodnutí o odmítnutí žádosti (i částečném) podle oblastí:

Poskytování informací dle zákona č. 106/1999 Sb., podle oblastí v roce 2019	**Počet podaných žádostí**	**Počet vydaných rozhodnutí o odmítnutí žádosti**
Kybernetická bezpečnost	6	3
Vzdělávání	1	0
Všeobecné	6	1
Celkem	13	4

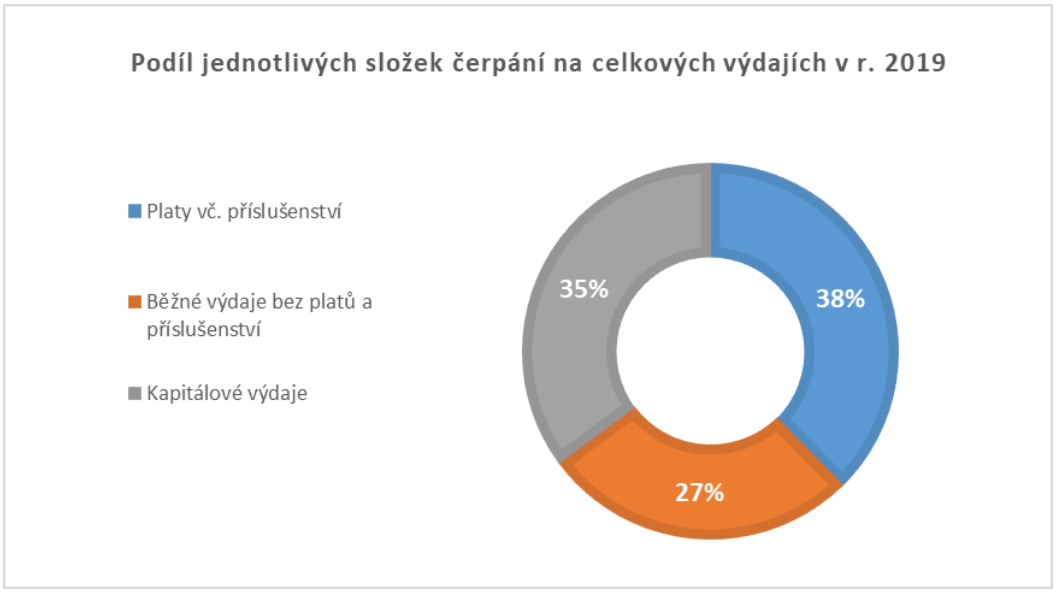
2. Počet podaných odvolání proti rozhodnutí NÚKIB podle zákona č. 106/1999 Sb.: žádné odvolání.
3. Počet podaných stížností na postup při vyřizování žádosti podle § 16 zákona č. 106/1999 Sb.: žádné stížnosti.
4. Rozsudky soudu ve vztahu k NÚKIB v oblasti poskytování informací: žádný rozsudek.
5. Výsledky 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

NÚKIB je od 01.08.2017 samostatnou kapitolou státního rozpočtu pod číslem 378.

Plánovaný rozpočet NÚKIB byl v roce 2019 ve výši 352,5 mil. Kč a byl upravován celkem jedenácti rozpočtovými opatřeními MF na celkovou částku **388,3 mil. Kč.**
K 31. 12. 2019 bylo vyčerpáno z upraveného rozpočtu **325,8 mil. Kč**, tj. 84 %. **Konečný rozpočet** celkových výdajů kapitoly za rok 2019, tedy rozpočet včetně zapojených nároků z nespotřebovaných výdajů ve výši 150 mil. Kč, byl v objemu **538,5 mil. Kč**. Čerpání konečného rozpočtu bylo v relativním vyjádření na 83 %, v absolutním vyjádření ve výši 444,8 mil. Kč.

Částka ve výši 10 mil. Kč z nároků z nespotřebovaných výdajů nebyla do rozpočtu roku 2019 zapojena. Jednalo se o investiční akce s plánovanou realizací po roce 2019, jmenovitě o část rozpočtových prostředků akce Národní Scrubbing Centrum a o investiční akci Honeypoty. Dále, objem nároků z nespotřebovaných výdajů ve výši 39,4 mil. Kč byl ukončen, neboť se jednalo o nečerpaný rozpočet úspěšně zrealizovaného EU projektu „SONDY“.



Výdaje na platy a příslušenství

Výdaje na platy a příslušenství byly rozpočtovány ve výši 138,4 mil. Kč pro 203 pracovních míst. Na žádost NÚKIB byly výdaje rozpočtovými opatřeními v kompetenci MF ČR upraveny na 167 mil. Kč. Zapojením nároků z nespotřebovaných výdajů byly upraveny na **konečný rozpočet ve výši 168,6 mil. Kč pro 211 pracovních míst (v ročním průměru to bylo pro 207 pracovních míst)**. Konečný rozpočet výdajů na platy a příslušenství byl čerpán ve výši 167,5 mil. Kč, tedy v relativním vyjádření na 99 %.

V období od 1. ledna 2019 do 31. prosince 2019 nastoupilo na NÚKIB 32 nových zaměstnanců a 19 zaměstnanců skončilo pracovní poměr. Průměrný plat, k průměrnému ročnímu přepočtenému počtu 197,13 zaměstnanců, činil 51 636 Kč.

Běžné výdaje

Běžné výdaje (bez výdajů na platy a příslušenství a bez běžných výdajů v rámci projektů EU) byly rozpočtovány ve výši 137,4 mil. Kč.

Rozpočtovými opatřeními byly upraveny na 141,5 mil. Kč. Zapojením nároků z nespotřebovaných výdajů byly upraveny na **konečný rozpočet ve výši 180,4 mil. Kč. Konečný rozpočet běžných výdajů byl čerpán v objemu 121 mil. Kč, v relativním vyjádření na 67 %.**

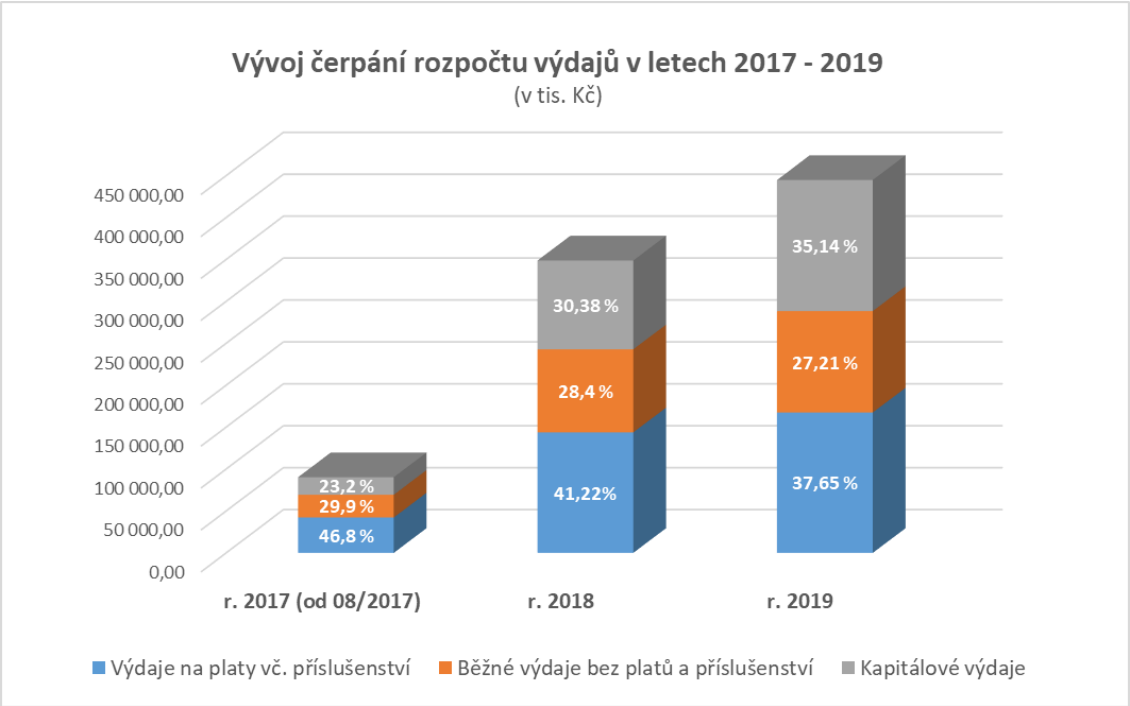
Kapitálové výdaje

Kapitálové výdaje jsou evidovány v informačním systému programového financování (Správa majetku ve vlastnictví státu-„SMVS"), a to pro kapitolu 378-NÚKIB ve výdajovém titulu „Rozvoj a obnova materiálně-technické základny Národního úřadu pro kybernetickou a informační bezpečnost".

Kapitálové výdaje vedené v SMVS byly rozpočtovány ve výši 76,7 mil. Kč.
Rozpočtovými opatřeními byly výdaje upraveny na 79,8 mil. Kč. Zapojením nároků z nespotřebovaných výdajů byly upraveny na **konečný rozpočet výdajů vedených v SMVS v objemu 190 mil. Kč. Konečný rozpočet kapitálových výdajů tak byl čerpán v objemu 156,2 mil. Kč, v relativním vyjádření na 82 %.** Částka ve výši 10 mil. Kč z nároků z nespotřebovaných výdajů nebyla do rozpočtu roku 2019 zapojena. Jednalo se o investiční akce s plánovanou realizací po roce 2019, jmenovitě o část rozpočtových prostředků akce Národní Scrubbing Centrum a o investiční akci Honeypoty.

Nejvýznamnější objem finančních prostředků byl vynaložen na výstavbu, posílení a obnovu ICT infrastruktury NÚKIB, a to téměř 100 mil. Kč. Dále bylo vynaloženo 24,6 mil. Kč na ochranu vnějšího perimetru (EU projekt „PERIMETR") a částka 1,7 mil. Kč na dokončení EU projektu „SONDY".

U investiční akce Architektonická soutěž a projektová dokumentace – ČERNÁ POLE proběhla v roce 2019 mezinárodní architektonická soutěž a výdaje činily 4,3 mil. Kč.



Evidence nároků z nespotřebovaných výdajů (dále jen „NNV“)

Celkové nároky z nespotřebovaných výdajů byly k 1. lednu 2019 ve výši 199,5 mil. Kč.

Celkem za rok 2019 bylo vyčerpáno z nároků z nespotřebovaných výdajů 119 mil. Kč.

Objem NNV ve výši 39,4 mil. Kč byl ukončen, neboť se jednalo o nečerpaný rozpočet zrealizovaného EU projektu „SONDY“.

Zůstatek nároků z nespotřebovaných výdajů k 31. prosinci 2019 byl ve výši 41,1 mil. Kč.

Převážnou část z celkového zůstatku nároků z nespotřebovaných výdajů roku 2019 ve výši 41,1 mil. Kč tvoří kapitálové výdaje, a to v objemu 26,3 mil. Kč. Kapitálové výdaje jsou plánovány k dočerpání během roku 2020, vyjma investiční akce Honeypoty. NNV účelově určené ve výši 3,9 mil. Kč budou využity na vymezené účely během roku 2020 (III. etapa oprav objektu Cejl Brno, dobudování pracoviště PRS). Nároky z nespotřebovaných neprofilujících výdajů v objemu 4,2 mil. Kč budou v roce 2020 použity na pokrytí plošného 10% krácení běžných výdajů v rámci návrhu státního rozpočtu na rok 2020. Poslední část NNV ve výši 6,7 mil. Kč byla již v lednu 2020 ukončena, neboť se jedná o nečerpaný rozpočet zrealizovaného EU projektu „PERIMETR“.

Vnitřní finanční kontroly a interní audit

Řídící a kontrolní mechanismy jsou pro jednotlivé oblasti činnosti NÚKIB nastaveny prostřednictvím interních normativních aktů řízení v souladu s ustanovením § 3 odst. 4 zákona č. 320/2001 Sb., o finanční kontrole. Interní normativní akty řízení NÚKIB tvoří základ jeho vnitřního kontrolního systému.

V průběhu roku 2019 byl zajišťován výkon řídící kontroly jednotlivými příkazci operací, hlavní účetní a správcem rozpočtu. V rámci své působnosti prováděly jmenované osoby finanční řídící

kontroly při hospodaření s finančními prostředky na příslušných rozpočtových položkách NÚKIB v rámci jeho rozpočtové skladby.

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 NÚKIB.

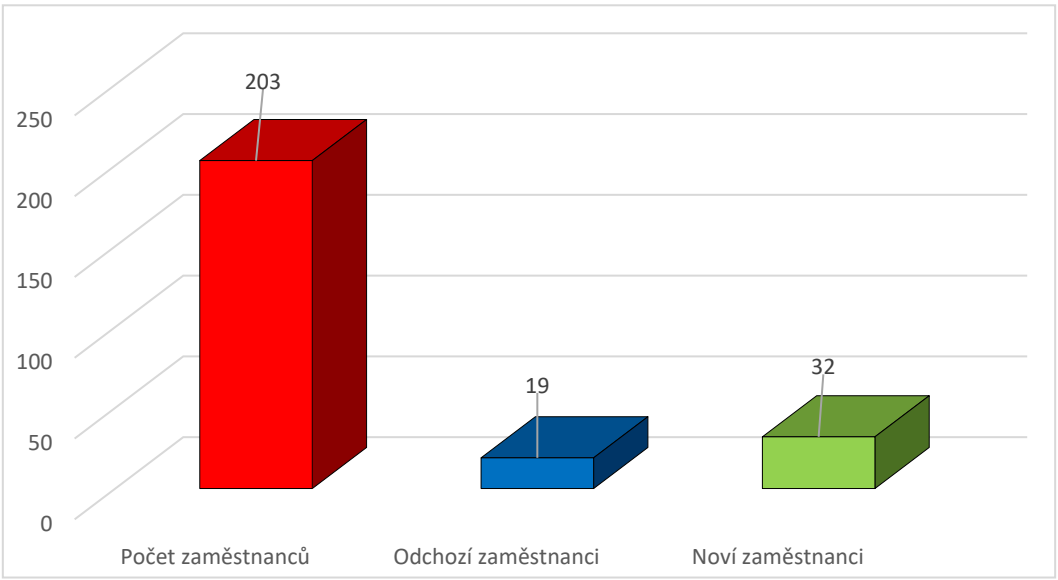
Personální zabezpečení úřadu

Personální zabezpečení úřadu

V roce 2019 byla postupně obsazována pracovní místa novými zaměstnanci. Do pracovního poměru v období od 1. 1. 2019 do 31. 12. 2019 bylo přijato 32 nových zaměstnanců. Dalších 13 zaměstnanců vykonávalo činnost na základě uzavřených dohod o pracích konaných mimo pracovní poměr.

Do konce roku 2019 ukončilo 19 zaměstnanců pracovní poměr, tj. 9,35% z celkového počtu zaměstnanců. Z tohoto počtu 4 zaměstnanci ukončili pracovní poměr uplynutím doby určité a 16 zaměstnanců v souladu se zákonem č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů, z toho 2 zaměstnanci dle § 52c tohoto zákona.
Nejčastější důvod pro odchod bylo ukončení pracovního poměru dohodou na žádost zaměstnance – 5 a dále výpověď ze strany zaměstnance – 8.

Nástupy a odchody zaměstnanců v roce 2019

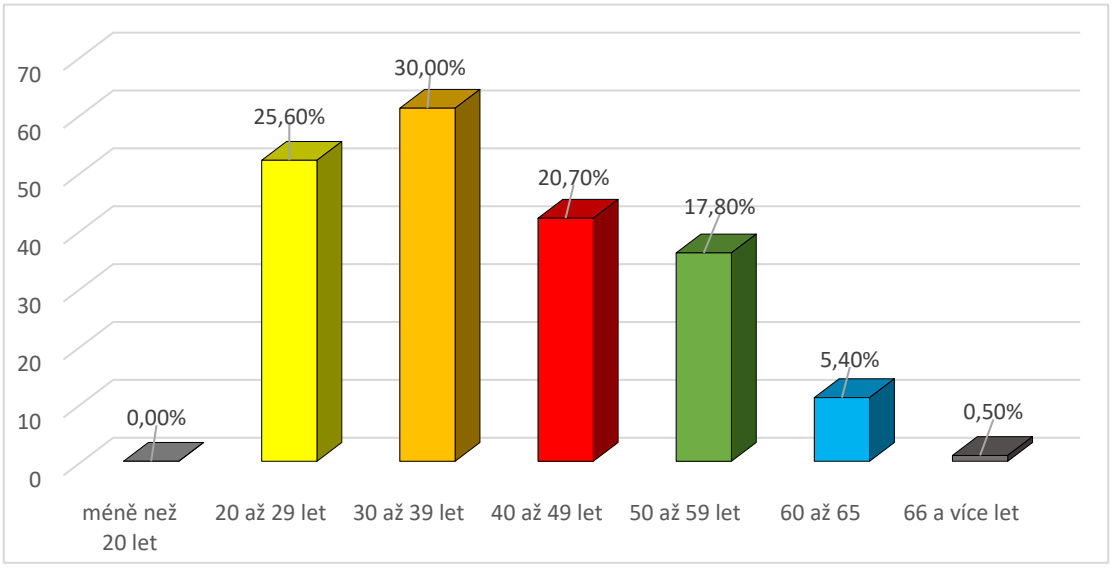


Věková struktura zaměstnanců k 31.12.2019

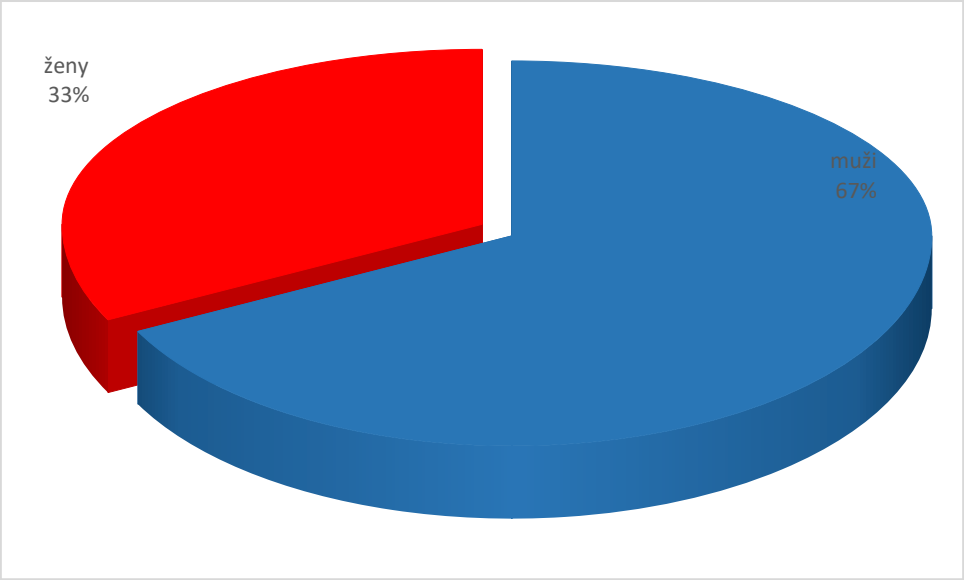
V následující tabulce uvádíme celkovou věkovou strukturu zaměstnanců:

Věková kategorie	Počet zaměstnanců k 31. 12. 2019	Podíl zaměstnanců v %	Z toho	
			muži	ženy
méně než 20 let	0	0,0 %	0	0
20 až 29 let	52	25,6 %	34	18
30 až 39 let	61	30,0 %	43	18
40 až 49 let	42	20,7 %	27	15
50 až 59 let	36	17,8 %	23	13
60 až 65	11	5,4 %	9	2
66 a více let	1	0,5 %	1	0
Celkem	**203**	**100,0 %**	**137**	**66**

Struktura zaměstnanců Úřadu podle věku (%)



Struktura zaměstnanců Úřadu – ženy/muži



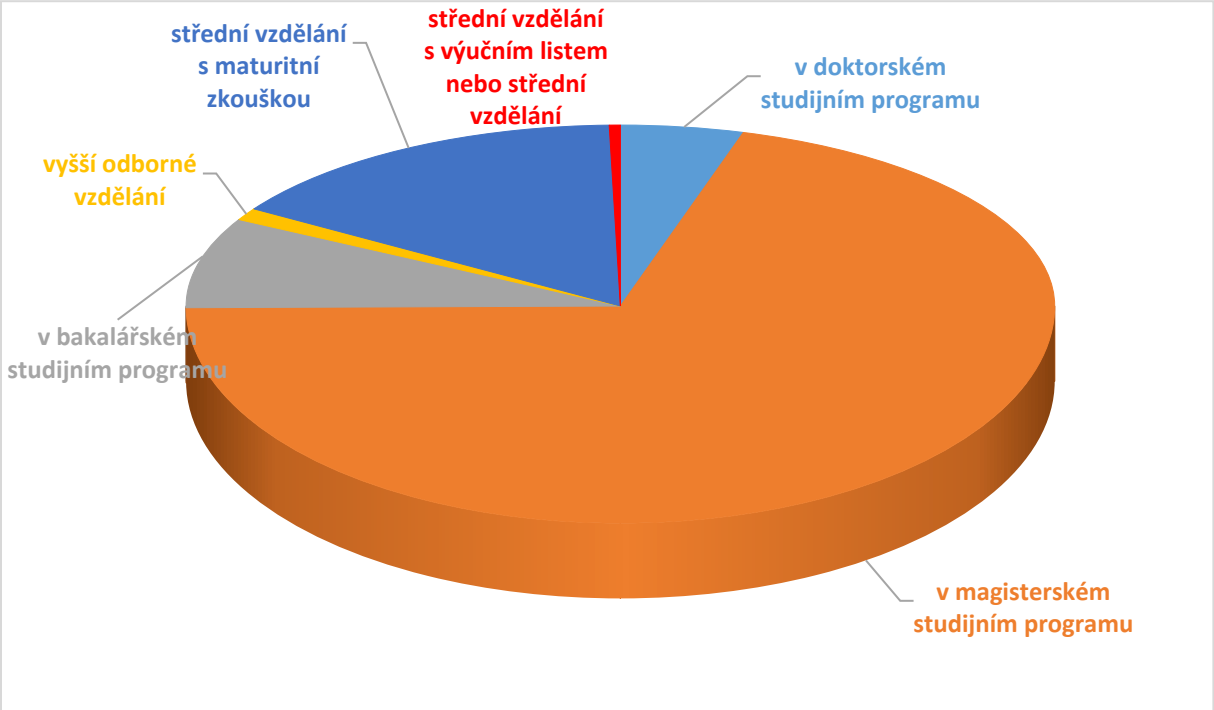
K 31. 12. 2019 bylo v evidenčním stavu celkem 203 zaměstnanců, z toho 67,5% mužů a 32,5% žen. Průměrný věk zaměstnanců úřadu je 39,4 let.

Kvalifikační struktura zaměstnanců

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

Dosažené vzdělání k 31. 12. 2019	Počet zaměstnanců k 31. 12. 2019	Procentní struktura
v doktorském studijním programu	11	5,4%
v magisterském studijním programu	141	69,5%
v bakalářském studijním programu	14	6,9%
vyšší odborné vzdělání	2	1,0%
střední vzdělání s maturitní zkouškou	34	16,7%
střední vzdělání s výučním listem nebo střední vzdělání	1	0,5%
základní vzdělání		
Celkem	**203**	**100%**

Struktura zaměstnanců podle vzdělání



Vzdělávání a rozvoj zaměstnanců

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

Za rok 2019 NÚKIB realizoval školení převážně v oblasti kybernetické bezpečnosti a informačních technologií jak v ČR, tak i v zahraničí. Převážná část školení byla zakončena certifikační zkouškou. Zaměstnanci NÚKIB zařazení do sekce NCKB a sekce technické se zúčastnili školení v oblasti předcházení, detekce a reakce na kybernetické útoky, zabezpečení serverů, bezpečnosti dat, bezpečné komunikace a šifrování, bezpečnosti webových aplikací, penetračního testování, kryptografie a další. Rovněž byla věnována pozornost i dalšímu odbornému vzdělávání zaměstnanců v oblastech, souvisejících s jejich pracovní činností, především v oblasti ekonomické a právní, u hromadných vzdělávacích akcí v oblasti projektového řízení, úpravy písemností podle ČSN 01 6910 a souvisejících zákonů a norem a v oblasti finanční kontroly.

Vzdělávání je zabezpečováno formou individuálních a hromadných vzdělávacích akcí.

Zaměstnávání osob se zdravotním postižením

NÚKIB je podle § 83 zákona č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů, povinen plnit stanovený podíl osob se zdravotním postižením. Jeho naplňování je dáno jednak zaměstnáváním osob se zdravotním postižením, jednak odběrem výrobků a služeb od zaměstnavatelů, kteří zaměstnávají více než 50% osob se zdravotním postižením.
Plnění povinného podílu bylo splněno zaměstnáváním osob se zdravotním postižením ve výši 1,48 osoba a odebíráním výrobků a služeb ve výši 7,11 osob.

Spolupráce s vysokými školami a odborné praxe studentů škol

Vedle pracovních příležitostí NÚKIB rovněž poskytuje za účelem přípravy na budoucí povolání praktické stáže pro vysokoškolské studenty, a to nejen v rámci povinné praxe dle studijních osnov, ale i z vlastního zájmu studentů z důvodu získání pracovních a oborných zkušeností pro svou budoucí kariéru.

V roce 2019 absolvovalo stáž 13 studentů, což bylo o 6 více než v roce 2018. Stáže byly jak technického, tak právního a politicko-bezpečnostního zaměření. Součástí spolupráce se studenty jsou také pravidelné odborné konzultace diplomových a seminárních prací.

Spokojení a motivovaní zaměstnanci jsou základní podmínkou pro zvyšování kvality práce, odpovědnosti, spolupráce a ochoty. Proto se snažíme pečovat o své zaměstnance, udržovat s nimi dobré vztahy a i přes problémy spojené s budováním pracovišť NÚKIB vytvářet dobré pracovní podmínky a zázemí.

Oddělení investic a rozvoje

V roce 2019 se realizovalo další rozšíření kancelářských prostor v objektu Cejl v Brně. Dále, v rámci objektu Cejl byla zpracována projektová dokumentace na opravu fasády.

Na pracovišti Vysoké učení technické v Brně – Fakulta Podnikatelská byl zpracován projektový záměr na rozšíření a optimalizace kancelářských prostor pro zaměstnance odboru OKBP.

Nová administrativní budova NÚKIB v Brně, Černá Pole

V lednu 2019 bylo vedením NÚKIB schváleno složení nezávislé a závislé části hodnotící poroty pro architektonickou soutěž na novou administrativní budovu. Porota vzešla z doporučení administrátora, přičemž se skládá z tuzemských odborníků na architektonická řešení a jednoho zahraničního architekta. Projektový tým a Administrátor soutěže zpracovali Zadávací dokumentaci, která byla následně zveřejněna prostřednictvím národního certifikovaného nástroje k zadávání veřejných zakázek (NEN) mezinárodní otevřenou dvoufázovou projektovou architektonickou soutěž o návrh „Černá Pole“, jejímž předmětem bylo navrhnout pro NÚKIB nové sídlo, které musí splňovat

vysoké nároky na efektivní práci jeho pracovníků, podporu inovativnosti, špičkové technologické vybavení, konkurenceschopné pracovní prostředí a bezpečnost. V červnu proběhlo první kolo hodnocení předložených návrhů, na kterém porota hodnotila 18 předložených návrhů a rozhodla o pěti návrzích, které nejlépe naplnily soutěžní zadání a jevily se jako nejvíce vyhovující (z hlediska možné variability, možnosti rozšíření, bezpečnosti apod.), ty postoupily do druhého kola architektonické soutěže o návrh „Černá Pole“. Zasedání poroty pro druhé kolo soutěže proběhlo v srpnu, kde hodnotící porota stanovila pořadí jednotlivých návrhů a rozhodla o ocenění prvních tří míst.

Po schválení výsledků vedením NÚKIB byla Soutěž o návrh (architektonická soutěž) uzavřena 2. října 2019. V návaznosti na to projektový tým NÚKIB společně s administrátorem soutěže připravil zadávací dokumentaci pro jednací řízení bez uveřejnění se třemi oceněnými účastníky soutěže o návrh (tj. 1. až 3. místo v soutěži o návrh), které navazuje na soutěž o návrh. Proběhla jednání se třemi oceněnými účastníky soutěže. Do konce roku 2019 nebylo Jednací řízení bez uveřejnění uzavřeno a bude probíhat i v roce 2020. Výsledkem tohoto řízení bude uzavření smlouvy na zpracování projektové dokumentace.

Odbor kybernetických bezpečnostních politik

Národní spolupráce

Na zvyšování úrovně kybernetické bezpečnosti ČR se nepodílí pouze NÚKIB, ale jedná se o širokou spolupráci na národní úrovni, kde NÚKIB jako národní gestor dané oblasti aktivně spolupracuje s ostatními subjekty nejenom státní správy. Snaží se tak harmonizovat jednotný postoj ČR i směrem do zahraničí. Na této spolupráci se taktéž podílí akademická sféra, spolu s níž NÚKIB připravuje budoucí odborníky a navyšuje celkové povědomí o kybernetické bezpečnosti. Dále např. s bezpečnostními týmy CSIRT sdílí NÚKIB informace a zkušenosti se zranitelnostmi a podílí se na vývoji nových technických nástrojů.

Národní spolupráci z velké části zajišťuje oddělení národních strategií a politik, které i v roce 2019 připravilo vyhodnocení plnění Akčního plánu, který kontroluje specifické úkoly vedoucí k naplňování Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020. Rok 2019 byl taktéž předposledním rokem plnění současného Akčního plánu. To se projevilo na klesajícím absolutním počtu zadaných úkolů v porovnání s předešlými roky a v roce 2019 došlo navíc

k plnění nesplněných úkolů z minulých let. Oproti letům minulým nedošlo v roce 2019 k neplnění úkolů uvedených na toto období.

Mezinárodní spolupráce

Mnoho rozhodnutí podstatných pro vývoj kybernetické bezpečnosti v ČR je tvořeno nikoli pouze na vnitrostátní, ale také na mezinárodní úrovni. NÚKIB se proto snaží aktivně a efektivně zastupovat zájmy ČR v klíčových mezinárodních organizacích, zejména pak v EU, OSN, NATO, ale i OECD a OBSE, neboť výsledky činnosti v těchto organizacích na sebe postupně navazují. V roce 2019 se pak práce NÚKIB soustředila zejména na jednání s členskými státy i institucemi EU, a to především pokud jde o agendu kybernetického balíčku (např. ECCG – Evropská skupina pro kybernetickou certifikaci), 5G EU Toolboxu, závěrů Evropské rady i Rady EU (Cyber Diplomacy Toolbox, Blueprint), povinností vyplývajících ze směrnice NIS a nového legislativního návrhu o kompetenčním centru. V rámci OSN byla ustavena OEWG, na jejíž činnosti se NÚKIB také aktivně podílí.

Evropská unie

Aktivity NÚKIB se ve vztahu k EU soustředily na vyjednávání týkající se návrhu nařízení o Evropském průmyslovém, technologickém a výzkumném centru kybernetické bezpečnosti a síti národních koordinačních center (dále jen „nařízení o kompetenčních centrech“). Dále se NÚKIB zaměřil na rozpracování rámce pro právní, politické a strategické směřování společného úsilí při budování sítí 5G v Evropské Unii, které bylo realizováno prostřednictvím vlastní národní předběžné analýzy rizik spojených s budováním sítí 5G a společným dokumentem (5G EU Toolbox), který přináší další konkrétní rizika a návrhy opatření k tomu, jak je zmírnit.

V Radě EU je NÚKIB reprezentován vlastním zástupcem v Horizontální pracovní skupině pro kybernetické otázky, která se zabývá bezpečnostně politickými aspekty spolupráce v kybernetické bezpečnosti v rámci EU. Hlavním tématem první poloviny roku 2019 byl návrh nařízení o kompetenčních centrech, který navrhuje realizaci podpory výzkumu a průmyslu v oblasti kybernetické bezpečnosti, a má být založen na čerpání financí také z projektů Program Digitální Evropa a Horizont Evropa. Toto nařízení nebylo prozatím do konce r. 2019 vydáno, předpokládá se, že jednání budou probíhat také v průběhu r. 2020. Stalo se tak zejména z toho důvodu, že doposud nebyly vyjasněny otázky v oblasti financování center, stejně jako pravomocí, kdy ty, jež byly centru přisuzovány, se minimálně částečně duplikovaly s činností Agentury ENISA.

V červnu r. 2019 vešlo nicméně v účinnost nařízení o Agentuře ENISA a bezpečnostní certifikaci ICT produktů, služeb a procesů. K naplnění úkolů dle tohoto nařízení (tvorba EU certifikačních „schémat“) byla vytvořena Evropská skupina pro kybernetickou certifikaci, jejíž je NÚKIB součástí, a kde se společně s ostatními státy podílí na přípravě EU-schémat pro certifikaci.

Dalším důležitým tématem, které rok 2019 provázelo, byla bezpečnost při budování sítí 5G v Evropské unii. V květnu r. 2019 vydala Evropská Komise doporučení, ve kterém členské státy i Agenturu ENISA vyzvala k plnění různé řady úkolů a cílů. Mezi ně patřily nejprve národní analýzy rizik soustředící se na 5G sítě, na jejichž základě měla být vydána ze strany Agentury ENISA koordinovaná analýza rizik všech členských států EU. K tomu skutečně došlo, přičemž členským státům bylo ze strany Komise také navrženo, aby v rámci pracovní skupiny pod Skupinou pro spolupráci ke směrnici NIS

vytvořily do konce r. 2019 tzv. 5G EU Toolbox, tedy sadu konkrétních opatření k tomu, jak by měla být bezpečnost sítí 5G v členských státech nastavena, regulována a realizována.

NÚKIB, spolu s Francií a dalšími členskými státy, zastával při přípravě tohoto 5G EU Toolboxu vedoucí úlohu, což znamenalo i skutečnost, že se do výsledného dokumentu podařilo z velké části promítnout český přístup. Z nejdůležitějších aspektů lze zmínit požadavek na to, aby v případě analýzy rizik byly hodnoceny nejen technické hrozby, ale i ty netechnické, např. právní a politické prostředí země, ze které výrobce pochází. Neformální verze dokumentu byla vytvořena do konce r. 2019.

Ke konci prvního pololetí byly také vydány závěry Rady EU k tzv. Blueprint, což je procesní dokument o zvládání přeshraničních kybernetických incidentů a krizí. Tyto závěry vyzývaly členské státy k tomu, aby se zaměřily na procvičování svých vnitrostátních krizových opatření a tyto napojily na ty v EU. Ve spolupráci se sítí CSIRT byla vytvořena taxonomie pro hodnocení kybernetických bezpečnostních incidentů, jejíž používání má zjednodušit a zefektivnit komunikaci mezi dotčenými subjekty.

Koncem r. 2019 se NÚKIB účastnil jednání k aplikaci kybernetického diplomatického souboru opatření (tzv. „cyber diplomacy toolbox“), kde byla diskutována jeho aplikace. Lze konstatovat, že tento nástroj, na jehož dalším vývoji státy pracovaly v průběhu minulého roku, nachází své užití a důležitost.

V rámci ENISA se ČR i v roce 2019 účastnila výročního a dalších mimořádných jednání správní rady ENISA. Dva zástupci NÚKIB zde působí jako řádný člen a alternát hájící zájmy ČR, sdílející pohled ČR na vybraná témata kybernetické bezpečnosti a již tradičně se podílejí na schvalování programu, plánu prací a rozpočtu ENISA. V ČR slouží i tzv. National Liaison Officer (pracovník NÚKIB), který v každé členské zemi EU vykonává funkci referenčního bodu v specifických otázkách kybernetické bezpečnosti, zprostředkovatele spolupráce a podporovatele aktivit ENISA. ENISA hraje dlouhodobě klíčovou roli v kybernetické bezpečnosti na úrovni EU.

Severoatlantická aliance

ČR pokračovala v plnění svých závazků v rámci NATO. Na Varšavském summitu v roce 2016 se v tzv. Cyber Defence Pledge spolu s ostatními spojenci zavázala posilovat bezpečnost svých národních sítí a neustále navyšovat odolnost proti kybernetickým útokům. Pro NATO proto byla počátkem roku 2019 připravena v úzké spolupráci NÚKIB, VZ a MO již třetí zpráva o stavu kybernetických schopností ČR se zvláštní kapitolou zaměřenou na oblast vzdělávání. Závěrečnou konferencí v Portugalsku byl úspěšně dokončen NATO Smart Defence projekt Multinational Cyber Defence Education and Training na němž se podílela i ČR, jehož cílem je vyplnit mezery ve vzdělávání a školení v oblasti kybernetické bezpečnosti a obrany vytvořením nového mezinárodního magisterského programu se zaměřením na právo v kybernetickém prostoru.

Organizace pro bezpečnost a spolupráci v Evropě

V roce 2019 pokračovala práce neformální pracovní skupiny OBSE zřízené rozhodnutím Stálé rady č. 1039. Pracovní skupina se již několikerý rok zabývá implementací dříve přijatých opatření pro budování důvěry v oblasti kybernetické bezpečnosti (dále „CBM“). Jedná se o soubor šestnácti opatření, jejichž cílem je podpořit spolupráci a transparentnost států v kyberprostoru, a to konkrétně

za účelem de-eskalace napětí v případě mezinárodního konfliktu pramenícího ze státních aktivit v kyberprostoru.

Pod vedením maďarského předsednictví skupiny byla v roce 2018 spuštěna inciativa „adopt a CBM“, v rámci které státy na dobrovolné bázi přebírají část zodpovědnosti za rozpracování konkrétních opatření. Česká republika se v rámci této iniciativy podílí na operacionalizaci CBM 16, zabývající se problematikou koordinovaného zveřejnění zranitelností. Na operacionalizaci CBM 16 se spolupodílí také Rumunsko, Maďarsko a Nizozemí. Mezi další osvojená opatření patří nově CBM 4 (Kanada a Kazachstán), již tradičně pak CBM 5 (Velká Británie), CBM 9 (Srbsko), CBM 13 (USA) a CBM 15 (Francie, Rumunsko, Slovensko). CBM 4 vyzývá státy, aby zajišťovaly otevřený, interoperabilní, bezpečný a spolehlivý provoz internetu, CBM 5 se věnuje otázce budování kybernetických kapacit třetích států, CBM 9 je zaměřené na vytvoření sjednocené terminologie pro oblast kybernetické bezpečnosti, CBM 13 si klade za cíl vytvoření jednotných komunikačních vzorů pro použití při komunikaci zabezpečeným kanálem OBSE a CBM 15 je zaměřené na kooperativní opatření v ochraně KII.

V roce 2019 proběhly další dvě komunikační cvičení pro styčné pracovníky ustavené v rámci CBM 8 (v ČR je pozice zajišťována NÚKIB). Cvičení se při každém opakování vyznačují rostoucí komplexitou (např. kombinací cvičení CBM 8 s jinými CBMs, zejména pak CBM 13), přesto ČR v obou případech dodala požadované informace včas a v rámci svého regionu v nadprůměrně krátké době.

V souvislosti s vysokou aktivitou v pracovní skupině se v roce 2019 NÚKIB personálně podílel na školení pořádaném sekretariátem OBSE pro státy balkánského regionu v Sarajevu a následně ve Skopje. Cílem školení bylo uvést obecenstvo z relevantních institucí státní správy do problematiky kybernetických CBM přijatých v rámci OBSE tak, aby se zvýšilo povědomí účastníků o možnosti využití těchto instrumentů k de-eskalaci možných konfliktů. Účast zástupce NÚKIB umožnila prezentovat úspěchy, které ČR doznala v budování právního rámce kybernetické bezpečnosti a navázat kontakty v pro ČR strategicky významném balkánském regionu. V roce 2019 byla ČR rovněž přizvána do užší skupiny států Friends of Chair, která slouží jako poradní skupina pro stálé předsednictví pracovní skupiny.

Prague 5G Security Conference a zveřejnění Prague Proposals

NÚKIB v roce 2019 zorganizoval první ročník mezinárodní expertní konference k bezpečnosti 5G sítí. Prague 5G Security Conference se uskutečnila ve dnech 2. a 3. května 2019 pod záštitou předsedy vlády ČR Andreje Babiše a za účasti ministra zahraničních věcí ČR Tomáše Petříčka. Dvoudenní uzavřené mezinárodní konference se zúčastnilo přes 150 vládních představitelů a expertů na problematiku 5G sítí a kybernetickou bezpečnost z více než 32 států, včetně představitelů EU a NATO.

V průběhu expertní uzavřené části konference se diskutovaly čtyři hlavní oblasti: politika, ekonomika, bezpečnost spojená s odolností a technologie. Na konferenci vystoupila řada zahraničních expertů, například Julian King, eurokomisař pro bezpečnost; Joshua Steinman, zvláštní poradce amerického prezidenta pro otázky kybernetické bezpečnosti; Greg Miller, první náměstek pro kybernetickou bezpečnostní politiku ministerstva vnitra Austrálie; Masato Ohtaka, velvyslanec pro kybernetickou politiku ministerstva zahraničních věcí Japonska; Ciaran Martin, ředitel britského centra kybernetické bezpečnosti; Kim Gunn, korejský velvyslanec pro mezinárodní bezpečnostní záležitosti ministerstva zahraničních věcí a další. Součástí konference byl i expertní panel zaměřený na operátory, kterého se účastnili zástupci pozvaných operátorů, včetně Deutsche Telekom, AT&T, Vodafone a O2.

Hlavním výstupem expertní konference bylo zveřejnění tzv. Pražských návrhů, série doporučení týkajících se bezpečnosti 5G sítí. Přípravu tohoto dokumentu koordinoval NÚKIB a reflektoval v něm české zkušenosti v oblasti kybernetické bezpečnosti. Členy užší přípravné skupiny byly dále USA, Austrálie, Izrael, Nizozemí, Německo, Japonsko, Francie, Velká Británie a další. Pražské návrhy mimo jiné zdůrazňují důležitost netechnických aspektů bezpečnosti komunikační infrastruktury a zásadní roli důvěry uživatelů (včetně státu) ve výrobce používaného hardwaru a softwaru.
Prague 5G Security Conference i samotné Pražské návrhy zaznamenaly značný mezinárodní ohlas. Obsah Pražských návrhů se stal vodítkem pro řadu bilaterálních dohod v oblasti kybernetické bezpečnosti, které byly během roku 2019 uzavřeny. Netechnické aspekty a otázka důvěry v dodavatele byly rovněž zařazeny mezi klíčové charakteristiky bezpečnosti 5G sítí a promítnuty do EU 5G Toolbox. Pražské návrhy jsou tak významným příspěvkem ČR ve formulaci principů bezpečnosti 5G na globální úrovni, na který naváže druhý ročník Prague 5G Security Conference, který se uskuteční ve dnech 5. a 6. května 2020.

Další mezinárodní organizace a platformy

V roce 2019 pokračovala práce i Středoevropské platformy kybernetické bezpečnosti (Central European Cyber Security Platform, která vznikla v roce 2013 ze společné iniciativy České republiky a Rakouska jako formát regionální spolupráce zemí Visegrádu a Rakouska. V roce 2019 skupině

předsedalo Rakousko. Byl zvolen formát jediného setkání na pracovní úrovni, kde došlo zejména k harmonizaci některých aspektů k návrhům projednávaným na poli EU a ke sdílení národních stanovisek k nejpalčivějším problémům v této oblasti.

Na půdě OSN v roce 2019 zahájily práci na kybernetických otázkách dvě skupiny. Již pošesté byla ustavena skupina vládních expertů zabývající se normami, pravidly a principy zodpovědného chování států v kyberprostoru na základě rezoluce předložené USA s přispěním států EU, která sestává pouze z 25 členů vybraných dle spravedlivého geografického rozložení a jejímž členem ČR není, přestože bedlivě sleduje její vývoj. Na základě druhé rezoluce předložené společně Ruskou federací a Čínskou lidovou republikou byla ustavena OEWG s neomezeným okruhem členů, které se mimo jiné účastní všechny státy EU. ČR se v roce 2019 aktivně podílela na činnosti OEWG, jejíž první substantivní zasedání se konalo v září 2019, a která plánuje vydat závěrečnou zprávu v červenci 2020. Přestože se konsensu pravděpodobně nepodaří dosáhnout, je OEWG významnou globální platformou k diskusi nad mezinárodním právem a dalšími normami aplikovatelnými na aktivitu států v kyberprostoru.

V rámci OECD v březnu 2019 vyvrcholil projekt Going Digital I. a následně započala jeho druhá fáze, Going Digital II. V červenci bylo na jednání výboru pro ekonomiku při OECD rozhodnuto o rozdělení stávající pracovní skupiny pro bezpečnost a soukromí v digitální ekonomice na dvě samostatné části: Pracovní skupinu pro správu dat a soukromí v digitální ekonomice (Data Management and Privacy in the Digital Economy, dále jen „DMPDE“) a Pracovní skupinu pro bezpečnost v digitální ekonomice (Security in the Digital Economy, dále jen „SDE“). V prosinci pak bylo publikováno revidované Doporučení o ochraně KII z roku 2008, které nyní nově zavádí pojem „ochrana kritických aktivit“ jako způsob zajištění nerušeného chodu státu i mimo úzce vymezenou oblast KII. Pojetí OECD odpovídá přístupu ČR, respektive EU ke kybernetické bezpečnosti, který je již promítnut v právních předpisech a strategických dokumentech přijatých v uplynulých pěti letech.

Poté co se ČR v roce 2018 oficiálně připojila k platformě Global Forum on Cyber Expertise (dále jen „GFCE“) byl v roce 2019 za podpory nizozemského ministerstva zahraničních věci na výročním jednání GFCE v Etiopii publikován tištěný průvodce organizací kybernetických cvičení. GFCE slouží k propojení nabídky a poptávky po budování kapacit kybernetické bezpečnosti mezi členskými státy. ČR se k platformě připojila jako její 71. člen a publikovaný průvodce je teprve třetím hmatatelným produktem této platformy.

Cvičení kybernetické bezpečnosti

Cvičení kybernetické bezpečnosti představovala významnou součást aktivit NÚKIB i v roce 2019. Stejně jako v předešlých letech se cvičení orientovala na ověřování technických, strategických i komunikačních dovedností účastníků. Mezi nejvýznamnější cvičení pořádané NÚKIB se řadí první sektorové cvičení Electro Czech, zaměřené na energetický sektor. Dále se NÚKIB aktivně podílel na plánování a přípravě cvičení krizového řízení NATO CMX 2019, které obsahovalo i významný kyberbezpečnostní element. ČR se kromě organizace a koordinace cvičení kybernetické bezpečnosti zapojuje aktivně také coby jeden z cvičících států. Příkladem takové účasti je mezinárodní technické cvičení Locked Shields 2019 nebo cvičení Cyber Coalition 2019, které se zaměřuje na prověřování technické i netechnické stránky řešení kybernetických incidentů.

Národní sektorové cvičení Electro Czech

V roce 2019 realizoval NÚKIB poprvé v historii vlastní sektorové cvičení. Jedná se o formát, který je do budoucna perspektivní hned z několika důvodů. Masivní kybernetické útoky mohou zasáhnout celé sektory či se jejich dopady mohou projevit i mimo napadenou instituci a rozšířit do celého odvětví. Dále tento formát umožňuje zapojit větší množství účastníků, což rozšiřuje okruh možných cvičících subjektů. Toto vše činí sektorová cvičení relevantní a umožňuje procvičit nejen reakci jedné organizace, ale i jejich vzájemnou koordinaci, komunikaci a spolupráci.

Electro Czech se zaměřil na oblast výroby, přenos a distribuci elektřiny. Zúčastnilo se jej šest subjektů a více než 40 účastníků. Každá ze společností sestavila vlastní tým skládající se z pracovníků pokrývající oblast bezpečnosti, kybernetické bezpečnosti, provozu, pravá a mediální komunikace. Díky tomuto složení mohli řešit krizovou situaci z mnoha perspektiv, vyměnit si vzájemné zkušenosti a porozumět komplexní povaze krize. Aktivně se účastnil také management všech společností řešící otázky na nejvyšší, strategické úrovni.

Zvolený formát se projevil jako vhodný. Umožnil vzájemné interakce cvičících i celých týmů, což představovalo zásadní přidanou hodnotu oproti separátním cvičením pro jednotlivé organizace.

Technické cvičení Cyber Czech 2018

Cyber Czech 2018 #3 a #2

V březnu 2019 se uskutečnil již třetí běh národního technického cvičení Cyber Czech. Cvičení, probíhající v prostředí speciálně upravené infrastruktury kybernetického polygonu Ústavu výpočetní techniky Masarykovy Univerzity mělo, stejně jako v předešlých letech, za cíl ověřit praktické znalosti a dovednosti zvládání kybernetických incidentů v souvislosti s ochranou prvků KII včetně komunikace s médii při řešení nastalé krize.

Cyber Czech probíhal na pozadí scénáře založeného na obraně informační infrastruktury integrovaného záchranného systému fiktivní země Pilsnerie. Do role obránců, tzv. modrých týmů, byli nominováni zástupci Zdravotnické záchranné služby a policie z celé ČR. Hackery, útočící na výše zmíněné informační systémy, představoval tzv. červený tým složený již tradičně ze zaměstnanců Vládního CERT týmu a Masarykovy univerzity.

Nově byl tento běh cvičení rozšířen o tzv. policejní hru, která tvořila nadstavbu tzv. právní hry. Cílem tohoto rozšíření bylo účastníkům přiblížit proces od nahlášení trestného činu až po poskytnutí důkazů. Součástí cvičení byl i mediální aspekt krize, kdy byli účastníci dotazováni fiktivními novináři, kteří prostřednictvím herního zpravodajského portálu informovali o situaci. Nedílnou součástí cvičení bylo i krátké vyhodnocení ihned po skončení cvičení a dále pak i poskytnutí podrobné písemné zprávy pro všechny účastníky.

Druhé opakování cvičení Cyber Czech v roce 2019 a celkově pak desáté technické cvičení pořádané pro veřejnost proběhlo v květnu 2019. Cvičení tentokrát probíhalo v angličtině a účastnily se jej týmy z Česka, Slovenska, Izraele a tým stálé strukturované spolupráce PESCO (tým rychlé reakce – jedná se o projekt EU, kam se mohou členské státy dobrovolně hlásit[1]). Jako pozorovatelé byli přizváni

[1] Viz https://pesco.europa.eu/project/cyber-rapid-response-teams-and-mutual-assistance-in-cyber-security/

například zástupci z Lucemburska, Německa, Japonska či Singapuru. Volně na toto cvičení navazovalo i netechnické cvičení provedené ve spolupráci s NCOZ (viz níže).

Table-top cvičení

Oddělení cvičení organizuje rovněž netechnická table-top cvičení. Ty jsou připravována na míru pro národní i mezinárodní partnery. Cvičení taktéž mohou tvořit součást významné konference nebo symposia se zaměřením se na rozličné účely jako například sdílení získaného know-how, vzdělávání státních zaměstnanců atd.

Národní table-top cvičení

V roce 2019 zorganizoval NÚKIB následující netechnická table-top cvičení na národní úrovni:

1. **Cvičení pro orgány činné v trestním řízení**
   V dubnu proběhlo v Praze v budově NÚKIB table-top cvičení, které bylo speciálně připravené pro orgány činné v trestním řízení. Cvičícími pak byli konkrétně příslušníci NCOZ, státní zástupci a členové Vládního CERT. V roli pozorovatelů se zúčastnili ředitel NCOZ Jiří Mazánek, vrchní státní zástupkyně Lenka Bradáčová a ředitel NÚKIB Dušan Navrátil. Cílem cvičení bylo poskytnout platformu pro sdílení přístupů a nastínit možný společný postup při řešení kybernetických incidentů. Cvičení mělo též za úkol otestovat komunikaci a sdílení informací mezi jednotlivými týmy a upozornit na případná bílá místa. Důležitým prvkem bylo rovněž procvičení kompetencí a povinností subjektů zapojených do řešení kybernetických incidentů a trestního řízení. Cvičení se rovněž zúčastnili i zástupci CZ.NIC a společnosti Axians a to jako členové tzv. poradního tělesa, které se vyjadřovalo ke stanoviskům cvičících.
2. **Cvičení pro SSHR**
   Dne 3. září 2019 se v Praze uskutečnilo netechnické cvičení organizované ve spolupráci NÚKIB a SSHR. Cílem cvičení bylo zejména procvičit rozhodovací procesy s nedostatkem informací v časovém tlaku a otestovat externí i interní komunikaci během krize. Scénář byl koherentně zasazen do souvislého děje. Skládal se ze tří hlavních událostí, které jej postupně rozvíjely tak, jak cvičící procházeli jednotlivými injecty. Cvičící pracovali formou diskuse. Konkrétní rozhodnutí pak prezentovaly osoby, které by v reálné situaci za řešení dané situace zodpovídaly.
3. **Cvičení pro Kurz Generálního štábu Armády České republiky**
   Kurz je pravidelnou akcí určenou pro vyšší důstojníky, kteří mají předpoklady v AČR zastávat velitelské funkce. Již podruhé bylo jeho součástí i komplexní netechnické cvičení zaměřené zejména na vojenský sektor bezpečnosti. Mimo samotné cvičení přispívá NÚKIB do náplně kurzu i přednáškami věnujícími se jeho oblasti působnosti a pomáhá tak udržet náplň reflektující aktuální hrozby a bezpečnostní prostředí.
4. **Cvičení pro SÚKL**
   Pro SÚKL připravil NÚKIB cvičení na míru. Zaměřilo se zejména na systém elektronické preskripce, ale neopomenulo i další důležité systémy organizace. Důraz byl kladen především na zvládnutí rozhodovacích procesů a na mediální komunikaci. I proto se ze strany SÚKL účastnili zaměstnanci, kteří by podobnou krizovou situaci řešili i ve skutečnosti.

Dále je nutné zmínit cvičení například v rámci, konference ISACA, konference CyberCon Brno 2019 a cvičení pro vysokoškolské studenty v rámci magisterského programu Bezpečnostní a strategická studia na Masarykové univerzitě nebo table-top cvičení pro Summer School on IT Law.

Table-top cvičení pro zahraniční partnery

NÚKIB organizoval i v uplynulém roce cvičení pro zahraniční partnery, a to v rámci následujících akcí:

1. **Symposium Africa Endeavor 2019**
   Jedná o konferenci každoročně pořádanou americkým velitelstvím pro Africký kontinent (U.S. AFRICOM). Akce je zaměřená na komunikační problematiku, interoperabilitu a kybernetickou bezpečnost. Ročníku 2019 se zúčastnilo přes 100 zástupců z více než 30 afrických států. Ti při exekuci umožnili nahlédnout do zcela jiného prostředí, než jaké panuje v Evropě. Rovněž velmi pozitivně ocenili přínos a ochotu české strany sdílet své know-how.

2. **Program on Cyber Security Studies**
   Jedná se o prestižní kurz, který pořádá George C. Marshall European Center for Security Studies. NÚKIB byl jeho organizátory již potřetí osloven s žádostí o uspořádání cvičení, které by sloužilo jako modelový příklad pro účastníky kurzu. Těmi jsou především vysoce postavení pracovníci s rozhodovacími pravomocemi v oblasti kybernetické bezpečnosti. Cvičení proběhlo ve dnech 17. a 18. prosince a účastnilo se jej více než 80 účastníků z 50 zemí světa. Jejich úkolem bylo reagovat na krizové scénáře, přicházet s řešeními a diskutovat možné dopady. Nad rámec cvičení pracovník NÚKIB vystoupil s příspěvkem o důležitosti netechnických cvičení a zkušenostech České republiky s jejich přípravou.

Cvičení NATO

Locked Shields 2019

Ve dnech 9. – 12. dubna se uskutečnilo největší a nejkomplexnější mezinárodní cvičení kybernetické bezpečnosti Locked Shields 2019. Do tohoto cvičení je pravidelně zainteresováno až 30 zemí. V uplynulém roce se jednalo již o pátý ročník, kterého se Česká republika účastnila jako samostatný cvičící tým. I přes velmi silnou konkurenci se tým České republiky již tradičně udržel na předních příčkách a obsadil druhé místo.

Locked Shields představuje simulaci série útoků tzv. Červeného týmu na systémy a sítě tzv. Modrých týmů. Modré týmy jsou složeny z expertů, kteří v reálném světě chrání IT systémy každodenně. Český Modrý tým, stejně jako v předchozích letech, reprezentovali přední odborníci nejen z řad NÚKIB, ale například též ze sdružení CESNET a CZ.NIC, dále z MO, AČR, VZ, či IT společností Net Suite, Red Hat, Accenture, Avast nebo Axians. Akademický sektor byl zastoupen Masarykovou univerzitou.

Vedle cvičícího, Modrého, týmu mívá Česká republika pravidelně své zástupce také v Červeném (útočném) a Bílém (organizačním) týmu. Oba týmy se prakticky podílí na plánování a přípravách celého cvičení, což pro jejich účastníky znamená významnou zkušenost uplatnitelnou pro vývoj a přípravu národních cvičení.

Součástí cvičení byla vedle technické části též paralelně probíhající strategická hra. Jejím cílem bylo vnímat rozdílnost technického řešení incidentu vs. tvorby strategického rozhodnutí při jeho eskalaci a zajistit adekvátní reakci nejen z technického pohledu.

Cyber Coalition 2019

V roce 2019 se již podeváté čeští experti zúčastnili cvičení Cyber Coalition, které je na národní úrovni koordinováno MO za vojenskou část a NÚKIB za část civilní. Pětidenní cvičení pořádané NATO patří k největším a nejvýznamnějším cvičením tohoto druhu. Do letošního ročníku bylo zapojeno rekordních 1000 odborníků z 28 členských a partnerských zemí, včetně EU a zástupců akademického a soukromého sektoru. Hlavním cílem a potažmo přínosem celého cvičení je především procvičení spolupráce a koordinace při řešení kybernetických bezpečnostních incidentů napříč státy a jednotlivými sektory.

Cvičení umožňuje účastníkům otestovat nové postupy a vyzkoušet si práci s novými technologiemi při řešení kybernetických bezpečnostních incidentů. Je řízeno z estonského Tartu a mimo jiné využívá virtualizované prostředí Cyber Range. Prostředí Cyber Range simuluje síťovou infrastrukturu a přidává tak cvičení na autenticitě.

Na národní úrovni cvičení proběhlo na pracovištích v Brně, konkrétně v prostorách NÚKIB a Centra CIRC Agentury komunikačních a informačních systémů AČR. Ačkoli není cvičení koncipováno jako soutěž, čeští odborníci pravidelně patří mezi nejlepší. Experti z Vládního CERT, CSIRT MU, PČR, CIRC MO (včetně příslušníku Aktivní zálohy CIRC), VeKySIO, NCKO, BIS a Avastu excelovali při forenzní analýze a řešení incidentu na SCADA systémech.

Ve cvičení byl reflektován i právní aspekt řešení incidentů, který prostupoval celým cvičením. Technické týmy tak konzultovaly své kroky s právníky, kteří kromě těchto konzultací v rámci cvičení vypracovávali i samostatné právní analýzy. Zapojení právní hry potvrzuje důležitost integrace právního aspektu do řešení kybernetických bezpečnostních incidentů.

CMX 2019

Pravidelné cvičení krizového řízení NATO proběhlo v termínu od 9. do 15. května. Jedná se o komplexní cvičení, v němž kybernetická bezpečnost představuje pouze jednu z vícero dimenzí, což umožňuje procvičit širokou paletu krizových procesů a zasadit kybernetické incidenty do komplexní krizové situace. Krizový scénář na úrovni aliance pokrýval mimo jiné i problematiku článků 4 a 5 Washingtonské smlouvy. NÚKIB se aktivně zapojil jak na straně plánování tohoto cvičení, tak také na straně cvičících.

Kontrola důležitých subjektů a metodická podpora v roce 2019

Za rok 2019 provedl NÚKIB **15 kontrol** podle zákona o kybernetické bezpečnosti, respektive vyhlášky 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 platném znění (dále jen „vyhláška o kybernetické bezpečnosti“). Kontrola u povinných orgánů a osob dle zákona o kybernetické bezpečnosti ověřuje plnění povinností plynoucích ze zákona o kybernetické bezpečnosti a vyhlášky o kybernetické bezpečnosti. V rámci každé kontroly je ověřeno rámcově 150 kontrolních bodů.

Za rok 2019 proběhla také **metodická podpora**, která je prováděna na základě usnesení vlády a dopadá na všechna ministerstva a ÚVČR. Dobrovolně se k metodické podpoře každý rok navíc hlásí kancelář Poslanecké sněmovny a Senátu Parlamentu České republiky a také Kancelář prezidenta republiky. Metodická podpora je založena na individuální analýze kybernetické bezpečnosti každého ze subjektu a na ní založených konzultací o vhodných řešeních identifikovaných kyberbezpečnostních nedostatků. Rozsahem pokrývá systémy spravované dotčenými subjekty, do kterých mohou pracovníci přistupovat z vnější sítě (internetu).

Vedení Komunity manažerů kybernetické bezpečnosti

Jedná se o komunitu manažerů kybernetické bezpečnosti (dále „MKB“) všech ministerstev, ÚV ČR, Poslanecké sněmovny, Hradu a Senátu, což jsou odborníci zodpovědní za kybernetickou bezpečnost u zmíněných subjektů. Primárním cílem této komunity je výměna informací, vzájemné sdílení zkušeností např. při implementaci bezpečnostní opatření a podpora od NÚKIB. Program je sestaven a témata jsou vybírána dle návrhů členů komunity MKB. Jedná se např. o problematiku analýzy rizik, témata spojená s novinkami v legislativě apod. Subjekty jsou také pravidelně informovány o aktuálních hrozbách v kyberprostoru. Akce jsou svolávány pravidelně jednou za kvartál.

Bezpečnost informačních a komunikačních systémů a kryptografická ochrana

NÚKIB 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 NÚKIB 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.

NÚKIB 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 2019 probíhalo řízení o certifikaci 192 informačních systémů. K 54 žádostem o certifikaci informačního systému, jejichž zpracování bylo zahájeno v přechozím roce (2018), přibylo v roce 2019 dalších 138 žádostí, a to 62 ze státní správy nebo samosprávy a 76 ze soukromé sféry. Ve většině případů se jednalo o žádosti o opakovanou certifikaci již provozovaných informačních systémů. Ve 26 případech byla podána žádost o certifikaci nově budovaného informačního systému, přičemž pouze 7 z těchto žádostí pochází ze státní správy.

V uvedeném roce bylo vydáno celkem 140 certifikátů informačních systémů, z toho 57 pro žadatele ze státní správy nebo samosprávy a 83 ze soukromé sféry.

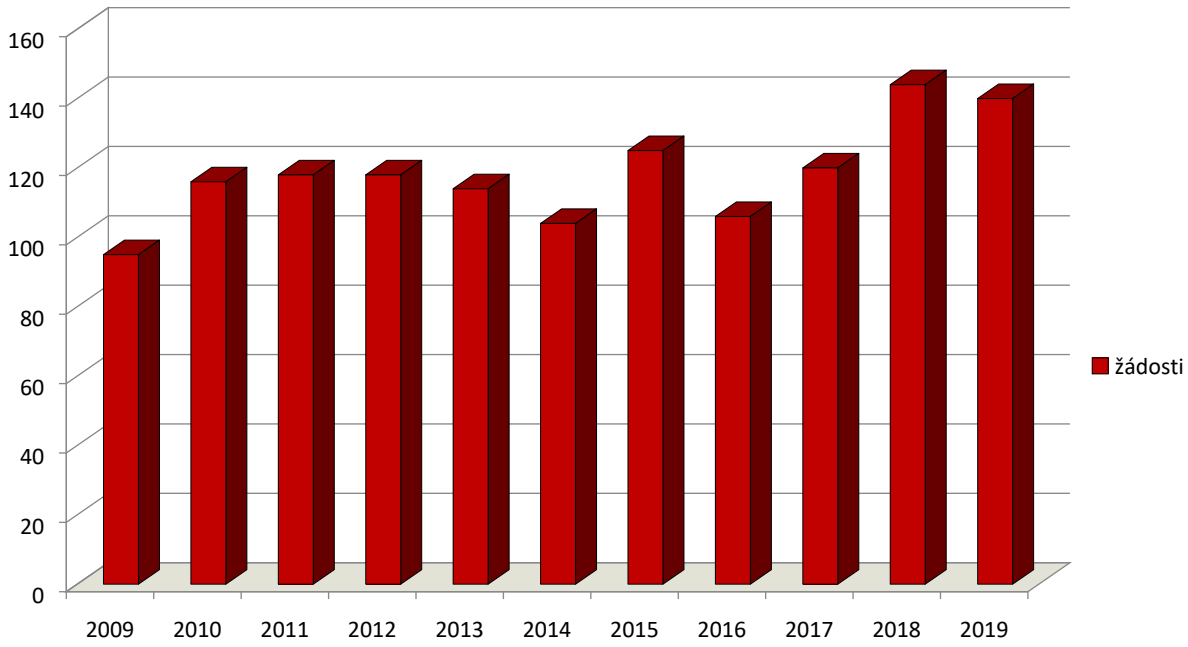
Celkem 84 certifikátů informačních systémů bylo vydáno na žádost podanou v roce 2019.

V 9 případech provozovatel informačního systému s certifikátem platným do data spadajícího do roku 201 nepožádal o opakovanou certifikaci a platnost certifikátu automaticky skončila.

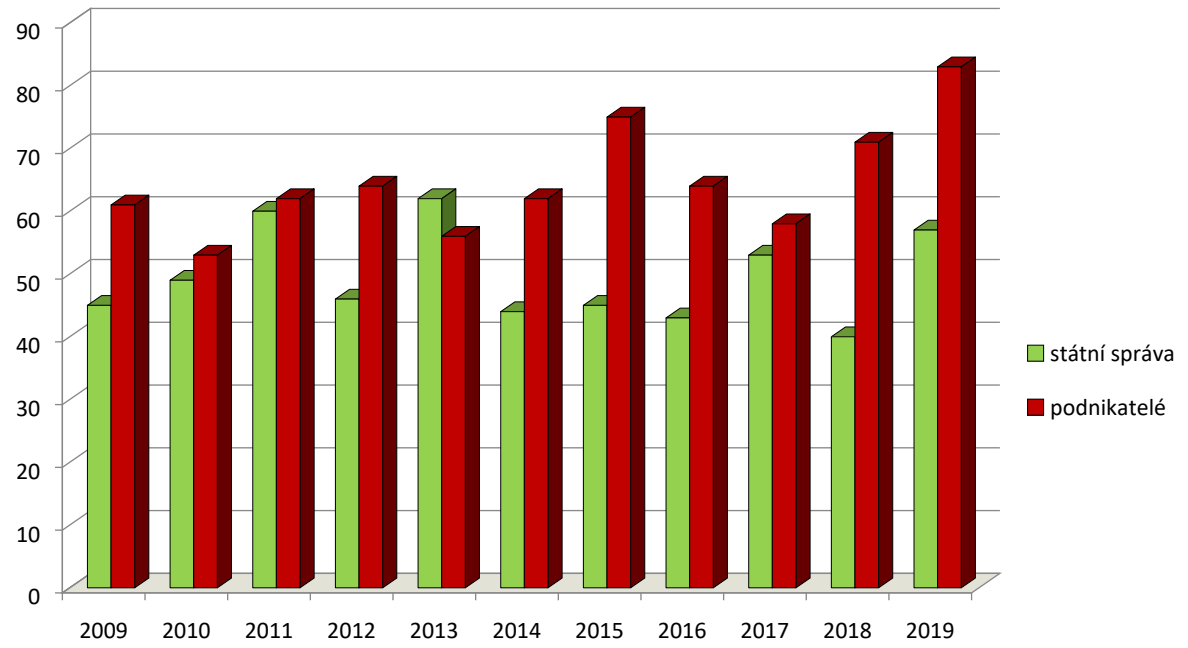
Certifikace informačních systémů v roce 2018

Řešené žádosti v roce 2019	Vydané certifikáty podle stupně utajení				Vydané certifikáty	
	Vyhrazené	Důvěrné	Tajné	Přísně tajné	státní správa	Podnikatelé
192	26,4 %	47,1 %	24,3 %	2,1 %	57	83

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 NÚKIB.

Lze konstatovat, že v roce 2019 přibylo 7 žádostí o certifikaci nově budovaného informačního systému ze státní správy a 19 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 se 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 2019, kromě certifikace menších informačních systémů podnikatelů, několika ministerstev a úřadů (MPSV, MPO, MZ, MD, MMR, ÚV ČR, ÚS, GIBS, ČOI, Vězeňská služba, několik krajských a městských úřadů) proběhla opakovaná nebo nová certifikace řady rozsáhlých informačních systémů rezortu MV a PČR, rezortu MO včetně VZ, MZV a BIS.

V rámci certifikace informačních systémů poskytovali zaměstnanci NÚKIB 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 2019 NÚKIB provedl pro rezorty MO, MV, MZV a BIS 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 2019 byla na území ČR zahájena akreditace 1 součinnostního systému. Dokončení se předpokládá v roce 2020.

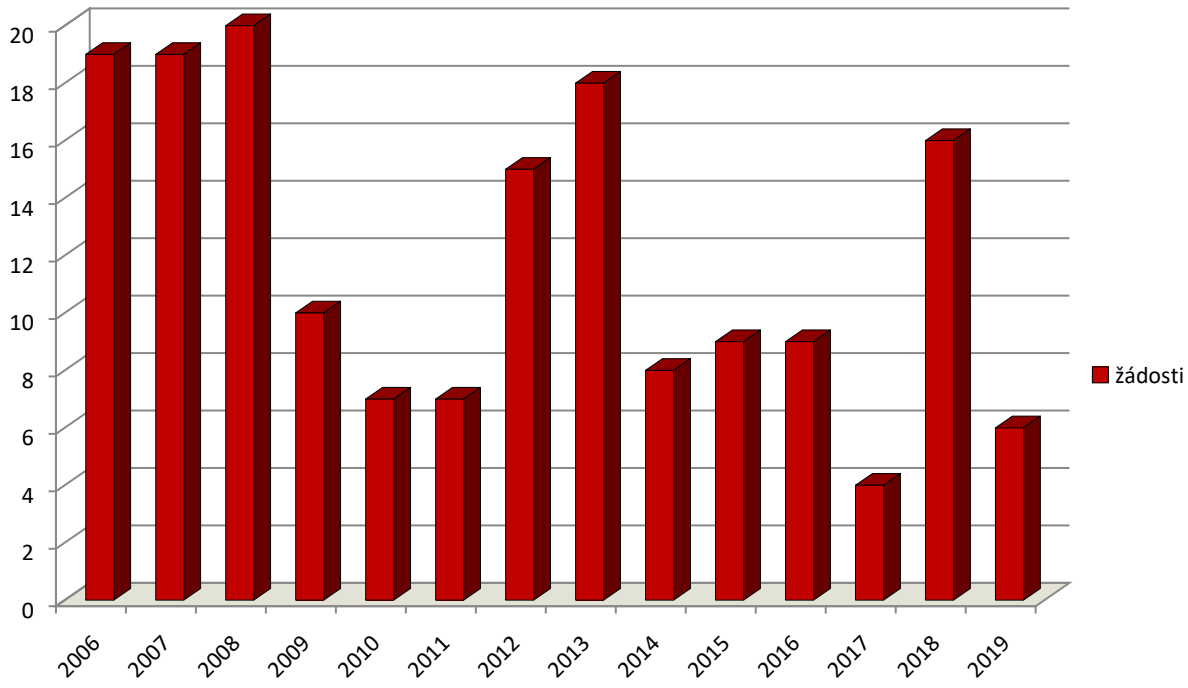
Certifikace kryptografických prostředků

V roce 2019 bylo NÚKIB podáno celkem 6 žádostí o certifikaci kryptografického prostředku, z toho 2 na nový kryptografický prostředek. V řízeních k certifikaci kryptografického prostředku bylo vydáno 13 certifikátů, žádné řízení nebylo ukončeno bez vydání certifikátu. Stav řízení je shrnut v následující tabulce.

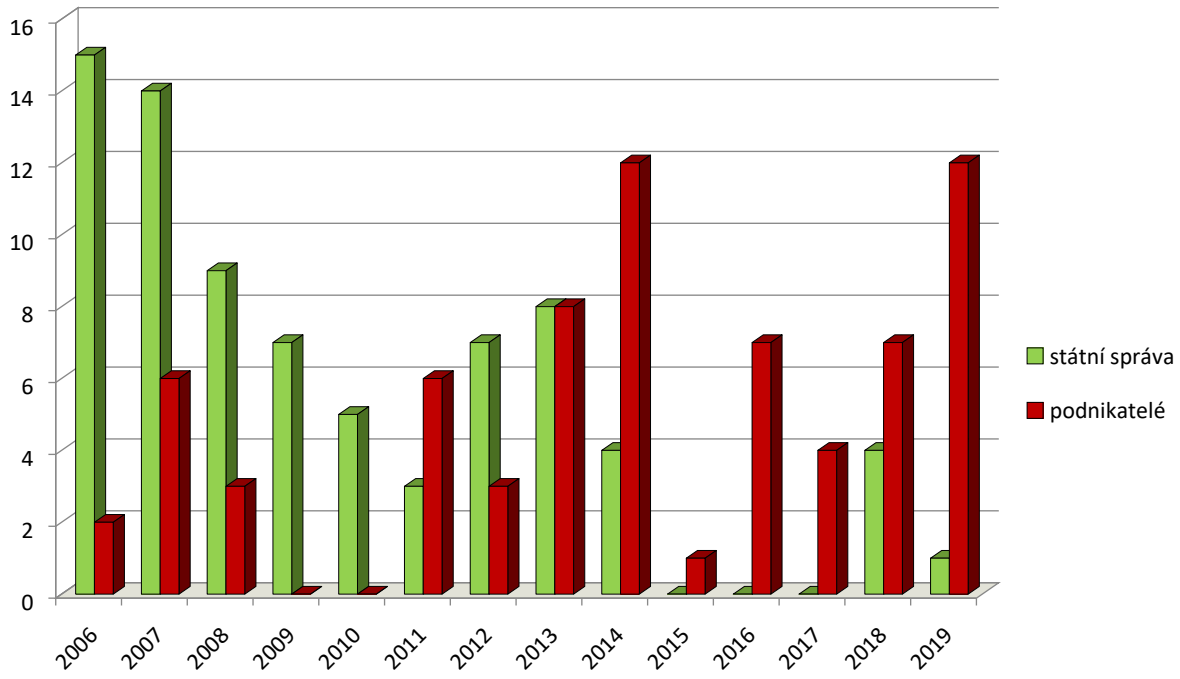
Certifikace kryptografických prostředků v roce 2019

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
6	0	5	0	0	1	12	13	9

Přijaté žádosti o certifikaci kryptografického prostředku v letech 2006 až 2019



Vydané certifikáty kryptografických prostředků v letech 2006 až 2019



Nově byly certifikovány kryptografické prostředky SINA Workstation H, SINA Workstation S a SINA Workstation S, 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 LANPCS, PCS1, SECTRA a THALES.

Nadále pokračovaly přípravné práce na vytvoření expozice historie kryptografických prostředků používaných v ČR v prostorách NÚKIB.

Certifikované kryptografické prostředky jsou nebo budou využívány především v rezortech MO, MV, MZV 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 NÚKIB, které vycházejí z národních zkušeností, mezinárodních standardů (CC a FIPS) i informací získaných na mezinárodních kryptografických konferencích.

Do seznamu „kontrolovaná kryptografická položka“ vedeného NÚKIB bylo nově zařazeno 8 kryptografických prostředků.

Schvalování projektů bezpečnosti komunikačních systémů

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

V roce 2019 nebyla podána žádná žádost o schválení projektu bezpečnosti nového komunikačního systému.

Nadále byl provozován komunikační systém v BIS, komunikační systém MODUS a komunikační systém RETIS.

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 2019 nadále zajišťoval NÚKIB.

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 NÚKIB.

Hlasovou komunikaci utajovaných informací na mezirezortní úrovni poskytují rovněž 2 informační systémy, tzv. vládního utajeného spojení, provozované MV, 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 NÚKIB podle zákona o ochraně utajovaných informací a jejich rozvoj a rozšiřování je pod jeho dohledem.

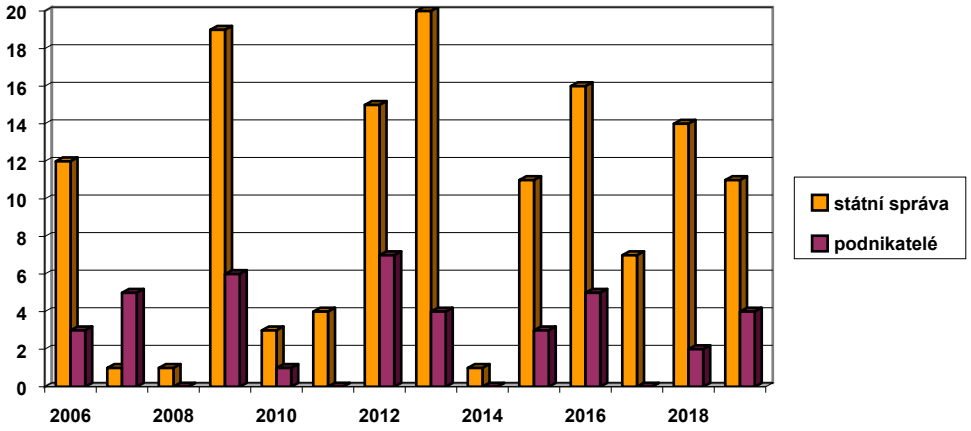
Certifikace kryptografických pracovišť

V roce 2019 bylo podáno celkem 15 žádostí o certifikaci kryptografického pracoviště. Většina žádostí o certifikaci spadá do kategorie opakovaných žádostí. Dvě žádosti jsou 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 NÚKIB. Stav řízení je shrnut v následující tabulce:

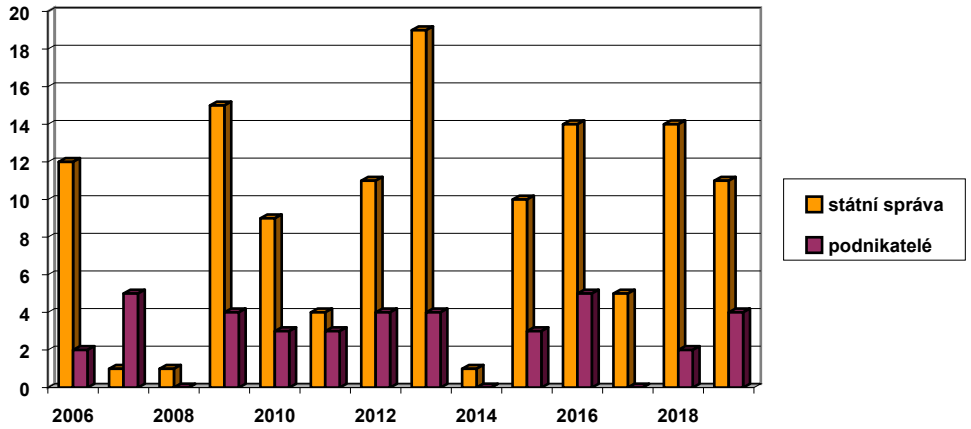
Certifikace kryptografických pracovišť v roce 2019

	Přijaté žádosti	Rozpracováno	Certifikováno	Zamítnuto	Zastaveno
Státní správa	11	2	11	0	0
Podnikatelé	4	0	4	0	0
Celkem	**15**	**2**	**15**	**0**	**0**

Přijaté žádosti o certifikaci kryptografického pracoviště v letech 2006 až 2019



Vydané certifikáty kryptografických pracovišť v letech 2006 až 2019



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 NÚKIB a orgány státu k zajištění ochrany utajovaných informací v komunikačních a informačních systémech.

V této oblasti NÚKIB spolupracoval s odborem bezpečnosti MO, který zabezpečuje generování, speciální balení a distribuci kryptografických klíčových materiálů pro kryptografické prostředky provozované v rámci rezortu MO.

V roce 2019 bylo na NÚKIB vygenerováno celkem 73 602 kryptografických klíčů a hesel uložených na 5 444 nosičích různých typů a dalších 160 ks jiného kryptografického materiálu (procesory, paměti, kryptografická dokumentace, instalační a šifrovací SW).

NÚKIB vzal do evidence a provedl distribuci celkem 2740 ks nového kryptografického a CCI materiálu a dále zajistil servis a opravy na území ČR u 252 ks kryptografických prostředků a mimo ČR u 10 ks kryptografických prostředků.

NÚKIB zajistil školení a vydal 11 autorizací pro přístup ke COMSEC materiálu EU a vzal do evidence a provedl distribuci celkem 20 ks kryptografického materiálu EU.

Na kryptografickém pracovišti NÚKIB probíhalo průběžné ničení utajovaných dokumentů vyřazených v rámci skartačního řízení.

Dále NÚKIB 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 jeho působnosti.

Měření kompromitujícího vyzařování (TEMPEST)

TEMPEST měření elektronických zařízení

NÚKIB prováděl v roce 2019 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 2019 provedeno více než 54 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. ÚV ČR, MZV, MO, MV, MPO, zpravodajské služby, krajské úřady aj.), nebo pro podnikatele. Z celkového počtu hodnocených zařízení byla většina vyžádána MO.

Zónové měření, instalační záznamy, obranné prohlídky

NÚKIB 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 NÚKIB, BIS, MO a MV. 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 MO a VZ.

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 38 lokalit.

V roce 2019 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 2019, je uveden v následující tabulce.

Měřená zařízení a objekty v roce 2019

Typ měření[9)]	**Počet**
Zónové měření	7 objektů
Kryptografické prostředky	2 typy
Komponenty ICT	více než 50 měření
Audiotechnika	2 typy zařízení
Obranné prohlídky i v rámci certifikace IS	17 objektů
Mobilní systémy	15 systémy
Instalační záznamy	38 lokalit

Školení pracovníků kryptografické ochrany a zkoušky odborné způsobilosti

NÚKIB v roce 2019 organizačně zajistil a provedl, v souladu se zákonem, celkem 12 školení skupin pracovníků kryptografické ochrany a po následující zkoušce odborné způsobilosti vydal 111

[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 MO nebo NÚKIB. U instalačních záznamů se jedná o systémy, které mohou mít několik instalací v rámci ČR i mimo ČR.

osvědčení o zvláštní odborné způsobilosti pracovníka kryptografické ochrany. Dále provedl zaškolení pracovníků provozní obsluhy kryptografického prostředku a vydal 7 potvrzení o odborném zaškolení pracovníka provozní obsluhy kryptografického prostředku. Kromě toho probíhají další školení a zkoušky odborné způsobilosti na MV, MO a MZV na základě smluv uzavřených mezi NÚKIB a uvedenými ministerstvy.

Kontroly ochrany utajovaných informací (státní dozor)

V roce 2019 provedl NÚKIB ve smyslu §143 odst. 6 zákona o ochraně utajovaných informací 16 kontrol za oblast bezpečnosti informačních nebo komunikačních systémů, případně kryptografické ochrany. Z tohoto počtu bylo 7 kontrol provedeno v rámci státní správy a 9 kontrol u podnikatelů.

Problémové oblasti bezpečnosti informačních a komunikačních systémů a kryptografické ochrany

Zákonem stanovené činnosti NÚKIB v oblasti bezpečnosti informačních systémů nakládajících s utajovanými informacemi a kryptografické ochrany byly v roce 2019 zajištěny.

- Stálou výzvou je rychlý rozvoj 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 NÚKIB 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 NÚKIB 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 NÚKIB 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 NÚKIB (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 NÚKIB, 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 NÚKIB 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 NÚKIB pro řešení vývojových a výzkumných projektů osvědčený model – kromě vlastních pracovišť zapojuje externí odborná pracoviště případně jednotlivé externí odborníky.

Projekty realizované v roce 2019

Koncepce výzkumu a vývoje se vytvářela na základě poznatků zjištěných NÚKIB při spolupráci s orgány státu, pilotním testování kryptografických prostředků, 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. Hlavním důvodem této skutečnosti je již výše zmíněný rychlý technologický pokrok, vzhledem k němuž je nutné neustálé reagovat na změny komunikační i technologické situace a inovovat již vyvinuté produkty, případně vyvíjet nové prostředky.

V rámci OKVKP bylo dokončen projekt rozvoje analytického nástroje CipherCAD pro rok 2019, probíhal vývoj střediska pro kryptografické prostředky PCA, byly zahájeny projekty dalšího rozvoje hlasových komunikátorů (iSacom, Sacom, OSK), osobních kryptografických prostředků a výzkum i vývoj GNZ. Uvedené projekty byly realizovány ve spolupráci s externími řešiteli, návazně probíhal interní aplikační vývoj na odborném pracovišti NÚKIB v předmětných oblastech.

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 NÚKIB spolupracuje.

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

V roce 2019 NÚKIB zajišťoval vývoj na základě schváleného Výzkumného záměru VaV, zpracoval výzkumnou zprávu a 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.

Přehled ZPC za rok 2019

- **CIS3 C&I Partnership – SCIP + NINE Working Group Meeting,**
  Setkání v rámci pracovních skupin SCIP a NINE. Účelem je především standardizace SCIP a NINE, vzájemné předávání informací o aktuálním stavu implementace protokolů SCIP a NINE i o jejich vývoji a dále příprava podkladů a návrhu pro následná jednání řídících výborů pro SCIP a NINE, které o dalším vývoji protokolů spolurozhodují.

- **CIS3 C&I Partnership – Work Package Board Meeting**
  Jednání řídících výborů v rámci CIS3 C&I Partnership pro pracovní skupiny SCIP a NINE. Účelem bylo zpracování výstupů z jednání pracovních skupin a příprava podkladů pro řídící výbor Partnerství.

- **CIS3 C&I Partnership – Partnership Committee Meeting**
  Jednání řídícího výboru CIS3 C&I Partnership, v rámci, kterých jsou rozhodovány otázky týkající se dalšího směrování Partnerství, vývoje jednotlivých protokolů a standardů. Řídící výbor je zastřešujícím orgánem a rozhoduje o aktivitách v rámci celého Partnerství.

- **RWC 2019 – Real World Crypto**
  RWC je významnou odbornou akcí zaměřenou na reálné problémy aplikované kryptologie. Cílem cesty bylo získání poznatků o současných tématech a výsledcích v této oblasti.
  (1/2019, USA)

- **MWC 2019 – Mobile World Conference**
  MWC je významnou odbornou akcí zaměřenou na řešení aktuálních problémů bezpečnosti mobilních komunikací. Cílem cesty bylo získání poznatků o současných tématech a trendech v této oblasti.
  (2/2019, Španělsko)

- **PQ NIST 2019 – Post Quantum Conference NIST**
  PQC NIST je významnou odbornou akcí zaměřenou na standardizaci post-kvantových kryptografických algoritmů. Cílem cesty bylo získání poznatků o současných tématech v této oblasti a zejména výsledcích standardizačního procesu.
  (8/2019, USA)

- **CHES 2019 – Cryptographic HW and Embedded Systems Conference**
  CHES je významnou odbornou akcí zaměřenou na kryptografický HW a procesory. Cílem cesty bylo získání poznatků o současných tématech a trendech v této oblasti.
  (9/2019, USA)

- **Cryptel IP Forum 2019 – Conference Thales**
  Cryptel IP Forum je významnou odbornou akcí a setkání uživatelů Thales Cryptel IP KP, zaměřené na kryptografické prostředky Thales. Cílem cesty bylo získání poznatků o současných tématech a trendech v této oblasti a zejména výměna zkušeností uživatelů.
  (9/2019, Norsko)

- **Trustech 2019 – konference a výstava**
  Trustech je významnou odbornou akcí, zaměřenou na bezpečnost mobilních technologií, čipové karty, kryptografické procesory a řadu technologií aplikované kryptografie. Cílem cesty bylo získání poznatků o současných tématech a trendech v této oblasti.
  (11/2019, Francie)

- **ICMC 2019 – International Cryptographic Module Conference**
  ICMC je významnou odbornou akcí zaměřenou na řešení aktuálních problémů vývoje, testování a provozování kryptografických modulů s důrazem na aplikaci standardů FIPS 140-2, ISO/IEC 19790 a Common Criteria. Cílem cesty bylo získání poznatků o současných tématech v oblasti hodnocení kryptografických modulů a o novinkách ve standardech týkajících se kryptografických modulů.
  (7. – 12. 5. 2019, Washington, USA)

- **Summer School on Real-world Crypto and Privacy 2019**
  Jedná se o významnou akci pořádanou prestižní nizozemskou univerzitou Radboud, na níž tradičně vystupují celosvětově uznávaní odborníci z oboru kryptologie. Probíhá formou klasických přednášek spojených do tematických bloků, což umožňuje hlubší vhled do dané problematiky. Cílem cesty bylo prohlubování odborných znalostí a získání přehledu o aktuálních trendech v oblasti kryptologie.

(10. – 16. 6. 2018, Šibenik, Chorvatsko)

- **Security and Policing 2019**
  Jedná se o tradiční výstavu, zaměřenou na speciální techniku, jak defenzivní, tak ofenzivní, nové technologie přenosu signálů a jejich zabezpečení. Na výstavě byly představeny nejnovější prostředky pro akustický i elektromagnetický monitoring prostorů, technologie bezpečných přenosů dat, měřicí technika pro obranné prohlídky, nová telekomunikační technika – GSM detektory, zabezpečení objektů aj.
  (Farnborough, Velká Británie)

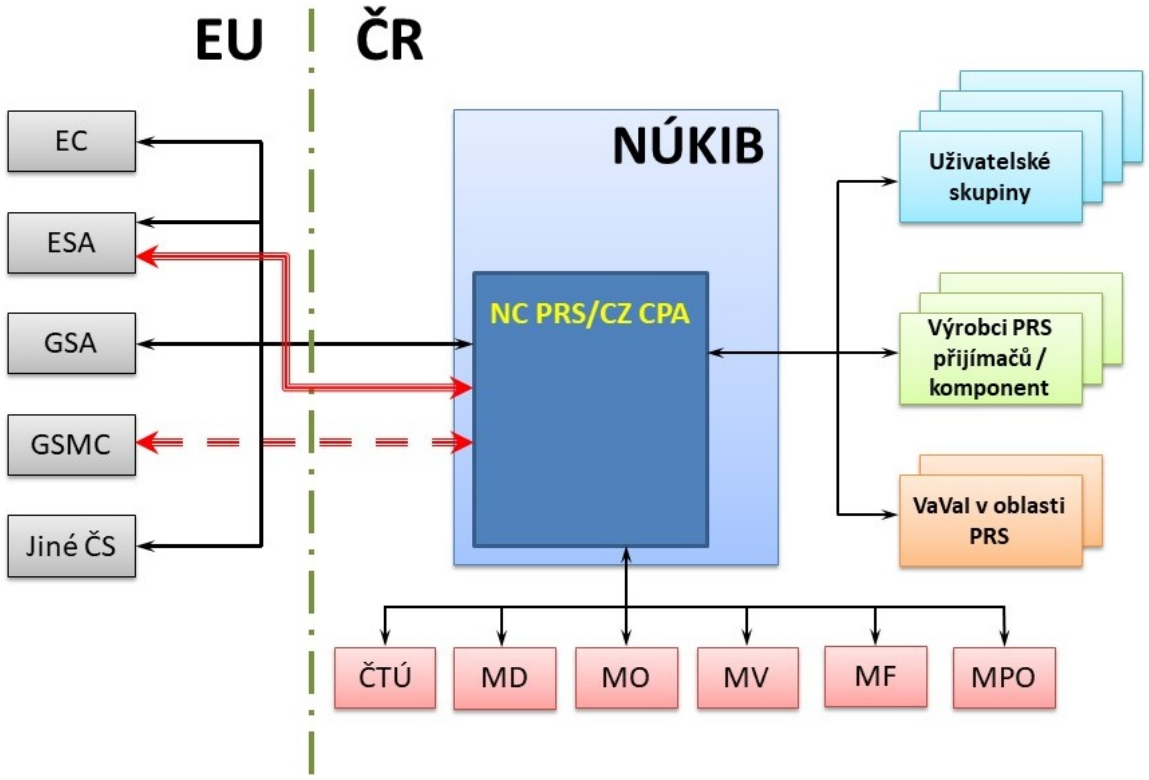
Výkon funkce příslušného orgánu PRS

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 služby PRS z kompetence rezortu MD na NÚKIB. Ředitel NÚKIB 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 NÚKIB 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 obrázku:

Organizační schéma zabezpečení služby PRS v ČR



Součástí povinností, kterými je NCPRS pověřeno, je mimo jiné též reprezentace NÚKIB, resp. ČR v pracovních skupinách programu Galileo (EU) řešících problematiku bezpečnosti programu Galileo a PRS. Tato aktivita přirozeně pokračovala i v roce 2019. 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.

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. Zástupci NCPRS se též zúčastnili kampaně testování GNSS přijímačů za přítomnosti rušení GNSS signálů. Tato kampaň byla organizována ve spolupráci s MO a přinesla cenné zkušenosti a poznatky, které budou využity při realizaci testování služby PRS. NCPRS pokračovalo v procesu nákupu speciálních technologií potřebných pro úspěšné provedení projektu. Samotná realizace projektu bude uskutečněna v závislosti na dostupnosti speciálních přijímačů PRS pravděpodobně v letech 2020-2021.

V rámci pravidelného setkání CPA evropských zemí zorganizovalo NCRPS v Brně mezinárodní dvoudenní setkání, jehož hlavním účelem byla diskuze nad současným stavem implementace PRS v členských státech EU, koordinace společného postupu při jednání s Evropskou komisí a výměna zkušeností.

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 s řešením problematiky implementace PRS do právního rámce ČR vedl k požadavku na rozšíření pracovního týmu NCPRS. Na tomto základě bylo již v roce 2018 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. V roce 2019 se pak podařilo obsadit další novou pozici tak, aby byly pokryty nejurgentnější požadavky.

Spolupráce s ostatními subjekty při implementaci služby PRS

Při řešení problematiky služby PRS NCPRS úzce spolupracuje zejména s MD coby národním koordinátorem pro správu a řízení evropských systémů družicové navigace. V roce 2019 byla též prohloubena spolupráce s MO, a to jak z důvodu zapojení do projektu společného testování PRS, tak z důvodu potenciálního využití služby PRS ze strany AČR.

Seznam zkratek

AČR – Armáda České republiky

BIS – Bezpečnostní Informační Služba

CERT – Computer Emergency Response Team (Skupina pro reakci na počítačový stav nouze)

CESNET - Czech Education and Scientific NETwork

CSIRT – Computer Security Incident Response Team (Skupina pro reakci na počítačové bezpečnostní události)

ČOI – Česká obchodní inspekce

ENISA - European Network and Security Agency (Evropská agentura pro bezpečnost sítí a komunikací)

EU – Evropská Unie

GIBS – Generální inspekce bezpečnostních sborů

ICT – Information and Communication Technologies (Informační a komunikační technologie)

KII – Kritická Informační Infrastruktura

MD – Ministerstvo dopravy

MF – Ministerstvo financí

MMR – Ministerstvo pro místní rozvoj

MO – Ministerstvo obrany

MPO – Ministerstvo průmyslu a obchodu

MPSV – Ministerstvo práce a sociálních věcí

MV – Ministerstvo vnitra

MZ – Ministerstvo zemědělství

MZV – Ministerstvo zahraničních věcí

NATO – North Atlantic Treaty Organization (Severoatlantická aliance)

NCKB – Národní Centrum Kybernetické Bezpečnosti

NCKO – Národní Centrum Kybernetických Operací

NCOZ – Národní Centrála proti Organizovanému Zločinu

OBSE – Organizace pro Bezpečnost a Spolupráci v Evropě

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

OEWG – Open-ended Working Group (Otevřená pracovní skupina)

OSN – Organizace Spojených Národů

PČR – Policie České republiky

PESCO – Permanent Structured Cooperation (Stálá strukturovaná spolupráce)

PRS – Public Regulated Service (Veřejně regulovaná služba)

PZS – Provozovatel Základní Služby

SCADA - Supervisory Control And Data Acquisition (Dispečerské řízení a sběr dat)

SSHR – Státní správa hmotných rezerv

SÚKL – Státní úřad pro kontrolu léčiv

ÚS – Ústavní soud

ÚVČR – Úřad vlády České republiky

VeKySIO – Velitelství Kybernetických Sil a Informačních Operací

VIS – Významný Informační Systém

VZ – Vojenské zpravodajství