NÚKIB

ZPRÁVA O ČINNOSTI 2020

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST

Praha 2021

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).

1 Sekce provozně právní

Právní agenda

Odbor právní zajišťuje celou řadu právních agend a administraci zadávacích řízení v režimu zákona o zadávání veřejných zakázek či postupů pod tento zákon nespadajících. Jedná se zejména o oblast smluvního zajištění veškerých projektů v rámci NÚKIB, pracovněprávní agendy, řešení problematiky ochrany osobních údajů (GDPR) ve spolupráci s pověřencem pro ochranu osobních údajů, přípravu memorand i jiných mimosmluvních dokumentů, zastoupení v projektových týmech úřadu i zpracovávání interních předpisů úřadu a podpůrnou a metodickou činnost pro ostatní organizační celky. Tento odbor dále vyřizuje žádosti o informace podle zákona č. 106/1999 Sb. a další podání občanů, vč. uplatnění nároku na náhradu škody dle zák. č. 82/1998 Sb. V neposlední řadě je součástí agendy zastupování Úřadu v řízeních před soudem a jinými orgány státu v občanskoprávním, správním nebo trestním řízením.

Významnou působností Úřadu je projednávání přestupků stanovených zákonem 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“) a podle části osmé zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů (dále jen „zákon o ochraně utajovaných informací“). V působnosti Úřadu dle zákona o ochraně utajovaných informací se jedná o přestupky proti bezpečnosti utajovaných informací v informačních a komunikačních systémech a proti bezpečnosti utajovaných informací při kryptografické ochraně.

Do působnosti Úřadu přitom spadá nejen projednávání přestupků podle § 25 a násl. zákona o kybernetické bezpečnosti a části osmé zákona o ochraně utajovaných informací, a ukládání správních trestů za jejich spáchání, ale zároveň i vybírání pokut, jež Úřad v rozhodnutí o spáchání přestupku pachateli uloží. Tuto kompletní agendu zajišťuje odbor právní.

V roce 2020 zahájil Úřad jedno přestupkové řízení pro podezření ze spáchání přestupku stanoveného zákonem o kybernetické bezpečnosti. Toto řízení nebylo do konce roku 2020 pravomocně skončeno.

V roce 2020 zahájil Úřad 2 přestupková řízení pro podezření ze spáchání přestupku stanoveného zákonem o ochraně utajovaných informací. Tato řízení nebyla do konce roku 2020 pravomocně skončena. Úřad dále prošetřoval 4 nové podněty, 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. Ve 2 případech Úřad neshledal důvody pro zahájení řízení o přestupku, v jednom případě Úřad věc předal orgánu příslušnému k projednání daného skutku a v jednom případě nebylo prošetřování důvodnosti tohoto podnětů do konce roku 2020 ukončeno.

Ekonomické zabezpečení Úřadu

Úřad je od 01.08.2017 samostatnou kapitolou státního rozpočtu pod číslem 378. Rozpočet Úřadu je tvořen příjmy a výdaji.

V celkových příjmech kapitoly za rok 2020 ve výši 196 312,85 Kč jsou zejména zahrnuty ostatní nedaňové příjmy, v tom hlavní část byla za příjem z licenčních práv výzkumu a vývoje v částce 120 000 Kč.

Schválený rozpočet celkových výdajů Úřadu byl v roce 2020 ve výši 425 317 706 Kč. Během roku 2020 byl upravován rozpočtovými opatřeními Ministerstva financí ČR (dále jen „MF“) na objem 475 348 191 Kč. K 31. prosinci 2020 bylo z upraveného rozpočtu celkových výdajů vyčerpáno 329 439 286,75 Kč, tedy v relativním vyjádření 69,3 %.

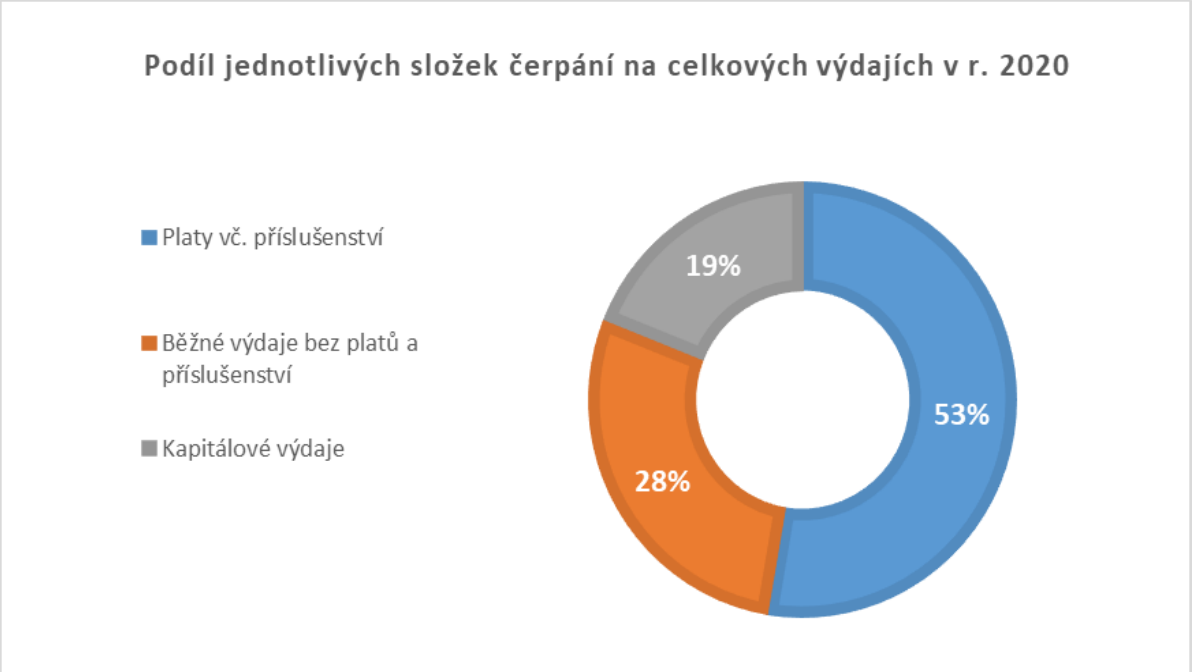
Konečný rozpočet celkových výdajů kapitoly za rok 2020, tedy rozpočet včetně zapojených nároků z nespotřebovaných výdajů ve výši 96 951 942,17 Kč, byl v objemu 572 300 133,17 Kč.

Čerpání konečného rozpočtu bylo v relativním vyjádření na 64,5 %, v absolutním vyjádření ve výši 369 388 000,49 Kč.

Nízké čerpání rozpočtu bylo zapříčiněno řadou faktorů. V důsledku pandemie covid-19 došlo ke snížení nákladů na zahraniční pracovní cesty a výdajů na pohonné hmoty. Řada konferencí a jiných akcí byla zcela zrušena, či přesunuta do on-line prostředí, což rovněž přispělo ke snížení nákladů.

Dalším významným faktorem byla změna ve vedení úřadu, neboť do nástupu nového ředitele byly Vládou ČR pozastaveny některé investiční akce, což se promítlo v nižším čerpání kapitálových výdajů v roce 2020, viz níže. V současné době však jsou tyto investiční akce opět v běhu.

Podíl jednotlivých složek čerpání na celkových výdajích v r. 2020



Výdaje na platy a příslušenství

Výdaje na platy, ostatní platby za provedenou práci a příslušenství byly rozpočtovány ve výši 189 491 873 Kč pro 221 pracovních míst.

Na žádost Úřadu byly rozpočtovými opatřeními v kompetenci MF ČR upraveny na 194 568 174 Kč. Zapojením nároků z nespotřebovaných výdajů byly upraveny na konečný rozpočet ve výši 195 697 996,24 Kč pro 241 pracovních míst (v ročním průměru to bylo pro 227 pracovních míst). Konečný rozpočet výdajů na platy, ostatní platby za provedenou práci a příslušenství byl čerpán ve výši 194 609 161,48 Kč, tedy v relativním vyjádření na 99,4 %.

Běžné výdaje

Běžné výdaje (bez výdajů na platy, ostatní platby za provedenou práci a příslušenství) byly rozpočtovány ve výši 138 074 368 Kč.

Rozpočtovými opatřeními byly upraveny na 143 028 552 Kč. Zapojením nároků z nespotřebovaných výdajů byly upraveny na konečný rozpočet ve výši 202 128 177,64 Kč. Konečný rozpočet běžných výdajů byl čerpán v objemu 104 742 178,24 Kč, v relativním vyjádření na 51,8 %.

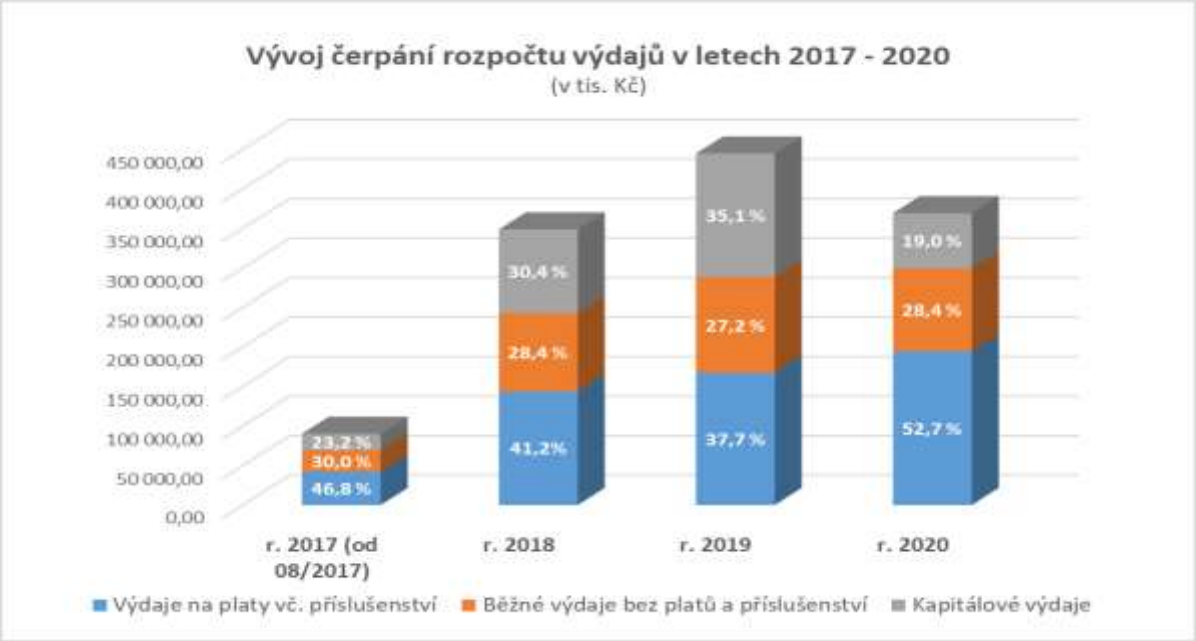
Kapitálové výdaje

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 informačním systému SMVS byly rozpočtovány ve výši 97 751 465 Kč. Rozpočtovými opatřeními byly upraveny na 137 751 465 Kč. Zapojením nároků z nespotřebovaných výdajů byly upraveny na konečný rozpočet výdajů vedených v SMVS v objemu 174 473 959,29 Kč. Konečný rozpočet kapitálových výdajů pak byl čerpán v objemu 70 036 660,77 Kč, v relativním vyjádření na 40,1 %.

Nejvýznamnější objem finančních prostředků byl vynaložen na výstavbu, posílení a obnovu ICT infrastruktury Úřadu, a to téměř 57 mil. Kč. Kapitálové výdaje v oblasti výzkumu a vývoje dosáhly objemu cca 11,5 mil. Kč.

Vývoj čerpání rozpočtu výdajů v letech 2017-2020



Evidence nároků z nespotřebovaných výdajů (dále „NNV“)

Celkové nároky z nespotřebovaných výdajů byly k 1. lednu 2020 ve výši 103 686 979,95 Kč.

Objem NNV ve výši 6 735 037,78 Kč byl ukončen, neboť se jednalo o nečerpaný rozpočet z úspěšně realizovaného EU projektu „PERIMETR“.

Celkem za rok 2020 bylo vyčerpáno z nároků z nespotřebovaných výdajů 39 948 713,74 Kč. Zůstatek nároků z nespotřebovaných výdajů k 31. prosinci 2020 byl ve výši 57 003 228,43 Kč. Převážnou část z celkového zůstatku nároků z nespotřebovaných výdajů roku 2020 tvoří neprofilující výdaje, a to v objemu 34,7 mil. Kč. Nečerpané neprofilující výdaje budou zčásti navrženy k převedení do rozpočtu kapitálových výdajů v rámci kapitoly 378-NÚKIB na základě materiálu, který byl v prvním pololetí letošního roku předložen do Vlády ČR. Profilující výdaje v objemu 22,3 mil. Kč jsou plánovány k dočerpání během roku 2021 na daný účel.

Vnitřní finanční kontroly a interní audit

Řídící a kontrolní mechanismy jsou pro jednotlivé oblasti činnosti Úřadu 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 Úřadu tvoří základ jeho vnitřního kontrolního systému.

V průběhu roku 2020 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 Úřadu v rámci jeho rozpočtové skladby.

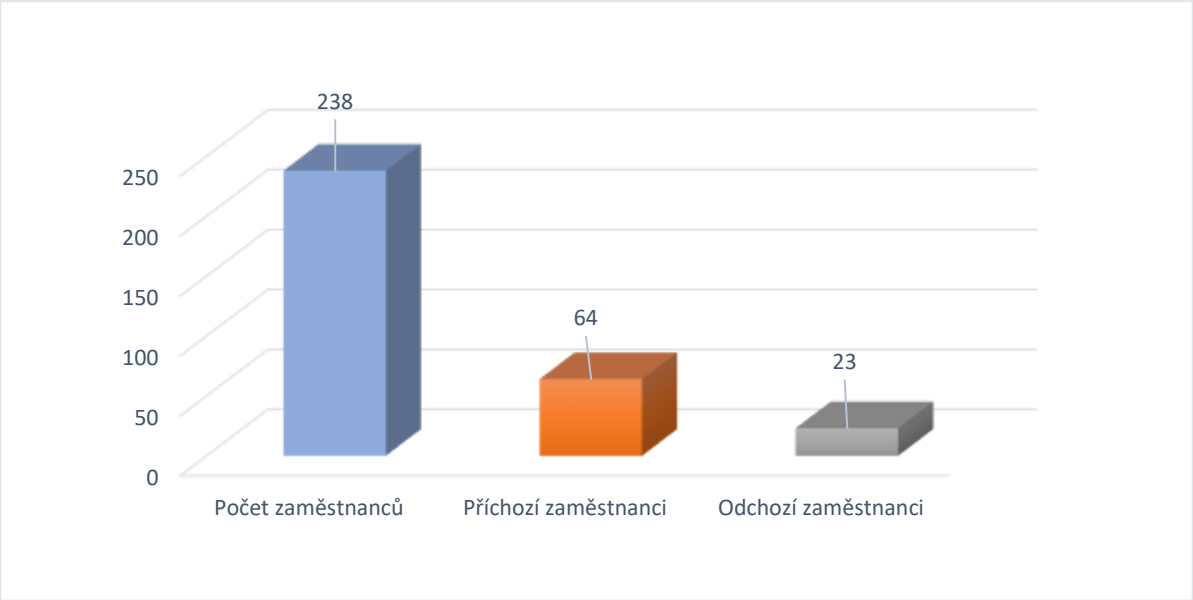
Při uskutečněných řídících kontrolách nebyly zjištěny skutečnosti, které by nasvědčovaly neoprávněnému nakládání s finančními prostředky, ani podezření na podvodné či korupční jednání. Finanční operace byly realizovány účelně, hospodárně a v souladu s naplňováním cílů a posláním Úřadu.

Personální zabezpečení Úřadu

Po navýšení počtu pracovních míst byla v roce 2020 tato pracovní místa postupně obsazována novými zaměstnanci. Do pracovního poměru v období od 01. 01. 2020 do 31. 12. 2020 bylo přijato 64 nových zaměstnanců. Další 4 zaměstnanci vykonávali činnost na základě uzavřených dohod o pracovní činnosti a se 14 osobami byla uzavřena dohoda o provedení práce.

Do konce roku 2020 ukončilo 23 zaměstnanců pracovní poměr, tj. 10,58 % z počtu zaměstnanců evidovaných na systemizovaných pracovních místech. Z tohoto počtu 2 zaměstnanci ukončili pracovní poměr ve zkušební době, 3 zaměstnanci ukončili pracovní poměr uplynutím doby určité, 11 zaměstnanců výpovědí ze strany zaměstnance, 5 pracovních poměrů bylo ukončeno dohodou na žádost zaměstnance, 1 zaměstnanec odešel do starobního důchodu a 1 zaměstnanec zemřel. Nejčastější důvod ukončení pracovního poměru byla výpověď ze strany zaměstnance.

Nástupy a odchody zaměstnanců v roce 2020



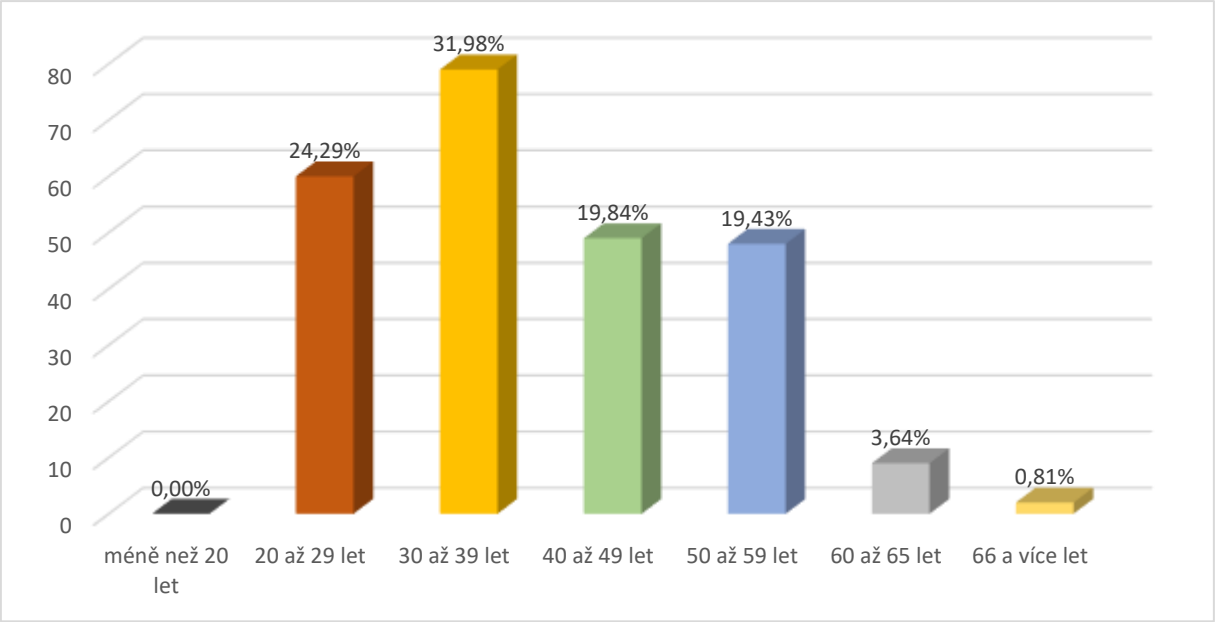
Struktura zaměstnanců podle věku

V následující tabulce uvádíme celkovou věkovou strukturu zaměstnanců (včetně zaměstnanců dočasně mimo systemizovaná pracovní místa).

Věková struktura zaměstnanců k 31.12.2020

Věková kategorie	**Počet zaměstnanců k 31. 12. 2020**	**Podíl zaměstnanců v %**	**Z toho**	
			muži	**ženy**
méně než 20 let	0	0,0 %	0	0
20 až 29 let	60	24,3 %	37	23
30 až 39 let	79	32,0 %	54	25
40 až 49 let	49	19,9 %	30	19
50 až 59 let	48	19,4 %	32	16
60 až 65	9	3,6 %	6	3
66 a více let	2	0,8 %	2	0
Celkem	**247**	**100,0 %**	**161**	**86**

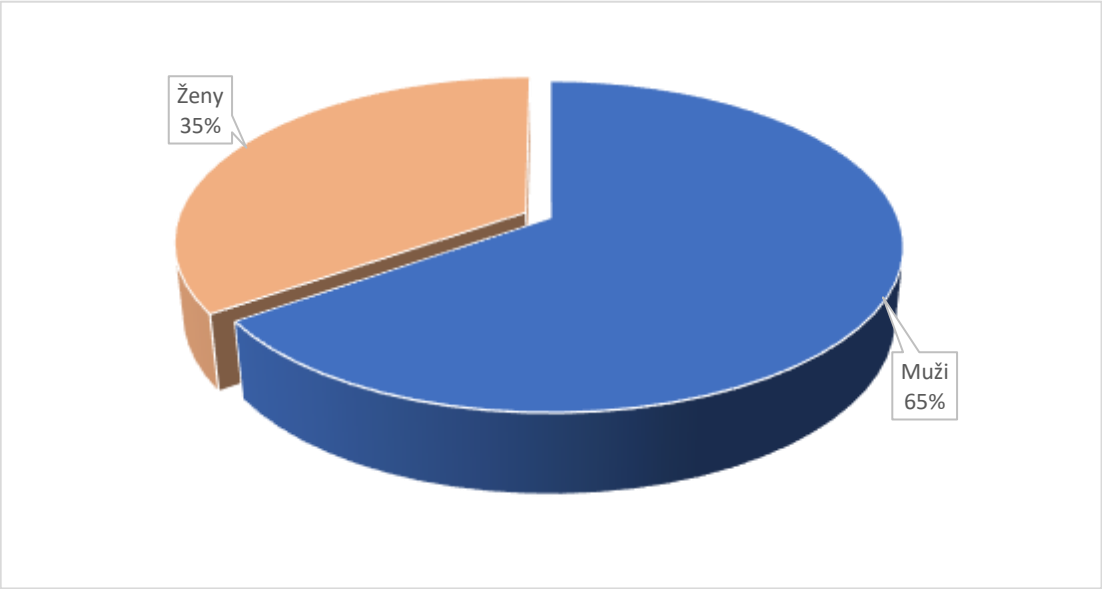
Struktura zaměstnanců Úřadu podle věku (%)



Struktura zaměstnanců Úřadu – ženy/muži

K 31. 12. 2020 evidoval NÚKIB celkem 247 zaměstnanců (238 na systemizovaných pracovních místech a 9 dočasně mimo systemizovaná pracovní místa), z toho bylo 65,2 % mužů a 34,8 % žen. Průměrný věk zaměstnance úřadu je 39,1 roku.

Struktura zaměstnanců Úřadu – ženy/muži

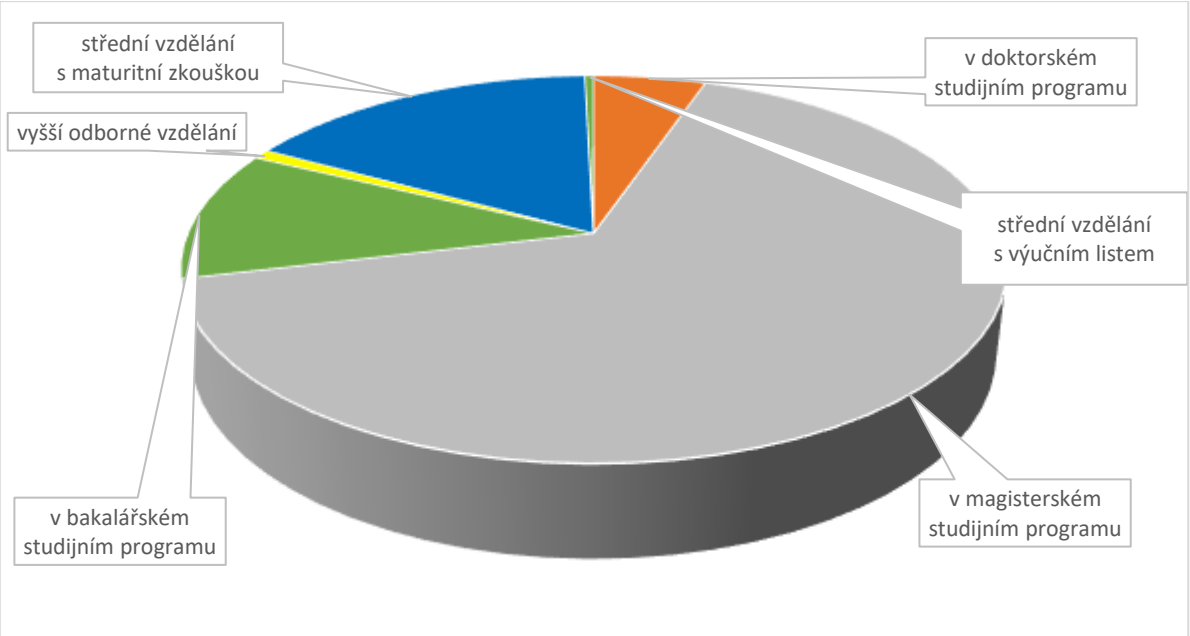


Kvalifikační struktura zaměstnanců

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

Kvalifikační struktura zaměstnanců

Dosažené vzdělání k 31. 12. 2020 (zahrnuti jsou též zaměstnanci dočasně na MD, RD a čerpající neplacené volno)	**Počet zaměstnanců k 31. 12. 2020**	**Procentní struktura**
v doktorském studijním programu	13	5,3%
v magisterském studijním programu	163	66%
v bakalářském studijním programu	27	10,9%
vyšší odborné vzdělání	2	0,8%
střední vzdělání s maturitní zkouškou	41	16,6%
střední vzdělání s výučním listem nebo střední vzdělání	1	0,4%
základní vzdělání	0	0%
Celkem	**247**	**100%**



Vzdělávání a rozvoj zaměstnanců

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

Vzdělávání je zabezpečováno formou individuálních a hromadných vzdělávacích akcí. Za rok 2020 byla Úřadem realizována školení převážně v oblasti kybernetické bezpečnosti, informačních technologií a projektového řízení. Dále byla věnována pozornost dalšímu odbornému vzdělávání zaměstnanců v oblasti ekonomické a právní. Byly realizovány hromadné vzdělávací akce v oblasti projektového řízení, práv a povinností vedoucích zaměstnanců vyplývajících ze zákoníku práce a manažerských dovedností pro vedoucí zaměstnance. Z důvodu pandemie covid-19 byla převážná část školení absolvována v ČR a online formou.

Zaměstnávání osob se zdravotním postižením

Úřad je v souladu podle § 83 zákona č. 435/2004 Sb., o zaměstnanosti, v platném znění, povinen plnit stanovený podíl osob se zdravotním postižením. Jeho naplňování je dáno jednak

zaměstnáváním osob se zdravotním postižením a dále odběrem výrobků a služeb od zaměstnavatelů, kteří zaměstnávají více než 50 % osob se zdravotním postižením.

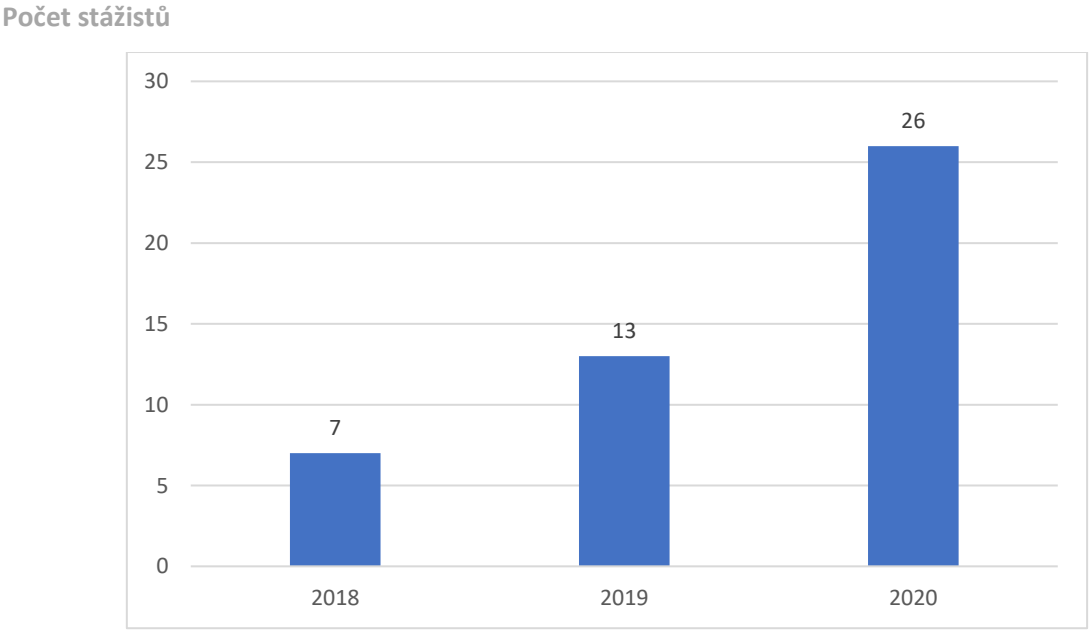
V roce 2020 měl Úřad naplnit povinný podíl v zaměstnávání osob se zdravotním postižením celkem ve výši 8,69 osob. Plnění povinného podílu bylo splněno zaměstnáváním osob se zdravotním postižením ve výši 1 osoba a odebíráním výrobků a služeb ve výši 11,54 osob.

Spolupráce s vysokými školami a odborné praxe studentů škol

Vedle pracovních příležitostí Úřad 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 2020 absolvovalo stáž 26 studentů, což bylo o 13 více než v roce 2019. Stáže byly jak technického, tak právního a politicko-bezpečnostního zaměření. Součástí spolupráce se studenty jsou také pravidelné odborné konzultace diplomových a seminárních prací.

V roce 2020 byly uzavřeny další smlouvy ke spolupráci s vysokými školami, a to Smlouva o spolupráci s Univerzitou Hradec Králové a Univerzitou Palackého v Olomouci.



Investice a rozvoj

V roce 2020 oddělení investic a rozvoje realizovalo několik investičních akcí, které zejména přispěly k rozšíření kancelářských prostor.

Na pracovišti Cejl, Brno proběhla očekávaná oprava fasády celého objektu a dále se v tomto objektu realizovala menší úprava kancelářských prostor. Pro nově plánované pracoviště Úřadu, objekt Gorkého, Brno, se připravila projektová dokumentace pro celkovou rekonstrukci tohoto objektu. Na pracovišti VUT – Fakulta Podnikatelská, Brno, došlo k rozšíření kancelářských prostor pro nově nastupující zaměstnance Úřadu. V Praze probíhaly přípravné práce související s rozšířením administrativních prostor v objektu Olšanská, a dále přípravné práce související s novým budoucím objektem v Praze 6.

Nová administrativní budova NÚKIB v Brně, Černých Polích

V únoru na základě informací Úřadu vlády ČR došlo k pozastavení činností spojených s přípravou zadávacího řízení na veřejnou zakázku „Výstavba administrativního objektu NÚKIB“. Tato informace byla prostřednictvím administrátora veřejné zakázky poskytnuta třem oceněným účastníkům soutěže o návrh. V září byl ředitelem úřadu znovuobnoven postup v zadávacím řízení, který reflektoval změny z hlediska plánovaného obsazení NÚKIB v souladu s Koncepcí rozvoje NÚKIB, schválenou usnesením vlády č. 848 ze dne 17. srpna 2020. V zájmu snížení výdajů ze státního rozpočtu byla stanovena kapacita objektu z původně plánovaných 400 zaměstnanců na 320 zaměstnanců.

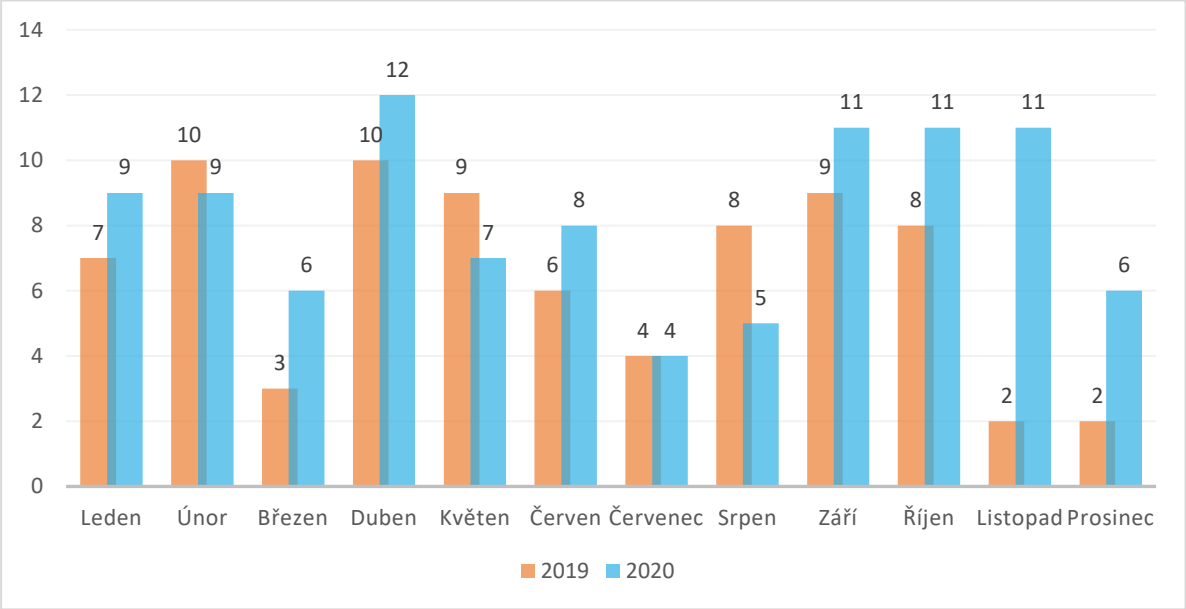
2 Sekce Národní centrum kybernetické bezpečnosti

Vládní CERT (GovCERT.CZ)

Evidence hlášení kybernetických bezpečnostních incidentů

Vývoj počtu kybernetických incidentů řešených GovCERT v letech 2019-2020

(dle měsíců)



V roce 2020 GovCERT řešil 99 kybernetických incidentů nahlášených 69 regulovanými subjekty a 29 neregulovanými subjekty. Proti roku 2019 jde o 26 % nárůst incidentů, který je velmi pravděpodobně výsledkem kombinace většího povědomí o existenci a aktivitách NÚKIB a samotného zvýšení počtu kybernetických útoků. Větší povědomí o NÚKIB velmi pravděpodobně stojí i za 967 % nárůstem řešených incidentů týkajících se neregulovaných subjektů (ze 3 v roce 2019 na 29 v roce 2020). V kombinaci s daty z roku 2019 lze říci, že nejvíce incidentů GovCERT řeší v dubnu a nejméně v červenci (viz graf).

Zhruba 45 % incidentů bylo méně významných, 45 % významných a 10 % z nich bylo klasifikováno jako velmi významné (pro definici kategorií viz BOX 1).

Nejvýznamnějším a nejzávažnějším incidentem bylo bezesporu zašifrování systémů Fakultní nemocnice Brno ransomwarem v březnu 2020, které vyústilo ve významné omezení provozu nemocnice a škody v řádu stovek milionů korun.

V březnu se obětí ransomwaru stala rovněž Psychiatrická nemocnice Kosmonosy, kde nebyla ohrožena schopnost nemocnice poskytovat péči pacientům a nedošlo ani k zasažení systémů, na kterých závisely lidské životy. Ochromena byla především administrativní infrastruktura nemocnice.

Závažnost incidentů dle Vyhlášky č. 82/2018 Sb.

Velmi významný kybernetický bezpečnostní incident, při kterém je přímo a významně narušena bezpečnost poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být všemi dostupnými prostředky zabráněno dalšímu šíření kybernetického bezpečnostního incidentu včetně minimalizace vzniklých i potenciálních škod.

Významný kybernetický bezpečnostní incident, při kterém je narušena bezpečnost poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být vhodnými prostředky zabráněno dalšímu šíření kybernetického bezpečnostního incidentu včetně minimalizace vzniklých škod.

Méně významný kybernetický bezpečnostní incident, při kterém dochází k méně významnému narušení bezpečnosti poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje zásahy obsluhy s tím, že musí být vhodnými prostředky omezeno další šíření kybernetického bezpečnostního incidentu včetně minimalizace vzniklých škod.

V srpnu došlo v důsledku úspěšné spear-phishingové kampaně proti významné instituci státní správy ke kompromitaci několika desítek e-mailových účtů. Kromě narušení důvěrnosti obsahu schránek došlo k výpadku e-mailových služeb.

Další aktivity GovCERT v roce 2020

V uplynulém roce GovCERT:

- upozornil na 22 hrozeb a zranitelností,
- provedl 12 penetračních testů,
- spustil službu skenování zranitelností s důrazem na zdravotnická zařízení, tuto službu se rozhodlo využít 10 organizací,

- rozšířil portfolio nabízených služeb o simulaci phishingové kampaně na míru, této nabídky využily 4 subjekty, jejichž pracovníci si vyzkoušeli, jaké to je být terčem cíleného phishingu,
- participoval na vydání 3 reaktivních opatření.

Odbor kybernetických bezpečnostních politik

Oddělení národních strategií a politik

Při zajišťování kybernetické bezpečnosti na národní úrovni je zásadní spolupráce dotčených subjektů, a to i v rovině nastavování strategického rámce. V rámci NÚKIB se této činnosti věnuje oddělení národních strategií a politik (dále jen „NASTAPO“).

NASTAPO zajišťuje efektivní koordinaci, harmonizaci a vyhodnocování kybernetických bezpečnostních politik napříč veřejnou sférou a dalšími subjekty. I za rok 2020 došlo k vyhodnocení plnění úkolů akčního plánu, který kontroluje specifické úkoly vedoucí k naplňování *Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020*. Jednalo se o poslední rok platnosti tohoto akčního plánu, a podstatná část úkolů tak byla vyhodnocena již jako splněná či plněná. Vlivem pandemie covid-19 nicméně ve srovnání s rokem předchozím vzrostl počet průběžných úkolů, které byly plněny pouze částečně.

Vzhledem ke konci platnosti předchozí zmíněné strategie probíhaly po celý rok 2020 intenzivní práce (ve spolupráci s dalšími relevantními aktéry) na strategii navazující. *Národní strategie kybernetické bezpečnosti České republiky* byla vládou schválena 30. listopadu 2020. Je založená na vizi vytváření odolné společnosti a infrastruktury proti kybernetickým hrozbám, sebevědomého působení státu v kyberprostoru a aktivním čelení celému spektru kybernetických hrozeb za pomoci spolehlivých spojenectví. Jedná se tak o kvalitativní posun v zajišťování kybernetické bezpečnosti, kdy je v České republice již vybudován pomyslný základ kybernetické bezpečnosti, na němž lze rozvíjet další aktivity. Naplňování vizí a cílů zmíněné strategie bude předmětem akčního plánu, který je vytvářen taktéž pod koordinací NASTAPO a za spolupráce s relevantními subjekty. Ke schválení bude předložen do poloviny roku 2021.

Pracovníci NASTAPO se v roce 2020 účastnili rozličných jednání a pracovních skupin (vlivem pandemie covid-19 povětšinou přesunutých na online platformy) a akcentovali v nich význam zajištění kybernetické bezpečnosti. Namátkou lze zmínit spolupráci na tvorbě *Národní strategie pro čelení hybridnímu působení*, jejímž gestorem je Ministerstvo obrany. Ta by měla být vládou schválena v první polovině roku 2021.

Pracovníci NASTAPO rovněž participovali na Pracovní skupině k atribuci, která je koordinována Vojenským zpravodajstvím. Cílem skupiny je vytvořit a nastavit národní systém atribuce u kybernetických útoků, který bude využívat veškeré dostupné informační zdroje a zároveň bude obsahovat procesy pro efektivní a koordinovanou reakci.

NASTAPO se v roce 2020 rovněž podílelo na nastavování bezpečnosti 5G sítí, a to prostřednictvím posouzení zavedení opatření EU 5G Toolboxu do českého právního řádu a přípravy návrhů na další implementaci těchto opatření. Kromě NASTAPO, které bylo iniciátorem a koordinátorem této aktivity, se na ní podíleli také zástupci dalších státních institucí, do jejichž působnosti spadá budování 5G sítí, regulace telekomunikací a ochrana bezpečnostních zájmů České republiky. V návaznosti na vyhodnocení zavedení EU 5G Toolboxu iniciovalo NASTAPO v závěru roku 2020 také diskusi o roli státu při zmírňování rizik spojených s dodavateli do 5G sítí, v níž NASTAPO v roce 2021 pokračuje také za přispění dalších zástupců veřejného a soukromého sektoru.

Posílení a prohlubování spolupráce napříč rozličnými aktéry si klade za cíl rovněž konference CyberCon, kterou uspořádal NÚKIB ve spolupráci se studentským spolkem Security Outlines již pošesté. Smyslem konference, která se uskutečnila 16.–17. září, je zejména výměna zkušeností mezi experty na kybernetickou bezpečnost z různých sfér. Konference byla pro účastníky zdarma, a i přes epidemiologická opatření omezující návštěvnost se jí v obou dnech celkově zúčastnilo přes 300 osob.

V rámci NASTAPO působí pracovník LEGAD, jehož náplní je mj. poskytování právního poradenství vládnímu CERT a odboru kybernetických bezpečnostních politik a řešení právních otázek v rámci sekce Národní centrum kybernetické bezpečnosti (ve spolupráci s dalšími organizačními celky NÚKIB). Mezi hlavní úkoly LEGADa v oblasti spolupráce s vládním CERT bylo v roce 2020 řešení právních otázek souvisejících se spuštěním platformy Neveřejného webu, příprava novelizace části působnosti vládního CERT dle zákona o kybernetické

bezpečnosti, příprava a konzultace smluv pro penetrační testování či nastavení mechanismu pro předávání informací z evidencí vedených NÚKIB bezpečnostním složkám. LEGAD v roce 2020 participoval na vyhodnocení zavedení opatření EU 5G Toolboxu v České republice, revizi krizové legislativy a na přípravě varování v souvislostmi s kybernetickými útoky na zdravotnická zařízení. Kromě uvedených aktivit se LEGAD zabýval také průběžným poradenstvím odboru vládní CERT, revizí legislativních materiálů v rámci mezirezortních připomínkových řízení, účastnil se mezinárodního cvičení Cyber Coalition atd.

Oddělení cvičení

Stejně jako v předchozích letech i v roce 2020 představovala významnou součást aktivit NÚKIB cvičení kybernetické bezpečnosti, a to navzdory situaci spojené s šířením nového typu koronaviru. Připravovaná i uskutečněná cvičení se opět zaměřovala mimo jiné na ověřování technických, strategických i komunikačních dovedností účastníků a řadila se do více typů cvičení kybernetické bezpečnosti[1]. Ta nejvýznamnější z nich jsou uvedena níže.

Aktivity v ČR

Národní komunikační cvičení Comm Czech 2020

Ve dnech 4.–7. srpna 2020 se konalo třetí komunikační cvičení Comm Czech 2020. Toto cvičení NÚKIB pořádá pravidelně jedenkrát za dva roky. Cílem cvičení bylo ověřit průchodnost nastavených komunikačních kanálů nahlášených povinnými subjekty dle ZKB, kde sledovanou jednotkou byl informační systém. Zároveň sledovalo jejich aktuálnost a soulad s § 16 ZKB. Aktuálnost a dostupnost těchto údajů je důležitá především pro případ krize, kdy by vyvstala potřeba s povinnými subjekty rychle komunikovat. V případě jejich nedostupnosti by tak mohlo dojít k četným škodám.

Převážná většina kontaktů uvedených ke konkrétním informačním systémům byla aktuální a dostupná, čímž výsledky cvičení prokázaly připravenost povinných subjektů s NÚKIB neprodleně komunikovat.

[1] Národní úřad pro kybernetickou a informační bezpečnost - Cvičení (nukib.cz)

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 potřetí jeho součástí bylo i komplexní netechnické cvičení připravené ve spolupráci s Velitelstvím kybernetických sil a informačních operací AČR zaměřené zejména na vojenský sektor bezpečnosti, ale také na hybridní hrozby, strategickou komunikaci a další netechnické aspekty kybernetické 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.

Cvičení pro Správu Pražského hradu

Cvičení pro Správu Pražského hradu se uskutečnilo dne 18. června 2020. Za cíl si stanovilo procvičit rozhodovací procesy pod časovým tlakem a při nedostatku informací a otestovat interní i externí komunikaci během krize.

Scénář byl koherentně zasazen do souvislého děje a připraven na míru cvičící instituci. Cvičení se zaměřovalo mimo jiné na problematiku zranitelnosti uživatele či mediální aspekt řešení krizové situace. Závěrem byla účastníkům poskytnuta prezentace s příklady dobré praxe.

Cvičení v rámci konference CyberCon Brno 2020

Součástí úřadem organizované konference bylo i krátké cvičení, které se uskutečnilo formou workshopu a nabídlo omezenému množství účastníků vyzkoušet si na vlastní kůži, jaké je to být v roli cvičícího na akci připravované NÚKIB.

Díky cvičení měli účastníci možnost mimo jiné získat hlubší porozumění ekonomickému, právnímu, mediálnímu či politickému kontextu krizové situace odehrávající se kyberprostoru, nebo z něj pocházející.

Cvičení mělo dále za cíl zdůraznit komplexnost krizového managementu a rozhodovacího procesu a postupů vedoucích k překonání krize; pochopit důsledky kompromitace citlivých dat útočníkem; poukázat na význam role nejvyššího vedení organizace při zvládání kybernetických bezpečnostních incidentů a navyšování kybernetické bezpečnosti jako takové; porozumět důsledkům ztráty důvěry v informační a komunikační systémy a technologie; a obecně zvýšit povědomí a prohloubit znalosti účastníků cvičení v oblasti kybernetické bezpečnosti.

Přednáška pro vysokoškolské studenty

Plánované cvičení v rámci předmětu Kybernetická bezpečnost mělo za cíl přiblížit studentům reálnou podobu kybernetických cvičení. Takové cvičení vyžaduje mimo jiné aktivní participaci studentů na jeho průběhu. Vzhledem k tomu, že celý semestr podzim 2020 probíhal na Masarykově univerzitě distanční formou, která by měla negativní vliv na průběh a výstup cvičení, byla aktivita nahrazena přednáškou.

Ta se věnovala především procesu přípravy cvičení a vybraným příkladům cvičení včetně doprovodných grafických materiálů. Diskutovány byly účel a přínosy cvičení a pozice NÚKIB při jejich tvorbě.

Zahraniční aktivity

Cyber Coalition 2020

V listopadu 2020 se uskutečnil již třináctý ročník pětidenního mezinárodního cvičení kybernetické bezpečnosti Cyber Coalition, pořádaného Severoatlantickou aliancí. Cvičení se zúčastnila přibližně tisícovka expertů z 29 zemí, a to ať už v roli cvičících či pozorovatelů.

Česká republika se v roce 2020 zapojila již po desáté. Stejně jako v předchozích letech bylo cvičení na národní úrovni koordinováno Národním úřadem pro kybernetickou a informační bezpečnost za civilní část a nově Velitelstvím kybernetických sil a informačních operací (dále VeKySIO) za vojenskou část. Obě koordinující složky pro cvičení tradičně vytvářejí své týmy, jejichž součástí jsou kromě zaměstnanců těchto institucí i přizvaní odborníci z partnerských institucí. VeKySIO bylo nuceno svou účast kvůli pandemii omezit a aktivně se tak cvičení zúčastnil pouze NÚKIB se svými partnery.

Scénář letošního ročníku byl zasazen do prostředí vojenské mise ve fiktivní zemi. Stejně jako v předchozích letech, i letos účastníci řešili úkoly zaměřené na procesní a koordinační aspekt spolupráce. Nedílnou součástí cvičení však byly i technické výzvy, které reflektovaly aktuální bezpečnostní trendy. V praxi tak účastníci řešili kompromitaci systémů pozemní satelitní stanice, exfiltraci dat za využití podvržené fitness aplikace nebo kybernetický útok provedený za pomoci infikovaného USB disku.

Stejně jako v předchozích letech prostupoval celým scénářem cvičení právní aspekt řešení incidentů, v rámci kterého, byly řešeny otázky jako vydání dat k dalšímu vyšetřování či přeshraniční spolupráce. Z partnerů NÚKIB se do cvičení zapojila Národní centrála proti organizovanému zločinu SKPV Policie České republiky a Vojenské zpravodajství.

Výraznou změnou oproti předchozím ročníkům byla transformace formy cvičení, a to v reakci na celosvětové šíření nového typu koronaviru, které znemožnilo vyslání nejen českých zástupců do estonského Tallinnu, ze kterého mělo být cvičení řízeno. Rovněž samotný plánovací proces byl jak pro organizátory, tak účastníky přesunut na virtuální platformu a veškerá koordinace a komunikace byla tomuto přizpůsobena. Pořádání cvičení vzdálenou formou bylo dobrou příležitostí k procvičení výše uvedeného v reálných podmínkách, tedy kdy většina zaměstnanců pracuje z domu, a držení se zásady „train as you fight".

Kromě toho, že jsou zástupci NÚKIB a VeKySIO po boku ostatních spojenců a partnerů členy plánovací skupiny cvičení, zástupce NÚKIB, respektive České republiky je rovněž součástí užšího plánovacího týmu cvičení (core planning team), který má na starosti přípravu a organizaci na nejvyšší úrovni. Jako středoevropský stát tak nemalou měrou přispíváme do aliančního cvičení, kterého se účastní spojenci a partneři ze Severní Ameriky a celé Evropy. Stejně je tomu tak i u dalších mezinárodních cvičení a dále to dokládá jen to, že Česká republika není pouhým konzumentem mezinárodních cvičeních, ale je významným a plnohodnotným partnerem nejen pro oblast kybernetických cvičení.

Locked Shields 2020

Šestý ročník největšího a nejkomplexnějšího mezinárodního cvičení Locked Shields konaného pod záštitou expertního centra CCD COE v estonském Tallinnu byl plánován na 26.–30. dubna 2020. Vlastnímu cvičení předcházely tři plánovací konference.

Vzhledem k nepříznivé situaci týkající se nového typu koronaviru bylo však cvičení krátce po finální plánovací konferenci bez náhrady zrušeno. S jeho realizací se však počítá v roce 2021, načež se zcela reálně nabízí možnost zcela vzdálené podoby cvičení. Zde bude maximálně využita již připravená část nerealizovaného ročníku.

Nedílnou podmínkou CCD COE pro aktivní účast jednotlivých států v roli Modrých (cvičících) týmů je aktivní podíl na přípravě obsahu cvičení. V této souvislosti Česká republika již tradičně

poskytla své zástupce do Bílého (organizačního, právního, mediálního), Červeného (simulujícího útočníky) a Zeleného (technická infrastruktura) týmu. Na přípravách aktivit Bílého a Červeného týmu se podílí zaměstnanci NÚKIB, na přípravách technické infrastruktury v Zeleném týmu se pravidelně podílí zástupci Armády ČR.

EU Integrated Resolve

Zástupci NÚKIB se na národní úrovni také částečně zapojili do přípravy a provedení první části cvičení EU Integrated Resolve zaměřeného na komplexní procvičení krizového managementu EU. Záměrem cvičení bylo zlepšit a posílit schopnost reakce EU na komplexní krizovou situaci hybridní povahy s vnější dimenzí. Z důvodu eskalace pandemické situace v Evropě však byla EU donucena druhou část cvičení přesunout na rok 2021.

Sdílení know-how se zahraničními partnery

Vzhledem k pandemické situaci byla část cvičení nahrazena či doplněna šířením know-how o přípravě a exekuci table-top cvičení. Jedním z takových případů byla účast Úřadu na iPCSS – distanční iteraci prestižního kurzu Program on Cyber Security Studies (PCSS), který pořádá George C. Marshall European Center for Security Studies.

V předešlých třech na sebe navazujících letech pro něj zástupci NÚKIB připravili a provedli netechnické cvičení, jehož cílem bylo přiblížit problematiku pro účastníky kurzu. Letos forma kurzu uspořádání cvičení neumožnila. Zástupci NÚKIB však své zkušenosti a dobrou praxi sdíleli s až 80 účastníky kurzu z přibližně 30 zemí, ve kterých jsou vysoce postavenými pracovníky v oblasti kybernetické bezpečnosti.

Dalším příkladem šíření know-how byla přednáška v rámci série přednášek expertů pro Organizaci pro bezpečnost a spolupráci v Evropě.

Oddělení strategických informací a analýz

Oddělení strategických informací a analýz se věnuje zejména analýze a monitoringu kybernetických hrozeb. Jeho činnost směřuje jednak k analytické podpoře dalších organizačních celků v rámci NÚKIB, jednak i partnerských institucí ve státní správě, veřejném a soukromém sektoru. Oddělení každoročně zpracovává Zprávu o stavu kybernetické

bezpečnosti České republiky, která přináší komplexní pohled na vývoj kybernetické bezpečnosti v celé společnosti.

Dalšími důležitými produkty jsou Měsíční souhrn dění v kybernetické bezpečnosti pro partnery Úřadu nebo automatizovaný monitoring zranitelností zdravotnických přístrojů pro nemocnice a další zdravotnická zařízení. V roce 2020 se NÚKIB významně posunul v rozvoji kapacit pro oblast Cyber Threat Intelligence a zlepšil tím své schopnosti monitoringu aktuálního dění v kyberprostoru a prevence kybernetických útoků.

Oddělení mezinárodních organizací a práva

Kybernetická bezpečnost České republiky závisí do velké míry na vývoji situace v zahraničí a rozhodnutích přijímaných na evropské a mezinárodní úrovni. Mezinárodní spolupráce je důležitým nástrojem České republiky k ovlivňování tohoto vývoje. Zájmy České republiky v oblasti kybernetické bezpečnosti v mezinárodních organizacích a integračních uskupeních, zejména pak v EU, OSN, NATO, ale i OECD, OBSE a ITU, zastupuje NÚKIB společně s Ministerstvem zahraničních věcí (dále jen „MZV"), Ministerstvem obrany a dalšími partnery[2].

Evropská unie (EU)

V Radě EU je NÚKIB reprezentován vlastním zástupcem v Horizontální pracovní skupině pro kybernetické otázky, která se zabývá aspekty spolupráce v kybernetické bezpečnosti v rámci EU.

V roce 2020 se aktivity NÚKIB 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").[3] Toto nařízení bude realizovat podporu výzkumu a průmyslu v oblasti kybernetické bezpečnosti a upravuje čerpání financí z projektů Program Digitální Evropa a Horizont Evropa. Nařízení se i zásluhou německého předsednictví podařilo po několikaletých peripetiích úspěšně projednat v tzv. trialozích ke konci roku 2020.

[2] Ministerstvo průmyslu a obchodu, Český telekomunikační úřad a další.
[3] Návrh nařízení Evropského parlamentu a Rady, kterým se zřizuje Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center.

Dále NÚKIB dokončil v lednu 2020 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),[4] který přináší další konkrétní rizika a návrhy opatření k tomu, jak je zmírnit. V roce 2020 tak probíhala implementace uvedených opatření.

K naplnění úkolů dle nařízení o Agentuře ENISA a bezpečnostní certifikaci ICT produktů, služeb a procesů (tvorba EU certifikačních „schémat“) účinném od června roku 2019 byla vytvořena Evropská skupina pro kybernetickou certifikaci, jejíž je NÚKIB součástí a kde se společně s ostatními státy podílí na přípravě schémat pro certifikaci (aktuálně např. v oblasti bezpečnosti cloudových služeb).

V roce 2020 došlo k první zásadnější aplikaci Cyber Diplomacy Toolboxu (uložení sankcí konkrétním osobám a entitám) a spuštění sítě CyCLONe (Cyber Crisis Liaison Organisation Network) a jejím prověření ve cvičení BlueOLEx.

Závěr roku 2020 přinesl nový kybernetický „balíček“ z dílny EU, na jehož přípravě se podílela i ČR. Strategie kybernetické bezpečnosti EU upozorňuje na ohrožení mezinárodní bezpečnosti a stability kvůli geopolitickému soupeření mezi státy. Hybridním hrozbám vyzdvihuje důležitost kybernetické bezpečnosti jako zásadního aspektu pro důvěru lidí v inovace a automatizaci; velký důraz klade na ochranu kritické infrastruktury. Dojde jak k posílení investic do technických řešení, tak k budování operačních kapacit k předcházení a řešení kybernetických útoků.

Pokud jde o návrh směrnice nahrazující Směrnici NIS, Evropská komise navrhuje podstatně více harmonizovat právní předpisy a přístupy členských států v oblasti kybernetické bezpečnosti. Nově by podle ní mělo být upraveno koordinované odhalování zranitelností, rozšířit by se měly sektory povinných osob, sjednotit by se měl způsob identifikace povinných osob a mají vzniknout nové povinnosti hlášení incidentů. Přestože je v některých ohledech navrhovaná harmonizace z pohledu ČR zbytečně silná, jedná se o solidní základ pro vyjednávání o konečné podobě této důležité unijní úpravy.

[4] Skupina pro spolupráci (Směrnice NIS), Kybernetická bezpečnost sítí 5G: Soubor opatření EU pro zmírnění rizik

Česká republika se v nadcházejících letech bude účastnit naplňování konkrétních opatření Strategie kybernetické bezpečnosti EU, jakož i důležitých vyjednávání o konečné podobě směrnice, která má nahradit Směrnici NIS. Oba dokumenty lze bez nadsázky označit za zásadní pro politické a legislativní ukotvení kybernetické bezpečnosti v EU na řadu let. Jejich ambicióznost odráží rostoucí důležitost kybernetické bezpečnosti na evropské i mezinárodní úrovni. Vedle vydání a postupné implementace 5G EU Toolboxu a dokončení vyjednávání o nařízení o kompetenčním centru se jedná o příklady úspěšné spolupráce ČR v rámci EU v roce 2020.

Organizace Severoatlantické smlouvy (NATO)

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 2020 připravena v úzké spolupráci NÚKIB, VZ a MO již čtvrtá zpráva o stavu kybernetických schopností ČR se zvláštní kapitolou zaměřenou na oblast bezpečnosti dodavatelského řetězce.

NÚKIB také pokračoval v úspěšné spolupráci s NATO Cooperative Cyber Defence Centre of Excellence v estonském Tallinnu a výzkumných projektech (Cyber Law Toolkit).[5]

Organizace spojených národů (OSN)

Na půdě OSN v roce 2020 pokračovaly v práci dvě skupiny, které byly ustanoveny v roce 2019 a věnují se otázkám odpovědného chování států v kyberprostoru.

První z nich je nově ustanovená Open-Ended Working Group (OEWG), která je aktuálně nejvýznamnější platformou v systému OSN ke kybernetické bezpečnosti a na jejíž činnosti se NÚKIB a MZV aktivně podílejí. Skupina se věnuje otázkám nových hrozeb v kyberprostoru; uplatnitelnosti mezinárodního práva v kyberprostoru; normám, pravidlům a principům v kyberprostoru; opatřením pro zvyšování důvěry mezi státy v kyberprostoru; budování kapacit v kybernetické bezpečnosti a budoucnosti dalšího mezivládního dialogu ke kybernetické bezpečnosti na úrovni OSN.

[5] International cyber law: interactive toolkit (ccdcoe.org)

NÚKIB se v průběhu roku 2020 účastnil řady neformálních jednání podobně smýšlejících zemí OEWG a podílel se na koordinaci a přípravě pozic ČR v OEWG spolu s příslušnými celky MZV ČR, které je hlavním gestorem.

V roce 2020 se v New Yorku uskutečnilo od 10. do 14. února druhé z celkem tří kol substantivních jednání OEWG. ČR zde vedle představitelů MZV ČR zastupoval i expert NÚKIB na mezinárodní právo. S ohledem na vývoj pandemické situace bylo třetí kolo substantivních jednání OEWG přesunuto na březen 2020. Cílem OEWG, které je doposud nejinkluzivnějším globálním formátem k otázkám kybernetické bezpečnosti, je přijetí konsenzuální zprávy k výše zmíněným tématům, která prohloubí již existující mezinárodní rámec odpovědného chování států v kyberprostoru.

Vedle OEWG NÚKIB v roce 2020 na úrovni OSN monitoroval také vývoj v UN Group of Governmental Experts (UN GGE), skupině vládních expertů zabývající se odpovědným chováním států v kyberprostoru. UN GGE se skládá z 25 členů vybraných dle spravedlivého geografického rozložení a ČR mezi členy není. NÚKIB však vývoj v této skupině dlouhodobě sleduje, a to zejména s ohledem na souvislost s paralelním formátem OEWG a možné důsledky jednání UN GGE v oblasti uplatnitelnosti mezinárodního práva v kyberprostoru.

Zároveň v roce 2020 započala příprava fungování Ad Hoc Committee on Cybercrime (AHC), která byla nově ustanovena na úrovni OSN koncem roku 2019. Cílem AHC je posílit stávající regionální a mezinárodní mechanismy v oblasti kyberzločinu se snahou vytvořit a přijmout v tomto ohledu novou mezinárodní úmluvu. NÚKIB, spolu s MZV ČR a MS ČR, vývoj příprav a organizačních jednání v roce 2019 sledoval. První organizační jednání skupiny by se mělo po četných odsunech uskutečnit v květnu 2021. Lze předpokládat, že NÚKIB bude vývoj v AHC i nadále sledovat, a to zejména s cílem zajistit, aby jakékoliv výstupy AHC byly v souladu se stávající Úmluvou Rady Evropy o kyberkriminalitě, kterou ČR ratifikovala v roce 2013, a jejími stávajícími i právě projednávanými dodatkovými protokoly.

Mezinárodní telekomunikační unie (ITU)

V roce 2020 NÚKIB nově věnoval zvýšenou pozornost a monitoroval vývoj v International Telecommunications Union (ITU), specializované agentuře OSN zabývající se problematikou informačních a komunikačních technologií. Problematika správy internetu, tzv. Internet

Governance, a kybernetické bezpečnosti jako takové se v agendě ITU v posledních letech objevuje čím dál častěji.

NÚKIB v roce 2020 sledoval a analyzoval dění zejména v oblasti standardizace telekomunikačních technologií, konkrétně pak v pracovních skupinách zabývajícími se budoucími sítěmi (tzv. Future Networks) a protokoly.

V roce 2020 se rovněž napříč pracovními skupinami standardizačního sektoru uskutečnila řada jednání k dalšímu pracovnímu programu ITU na období 2021–2025. Lze předpokládat, že agenda správy internetu a snaha některých států v ITU unilaterálně prosadit nové standardy a vlastní přístup ke správě bude pouze sílit. Takové snahy mohou mít negativní důsledky na stávající model správy internetu a kybernetickou bezpečnost jako takovou. I proto se NÚKIB bude problematice na úrovni ITU společně s dalšími národními partnery nadále věnovat.

Organizace pro bezpečnost a spolupráci v Evropě (OBSE)

V rámci OBSE roce 2020 pokračovala práce Informal Working Group (IWG) k otázkám kybernetické bezpečnosti. Skupina se primárně zabývá implementací dříve přijatých opatření pro budování důvěry mezi státy v oblasti kybernetické bezpečnosti, tzv. Confidence Building Measures (CBMs). Celkem šestnáct opatření má za cíl podpořit spolupráci a transparentnost států v kyberprostoru.

NÚKIB se v roce 2020 účastnil dvou zasedání IWG, během kterého zástupci NÚKIB představili poslední vývoj v implementaci jednotlivých CBMs s důrazem na nejnovější vývoj strategií, právních předpisů a politik v oblasti kybernetické bezpečnosti.

NÚKIB se i nadále podílel na implementaci zejména CBM 16 (Koordinované zveřejňování zranitelností) a realizoval bilaterální výměnu informací s vybranými státy (Kazachstán, Mongolsko, Kyrgyzstán, Ukrajina, Velká Británie) v rámci CBM 8 (Výměna informací mezi styčnými pracovníky). Podobně jako v předešlých létech, proběhla i v roce 2020 dvě komunikační cvičení pro styčné pracovníky, která slouží k zajištění funkčních komunikačních kanálů a výměně informací mezi jednotlivými členskými státy a příslušnými celky.

ČR při tomto cvičení zastupovali právě pracovníci NÚKIB. Ti se účastnili i řady virtuálních workshopů na téma kybernetické bezpečnosti, které OBSE v důsledku globální pandemické

krize připravilo. Zároveň NÚKIB uspořádal pro členské státy OBSE vlastní workshop na téma přípravy cvičení kybernetické bezpečnosti, kde pracovníci NÚKIB sdíleli dlouholeté know-how a zkušenosti z praxe. NÚKIB se bude dění v IWG během nadcházejícího švédského předsednictví OBSE nadále aktivně účastnit i v roce 2021.

Organizace pro hospodářskou spolupráci a rozvoj (OECD)

V OECD v roce 2020 pokračovala práce Working Group on Security in the Digital Economy (SDE), které se NÚKIB pravidelně účastní. Stěžejní pro NÚKIB byla práce v nově ustanovených expertních podskupinách, jejichž analytické výstupy mohou posloužit jako vodítko při zavádění nebo revizi národních politik, strategií a legislativy v oblasti digitální bezpečnosti. Pracovníci NÚKIB se proto účastnili jednání expertní skupiny k bezpečnosti internetu věcí, tzv. IoTs, a expertní skupiny ke koordinovanému zveřejňování zranitelností, tzv. Coordinated Vulnerability Disclosure.

Výstupem práce těchto skupin jsou expertní zprávy OECD, které mapují stávající úpravu napříč členskými státy OECD, doporučují ověřené postupy a shrnují opatření, které v tomto ohledu mohou zavést vládní instituce i soukromý sektor.

V průběhu roku 2020 rovněž na úrovni OECD vznikla nová expertní skupina k odpovědné reakci soukromého sektoru na kybernetické incidenty (tzv. Responsible Response). NÚKIB se v této expertní skupině bude prostřednictvím svých pracovníků nadále angažovat.

Global Forum on Cyber Expertise (GFCE)

V roce 2020 se NÚKIB i nadále angažoval virtuální formou v aktivitách Global Forum on Cyber Expertise (GFCE), ke které se ČR připojila v roce 2018. Začátkem roku se z mezinárodní platformy GFCE stala nadace s vlastním sekretariátem. Další směřování a pracovní program na nadcházející roky byl představen během virtuálního výročního jednání, kterého se zástupci NÚKIB účastnili. Rovněž se NÚKIB angažoval v pracovní skupině k CBMs, normám a kybernetické diplomacii a v pracovní skupině k ochraně kritické infrastruktury.

V roce 2020 GFCE rovněž zveřejnilo tzv. Global Research Agenda s cílem analyzovat konkrétní nedostatky kapacit v oblasti kybernetické bezpečnosti a formulovat možné odpovědi a projekty, které by k budování kapacit přispěly.

Prague 5G Security Conference a spuštění Prague 5G Repository

V roce 2020 uspořádal NÚKIB druhý ročník Prague 5G Security Conference, která proběhla od 23. do 24. září virtuální formou. Konference k bezpečnosti 5G s globálním přesahem se opět uskutečnila pod záštitou premiéra ČR Andreje Babiše a v koordinaci s MZV ČR. Akce byla uzavřena pouze pro pozvané hosty a celkem na ni bylo pozváno více než 1200 hostů ze 120 zemí.

Kromě vládních představitelů a zástupců mezinárodních organizací a předních think-tanků se konference účastnili i zástupci vybraných operátorů. Na konferenci vystoupilo téměř 50 řečníků z celého světa. Hlavním tématem byl konstruktivní dialog o konkrétních řešeních a opatřeních (legislativních, strategických, technických a jiných) v oblasti bezpečnosti 5G.

Za ČR na konferenci vystoupil premiér ČR Andrej Babiš, který ocenil Prague Proposals z r. 2019, které přispěly ke zvýšení povědomí o tomto tématu a poukázal na nutnost implementace EU 5G Security Toolbox, stejně jako Tomáš Petříček, ministr zahraničních věcí ČR. Mezi řečníky nechyběl ani ředitel NÚKIB Karel Řehka, náměstek MPO ČR pan Petr Očko a Předsedkyně rady ČTÚ paní Hana Továrková.

Konference se těšila, podobně jako v roce 2019, velkému zájmu high-level zahraničních představitelů vlád zejména ze států, které jsou strategickými partnery nebo partnery ČR v kybernetické bezpečnosti.

Na konferenci vystoupil Mike Pompeo, ministr zahraničních věcí USA, který představil tzv. 5G Clean Path Initiative. Rovněž vystoupil Peter Dutton, ministr vnitra Austrálie, který představil novou strategii kybernetické bezpečnosti a národní rámec pro posílení ochrany před nedůvěryhodnými vendory, kteří by mohli porušovat australskou legislativu. Nechyběl ani Matt Warman, ministr pro digitální infrastrukturu Velké Británie, který představil nový zákon o bezpečnosti telekomunikací, který zavede kontrolní mechanismy nedůvěryhodných vendorů a zpřísní bezpečnostní kritéria a povinnosti pro operátory.

Na konferenci také vystoupila Věra Jourová, místopředsedkyně EK pro hodnoty a transparentnost, která upozornila na nárůst útoků na kritickou infrastrukturu ze strany státy sponzorovaných aktérů a zdůraznila zásadní roli implementace EU 5G Security Toolbox na národní úrovni ČS EU.

Hlavním výstupem konference v roce 2020 bylo představení tzv. Prague 5G Repository, virtuální platformy pro sdílení stávajících nástrojů a přístupů k bezpečnosti 5G jednotlivých států. Konference navazovala na Prague Proposals, sadu doporučení zveřejněných v roce 2019 a na EU 5G Security Toolbox, který EU zveřejnila v lednu 2020.

Odbor kontroly

Rok 2020 byl z pohledu kontrolní a auditní činnosti negativně ovlivněn pandemií covid-19, kdy nová a neznámá situace zapříčinila nižší počet provedených kontrol a auditů, v porovnání s rokem předchozím, především z důvodu, že tyto činnosti nelze vykonávat zcela bez přímého kontaktu mezi zúčastněnými osobami, a to jak na straně kontrolujících, resp. auditorů, tak kontrolovaných, resp. auditovaných subjektů.

Za rok 2020 NÚKIB provedl 8 kontrol či auditů podle ZKB, respektive vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti (dále „VKB“). Kontrola či audit u povinných orgánů a osob dle ZKB ověřuje plnění povinností plynoucích ze ZKB a VKB. V rámci každé kontroly nebo auditu je rámcově ověřováno cca 150 kontrolních bodů. V oblasti kontroly a auditu byl pro NÚKIB zejména ve druhé polovině roku prioritou sektor zdravotnictví.

I v uplynulém roce NÚKIB rozvíjel spolupráci v kontrolní činnosti s dalšími regulátory. Jmenovitě například s Úřadem pro civilní letectví, se kterým NÚKIB spolupracuje dlouhodobě. NÚKIB dále nově podepsal memorandum s Úřadem pro jadernou bezpečnost, čímž tak vzájemně stvrdily oboustrannou podporu a spolupráci nejen při provádění kontrolní činnosti, ale i nad její rámec. Důležitým cílem spolupráce mezi NÚKIB a spolupracujícími úřady v oblasti kontroly je především snaha minimalizovat zátěž povinných orgánů a osob.

V průběhu kontrolní a auditní činnosti jsou identifikovány nejčastěji tyto nedostatky:

- nastavený systém zajišťování kybernetické bezpečnosti nepokrývá požadavky všech zainteresovaných stran,
- subjekty nedostatečně řídí aktiva a rizika spojená s kybernetickou bezpečností,
- bezpečnostní politiky a bezpečnostní dokumentace se často neaplikují v praxi, nebo jsou neaktuální,
- subjekty řídí nedostatečně rizika spojená s dodavateli,

- nefunkční systém zajišťování kontinuity činností,
- nedostatek odborníků na kybernetickou bezpečnost,
- nevhodná segmentace sítě,
- nedostatečný monitoring interní sítě,
- příliš krátká doba uchovávání log záznamů,
- používání zastaralého hardware a software, který již jeho výrobce nepodporuje.

Odbor regulace

V roce 2020 pracoval odbor regulace na novelizaci a tvorbě těchto vyhlášek a zákonů:

- **Novela vyhlášky o významných informačních systémech**

  V září 2020 vstoupila v platnost novela vyhlášky o VIS s účinností od 1.1.2021. Cílem této novely pak bylo zejména zjednodušit a zpřehlednit proces identifikace; zvýšit efektivnost vyhlášky a zvýšit tak i právní jistotu jejích adresátů.
- **Novela vyhlášky o provozovatelích základních služeb v oblasti zdravotnictví**

  V reakci na probíhající pandemii nemoci covid-19 a proběhnuvší kybernetické útoky na nemocnice v České republice došlo k úpravě znění vyhlášky o provozovatelích základních služeb ve vztahu k odvětví zdravotnictví. Účelem této úpravy bylo zařazení většího počtu nemocnic mezi provozovatele základní služby. Novela je účinná od 1. ledna 2021 a pro zařazení nových nemocnic mezi provozovatele základní služby musí proběhnout správní řízení.
- **Úprava cloud computingu**

  V srpnu 2020 vstoupila v účinnost novela zákona o informačních systémech veřejné správy, která upravuje využívání cloud computingu orgány veřejné správy. Uvedená úprava zavádí pravidla pro ověření poskytovatelů cloud computingu a služeb cloud computingu. Tato úprava trpěla řadou nedostatků, a proto se v průběhu roku 2021 bude dále upravovat. NÚKIB v souvislosti s touto úpravou aktivně pracoval na přípravě prováděcích právních předpisů a vyjednávání o celkovém regulatorním rámci. Termín vydání prováděcích právních předpisů je očekáván v roce 2021.

- **Opravy a doplnění zákonných ustanovení**

  Na počátku roku 2020 došlo k novelizaci zákona o kybernetické bezpečnosti, především k celkové změně ustanovení o přestupcích a pokutách za ně. Od roku 2017 trvající stav, kdy nevhodnou novelizací zákona došlo k vytvoření situace, že některé přestupky se překrývaly a za některé chyběly jakékoliv možnosti udělení pokuty, byl tak napraven.

Určování povinných osob

Určování informačních systémů, které spadají do působnosti ZKB, stále probíhá a počty povinných subjektů narůstají. Na konci roku 2020 byly počty následující:

- Správci kritické informační infrastruktury: 52 subjektů
- Prvky kritické informační infrastruktury: 120 informačních systémů
- Významné informační systémy: 177 informačních systémů
- Provozovatelé základní služby: 56 subjektů
- Informační systémy základní služby: 61 informačních systémů

Varování a reaktivní opatření NÚKIB: Opatření proti bezprostředním hrozbám

Jedním z úkolů NÚKIB je vydávání opatření podle zákona o kybernetické bezpečnosti. Mezi tato opatření pak patří varování o hrozbách v oblasti kybernetické bezpečnosti; reaktivní opatření k řešení kybernetického bezpečnostního incidentu anebo k zabezpečení informačních systémů nebo sítí a služeb elektronických komunikací a ochranné opatření ke zvýšení ochrany informačních systémů nebo služeb a sítí elektronických komunikací a na základě analýzy již vyřešeného kybernetického bezpečnostního incidentu.

Reaktivní opatření ze dne 17. 3. 2020 pro vybrané subjekty ve zdravotnictví v rámci reakce na závažný kybernetický bezpečnostní incident

Prvním reaktivní opatření, které NÚKIB v roce 2020 vydal uložil vybraným subjektům v oblasti zdravotnictví provést nezbytné úkony, které vedly k zabezpečení důležitých informačních a komunikačních systémů vybraných subjektů spadajících pod zákon o kybernetické bezpečnosti před kybernetickým bezpečnostním incidentem.

Reaktivní opatření nebylo vydáno plošně a jeho implementace byla povinná pouze pro konkrétní subjekty, kterým bylo doručeno. K reaktivnímu opatření byla vydána metodika, která měla za cíl napomoci adresátům reaktivního opatření při výkladu a praktické realizaci povinností, které jim byly reaktivním opatřením uloženy.

Varování ze dne 16. 4. 2020 před hrozbou kybernetických útoků na nemocnice a jiné významné cíle ČR

Měsíc po vydání reaktivního opatření vydal NÚKIB varování před hrozbou v oblasti kybernetické bezpečnosti, spočívající v realizaci rozsáhlé kampaně závažných kybernetických útoků na informační a komunikační systémy v České republice, zejména pak na systémy zdravotnických zařízení.

V důsledku vydání tohoto varování se subjekty regulované zákonem o kybernetické bezpečnosti museli popsanými hrozbami zabývat a přijmout adekvátní opatření. K varování NÚKIB vydal doporučení, které se zaměřovalo na technické a organizační otázky a konkretizovalo postupy definované ve varování.

Reaktivní opatření ze dne 16. 12. 2020 ve vztahu k aplikacím platformy Orion společnosti SolarWinds

Poslední reaktivní opatření roku 2020 vydal NÚKIB v souvislosti s riziky spojenými se softwarem americké společnosti SolarWinds. Správci systémů kritické informační infrastruktury, významných informačních systémů a systémů základní služby museli neprodleně provést bezpečnostní aktualizace, zkontrolovat, zda jejich systém nebyl kompromitován, a provést bezpečnostní audit.

Podpůrné materiály v oblasti kybernetické bezpečnosti v roce 2020

Přestože stejně jako v minulých letech NÚKIB i v roce 2020 pokračoval ve vydávání a aktualizaci celé řady podpůrných materiálů pro odbornou i laickou veřejnost, je vhodné výslovně uvést alespoň ty, které vznikly v návaznosti na změny každodenního života spojené s pandemií nemoci covid-19.

Z důvodu nutnosti přesunout každodenní soukromý i pracovní život alespoň z části do virtuální roviny došlo k obrovskému nárůstu využití videokonferenčních služeb. Na tuto

situaci NÚKIB spolu s dalšími institucemi zareagoval a vypracoval komplexní Bezpečnostní standard pro videokonference, který je pro jakoukoliv organizaci dobrovolně aplikovatelný.

Protože situace kolem pandemie vedla dále také ke zvýšení aktivity útočníků a obecně přinesla nárůst hrozeb v oblasti kybernetické bezpečnosti, vydal NÚKIB spolu s dalšími institucemi Minimální bezpečnostní standard, který nabízí zjednodušené principy, postupy a doporučení v oblasti kybernetické bezpečnosti pro organizace, které nespadají pod regulaci zákona o kybernetické bezpečnosti.

Z dalších podpůrných materiálů je vhodné uvést také komplexního průvodce identifikací významných informačních systémů, který je určen všem orgánům veřejné moci v souvislosti s novelizací vyhlášky o významných informačních systémech. Celkové revize se dočkal také podpůrný materiál popisující zákonný institut provozovatele informačního nebo komunikačního systému a materiály zohledňující zadávání veřejných zakázek se vztahem ke kybernetické bezpečnosti.

3 Sekce informační bezpečnosti

Bezpečnost informačních a komunikačních systémů a kryptografická ochrana

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

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

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

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

Certifikační a akreditační činnost

Nezbytnou zákonnou podmínkou pro používání informačních systémů, kryptografických prostředků, stínicích komor a zákonem stanovených kryptografických pracovišť při ochraně utajovaných informací je jejich certifikace.

Certifikace a akreditace informačních systémů

V roce 2020 probíhalo řízení o certifikaci 157 informačních systémů. K 52 žádostem o certifikaci informačního systému, jejichž zpracování bylo zahájeno v přechozím roce (2019), přibylo v roce 2020 dalších 105 žádostí, a to 39 ze státní správy nebo samosprávy a 66 ze soukromé sféry. Ve většině případů se jednalo o žádosti o opakovanou certifikaci již provozovaných informačních systémů. Ve 21 případu byla podána žádost o certifikaci nově budovaného informačního systému, přičemž pouze 1 z těchto žádostí pochází ze státní správy.

V uvedeném roce bylo vydáno celkem 107 certifikátů informačních systémů, z toho 43 pro žadatele ze státní správy nebo samosprávy a 64 ze soukromé sféry.

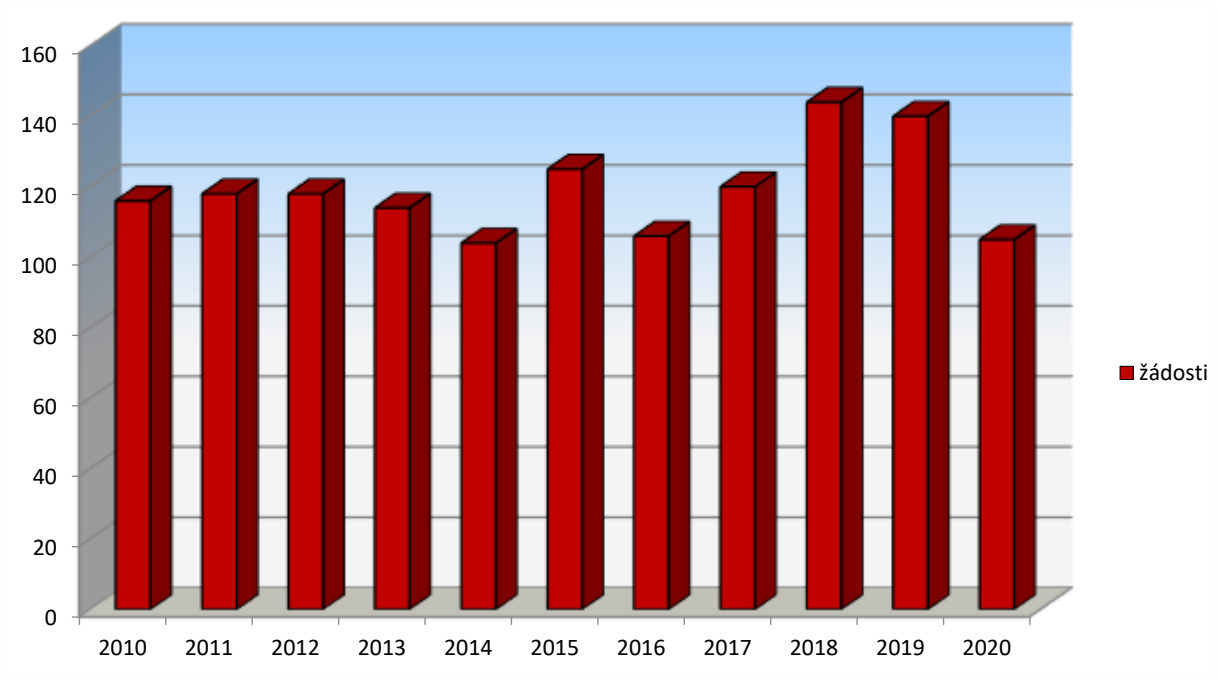
Celkem 56 certifikátů informačních systémů bylo vydáno na žádost podanou v roce 2020.

V 8 případech provozovatel informačního systému s certifikátem platným do data spadajícího do roku 2020 nepožádal o opakovanou certifikaci a platnost certifikátu automaticky skončila.

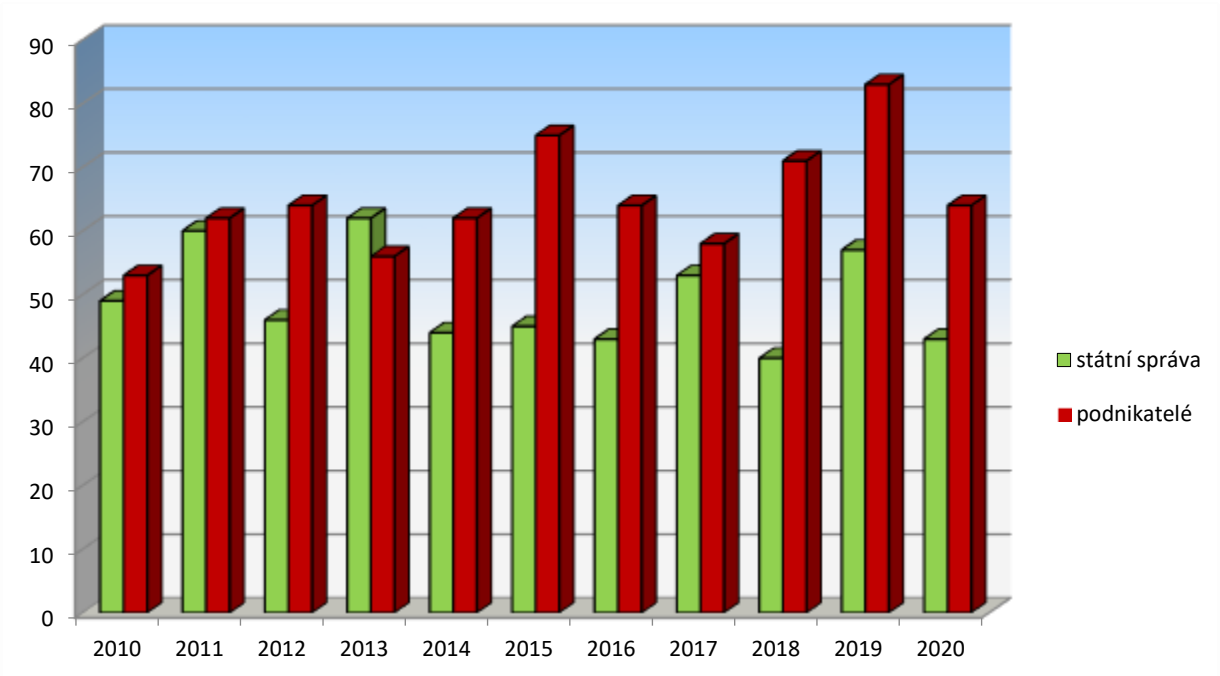
Certifikace informačních systémů v roce 2020

Řešené žádosti v roce 2020	Vydané certifikáty podle stupně utajení				Vydané certifikáty	
	Vyhrazené	Důvěrné	Tajné	Přísně tajné	státní správa	podnikatelé
159	22,4 %	49,5 %	26,2 %	1,9 %	43	64

Přijaté žádosti o certifikaci informačního systému v letech 2010 až 2020



Vydané certifikáty informačních systémů v letech 2010 až 2020



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

Lze konstatovat, že v roce 2020 přibyla 1 žádost o certifikaci nově budovaného informačního systému ze státní správy a 20 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 2020, kromě certifikace menších informačních systémů podnikatelů, několika ministerstev a úřadů (Ministerstvo práce a sociálních věcí, Ministerstvo průmyslu a obchodu, Ministerstvo financí, Ministerstvo spravedlnosti, Ministerstvo kultury, Ústavní soud, Kancelář poslanecké sněmovny, Generální ředitelství cel, Nejvyšší kontrolní úřad, několik krajských a městských úřadů) proběhla opakovaná nebo nová certifikace řady rozsáhlých informačních systémů rezortu Ministerstva vnitra a Policie ČR, rezortu Ministerstva obrany včetně Vojenského zpravodajství, Ministerstva zahraničních věcí a Bezpečnostní informační služby.

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

V roce 2020 Úřad provedl pro rezorty Ministerstva obrany, Ministerstva vnitra, Ministerstva zahraničních věcí a Bezpečnostní informační služby národní akreditaci 7 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 2020 byla na území ČR zahájena akreditace 1 součinnostního systému a byla v tomto roce dokončena.

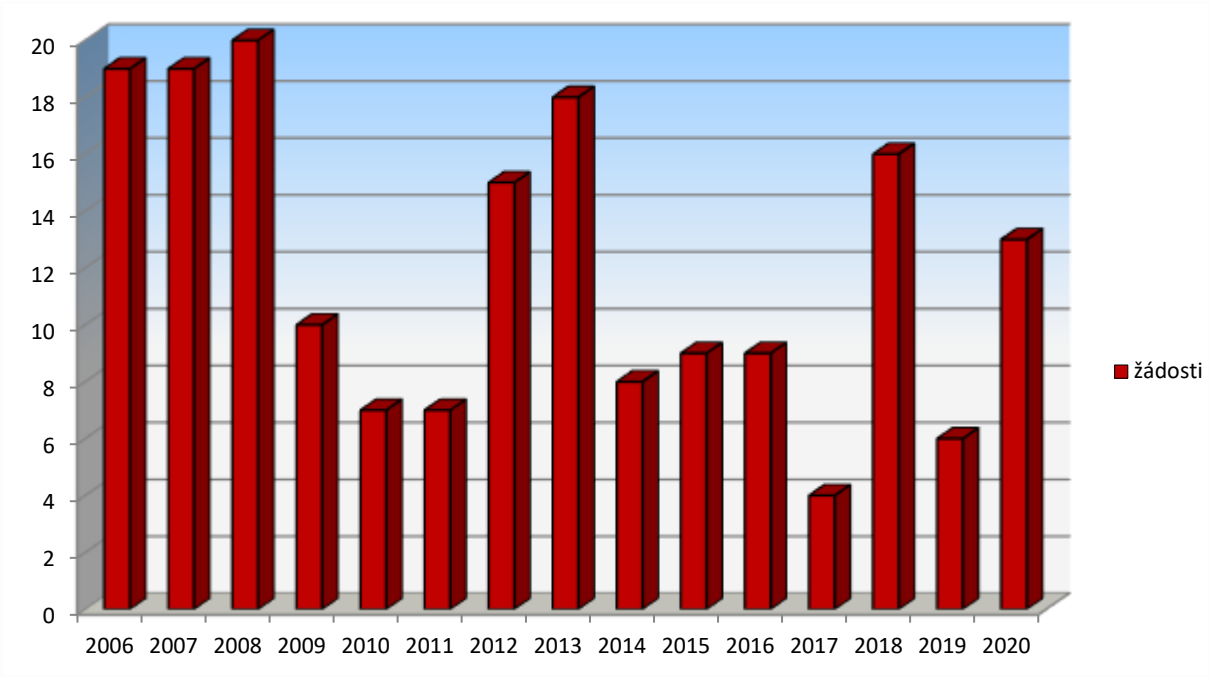
Certifikace kryptografických prostředků

V roce 2020 bylo Úřadu podáno celkem 13 žádostí o certifikaci kryptografického prostředku, z toho 8 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.

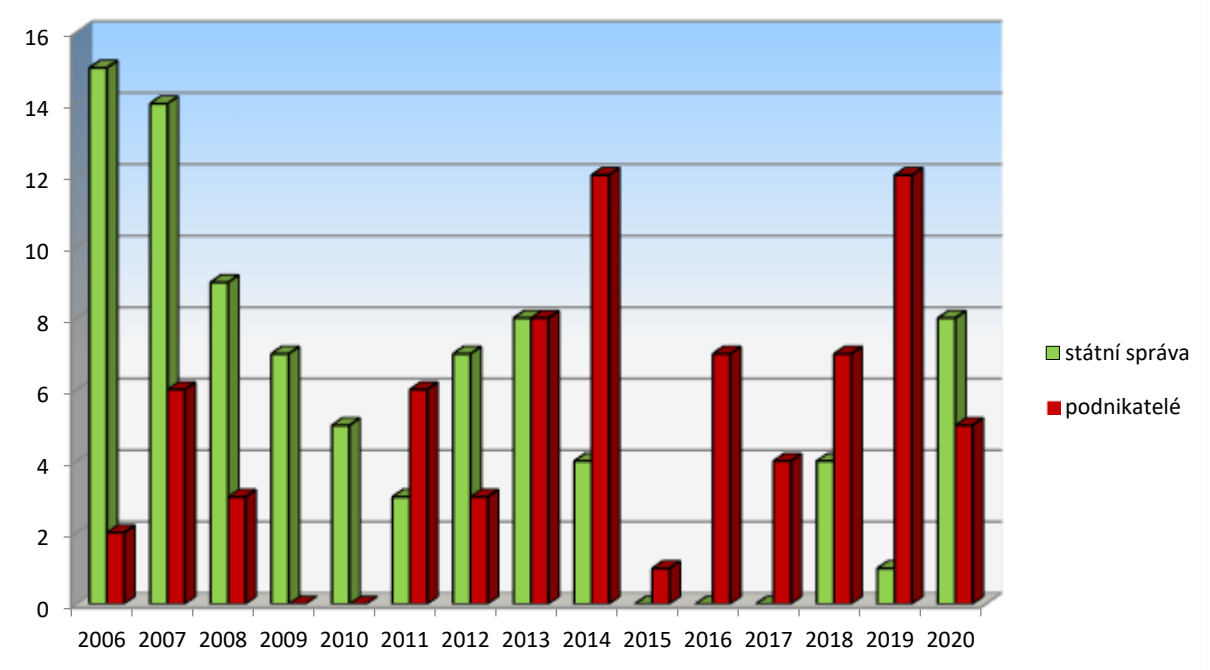
Certifikace kryptografických prostředků v roce 2020

Přijaté žádosti vč. opak.	Probíhající řízení		Ukončené bez vydání certifikátu		Vydané certifikáty		Pro NATO a EU	
	státní správa	podnikatelé	státní správa	podnikatelé	státní správa	podnikatelé	NATO	EU
13	0	4	0	0	8	5	13	6

Přijaté žádosti o certifikaci kryptografického prostředku v letech 2006 až 2020



Vydané certifikáty kryptografických prostředků v letech 2006 až 2020



Nově byly certifikovány kryptografické prostředky LANPCS-RG3, SINA Workstation H R RW11 27A a SINA WS H Client III 27A, radiostanice tříd HARRIS a THALES určené pro operační prostředí, 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, SINA a THALES) a schvalování projektů zástaveb kryptografických prostředků do mobilních a systémů, které lze rozmístit.

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

Spektrum kryptografických prostředků certifikovaných v ČR v zásadě pokrývá ochranu lokálního ukládání a přenosu utajovaných informací v informačních a komunikačních systémech, včetně ochrany utajované informace v hlasové formě. Početně významné zastoupení mají kryptografické prostředky pro ochranu utajovaných informací v prostředí IP sítí (prostředky tříd LANPCS a systému THALES a SINA) a hlasové komunikace (systém SECTRA).

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

Do seznamu Úřadu materiálu „kontrolovaná kryptografická položka“ byly nově zařazeny 2 kryptografické prostředky.

Schvalování projektů bezpečnosti komunikačních systémů

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

V roce 2020 nebyla podána žádná žádost o schválení projektu bezpečnosti nového komunikačního systému.

Nadále byl provozován komunikační systém v Bezpečnostní informační službě, 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 2020 nadále zajišťoval Úřad.

Od roku 2017 je v provozu komunikační systém RETIS, který pro mobilní komunikaci informací stupně utajení Vyhrazené využívá certifikovaný kryptografický prostředek SECTRA Tiger/R (nová generace KP SECTRA Panthon 3). Provoz tohoto systému nadále zajišťuje Úřad.

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

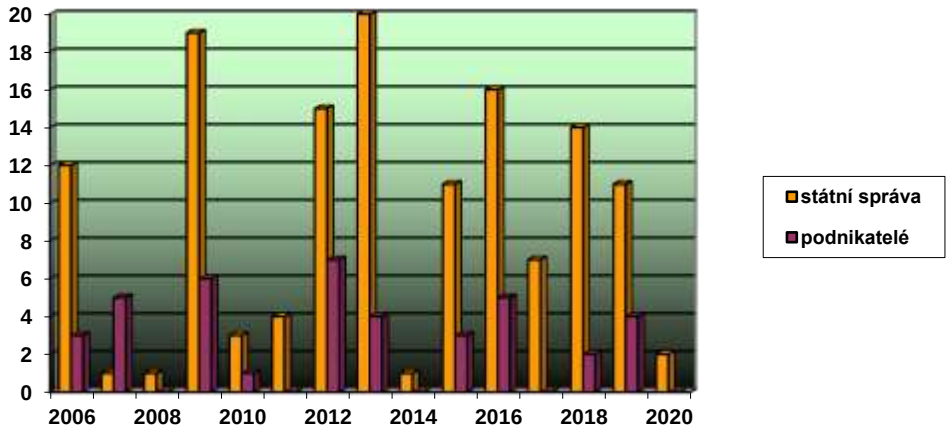
Certifikace kryptografických pracovišť

V roce 2020 byly podány celkem 2 žádosti o certifikaci kryptografického pracoviště. Obě žádosti o certifikaci spadají 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 Úřadem. Stav řízení je shrnut v následující tabulce.

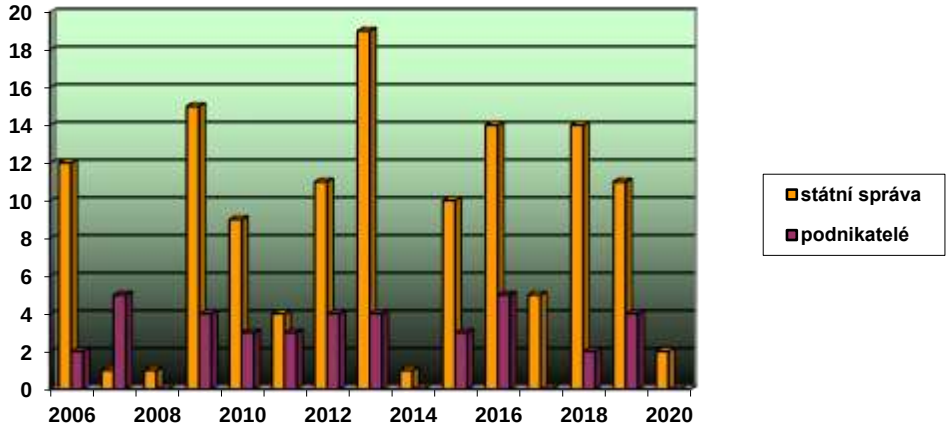
Certifikace kryptografických pracovišť v roce 2020

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

Přijaté žádosti o certifikaci kryptografického pracoviště v letech 2006 až 2020



Vydané certifikáty kryptografických pracovišť v letech 2006 až 2020



Další odborná činnost

Výroba kryptografického materiálu

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

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

V roce 2020 bylo v Úřadu vygenerováno celkem 62 346 kryptografických klíčů a hesel uložených na 4 862 nosičích různých typů a dalších 124 ks jiného kryptografického materiálu (procesory, paměti, kryptografická dokumentace, instalační a šifrovací SW).

Uzavření hranic, z důvodů epidemiologické situace v ČR, omezilo v roce 2020 dovoz nakoupeného kryptografického materiálu a také přepravu kryptografický prostředků na servis v zahraničí. Úřad vzal do evidence a provedl distribuci celkem 634 ks nového kryptografického a CCI materiálu a dále zajistil servis a opravy na území ČR u 125 ks kryptografických prostředků a mimo ČR u 11 ks kryptografických prostředků.

Úřad zajistil výrobu, vzal do evidence a provedl distribuci celkem 6 ks kryptografického materiálu EU.

Dále Úřad zajišťoval speciální balení a distribuci kryptografického materiálu, vedení ústřední evidence certifikovaných kryptografických prostředků dislokovaných u orgánů státu, jakož i centrální databáze všech pracovníků kryptografické ochrany, pracovníků provozních obsluh kryptografického prostředku a kurýrů kryptografického materiálu v působnosti Úřadu.

Měření kompromitujícího vyzařování (TEMPEST)

TEMPEST měření elektronických zařízení

Úřad prováděl v roce 2020 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 2020 provedeno více než 40 měření různých typů zařízení. Z toho bylo prováděno TEMPEST měření samostatných zařízení nebo v kombinaci s kryptografickým prostředkem PCS1. Tato měření byla prováděna podle metodiky standardu SDIP-27/2. Většina zařízení splňovala požadavky tohoto standardu.

Další TEMPEST měření byla prováděna v rámci certifikace nebo akreditace informačních systémů pro zpracování utajovaných informací stupně utajení Důvěrné nebo Tajné, buď pro orgány státu (např. Úřad vlády ČR, Ministerstvo zahraničních věcí, Ministerstvo obrany,

Ministerstvo vnitra, Ministerstvo průmyslu a obchodu, zpravodajské služby aj.), nebo pro podnikatele. Z celkového počtu hodnocených zařízení byla většina vyžádána Ministerstvem obrany.

Zónové měření, instalační záznamy, obranné prohlídky

Úřad dále prováděl ohodnocování prostorů metodou zónového měření. Jednalo se o prostory, ve kterých se nacházela zařízení zpracovávající utajované informace. Tento druh měření byl především použit u objektů Úřadu, Bezpečnostní informační služby, Ministerstva obrany a Ministerstva vnitra. Další zónová měření byla prováděna pro státní správu i pro soukromé subjekty v rámci certifikace informačních systémů. Prováděno bylo rovněž zónové hodnocení prostorů na základě podkladů dodaných akreditovanými pracovišti Ministerstva obrany, BIS a Vojenského zpravodajství.

Bylo provedeno hodnocení instalace informačních systémů zpracovávajících utajované informace stupně utajení Důvěrné a Tajné a v rámci certifikace těchto systémů byly zpracovány instalační záznamy z 22 lokalit.

V roce 2020 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 2020, je uveden v následující tabulce.

Měřená zařízení a objekty v roce 2020

Typ měření[6]	Počet
Zónové měření	2 objekty
Kryptografické prostředky	1 typ
Komponenty ICT	41 měření
Audiotechnika	2 typy zařízení
Obranné prohlídky i v rámci certifikace IS	15 objektů
Mobilní systémy	8 systémů
Instalační záznamy	22 lokalit

Školení pracovníků kryptografické ochrany a zkoušky odborné způsobilosti

Opatření vlády ČR v souvislosti s covid-19 značně omezili možnosti provádět zkoušky zvláštní odborné způsobilosti pro pracovníky kryptografické ochrany. Proto Úřad povolil, aby u pracovníků kryptografické ochrany, kterým platnost osvědčení o zvláštní odborné způsobilosti skončila, byla doba platnosti osvědčení na nezbytně nutnou dobu prodloužena.

Úřad v roce 2020 organizačně zajistil a provedl, v souladu se zákonem, celkem 3 školení skupin pracovníků kryptografické ochrany a po následující zkoušce odborné způsobilosti vydal 62 osvědčení o zvláštní odborné způsobilosti pracovníka kryptografické ochrany. Dále provedl zaškolení pracovníků provozní obsluhy kryptografického prostředku a vydal 2 potvrzení o odborném zaškolení pracovníka provozní obsluhy kryptografického prostředku. Školení, která jsou v neutajovaném režimu, proběhla korespondenční formou.

Kontroly ochrany utajovaných informací (státní dozor)

V roce 2020 provedl Úřad ve smyslu §143 odst. 6 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti 15 kontrol za oblast bezpečnosti informačních nebo komunikačních systémů, případně kryptografické ochrany. Z tohoto počtu byly 3 kontroly provedeny v rámci státní správy a 12 kontrol u podnikatelů.

[6] U zónového měření a obranných prohlídek se jedná o objekty; v rámci jednoho objektu bylo měřeno více místností nebo budov. U kryptografických prostředků se jednalo i o ověřovací měření. U PC sestav třídy 1 a 2 se jednalo i o měření v rámci výběrových řízení např. pro Ministerstvo obrany nebo Úřad. U instalačních záznamů se jedná o systémy, které mohou mít několik instalací v rámci ČR i mimo ČR.

Problémové oblasti bezpečnosti informačních a komunikačních systémů a kryptografické ochrany

Zákonem stanovené činnosti Úřadu v oblasti bezpečnosti informačních systémů nakládajících s utajovanými informacemi a kryptografické ochrany byly v roce 2020 zajištěny.

- Stálou výzvou je rychlý rozvoj informačních a komunikačních technologií (ICT) a s ním spjaté bezpečnostní problémy. Některé nové technologie nelze nasadit bez jejich důkladného testování anebo bez podkladů vzniklých jejich kvalifikovaným hodnocením z hlediska bezpečnosti podle uznávaných mezinárodních kritérií. Zároveň mají subjekty vedoucí útoky proti důvěrnosti, integritě a dostupnosti utajovaných nebo citlivých informací k dispozici stále sofistikovanější nástroje. Informace o skrytých zranitelnostech ICT produktů jsou obtížně dosažitelné a jejich objevení zpravidla vyžaduje vysoce nadstandardní technické vybavení.
- V oblasti certifikace informačních systémů, kryptografických prostředků a pracovišť jsou pracovní místa v Úřadu aktuálně přidělená pro tyto činnosti kvalitně obsazena, avšak celkově je tato oblast personálně poddimenzována a bude třeba ji průběžně posilovat.
- V oblasti kryptografické ochrany jsou v rámci ČR zajišťovány národní kryptografické prostředky certifikované pro ochranu utajované informace v různých komunikačních prostředích. Tato komunikační prostředí se však neustále mění (u mobilních komunikací zcela překotně). Vývoj národních kryptografických prostředků probíhá v podmínkách odborných pracovišť Úřadu a ve spolupráci se specializovanými subjekty ze soukromého sektoru v rámci externích vývojových projektů. Vzhledem k vysokým požadavkům na průmyslovou bezpečnost, vysokou odbornou náročnost a nedostatečné portfolio privátních odborných pracovišť v ČR se projevuje jistý nedostatek zájmu kvalifikovaného soukromého sektoru účastnit se externího vývoje, ačkoliv je externí vývoj do značné míry financován z rozpočtu Úřadu (tedy státu). Zájem privátních subjektů také negativně ovlivňuje malý národní trh kryptografických prostředků (počty kusů kryptografických prostředků uplatnitelných v ČR).
- Z hlediska zajištění praktické ochrany utajovaných informací v informačních nebo komunikačních systémech a zajištění kryptografické ochrany všeobecně ve státní správě

je potřebné také personální posílení pracoviště Úřadu, zajišťujícího výrobu, evidenci a distribuci kryptografického materiálu národního a EU v ČR. V rámci rezortů je třeba mít stále na zřeteli nedostatek odborníků v oboru informačních technologií a kryptografické ochrany, kteří by zároveň splňovali podmínky pro přístup fyzické osoby k utajované informaci stupně utajení Důvěrné, Tajné nebo Přísně tajné. Stabilizované obsazení pracovních míst potřebné zejména v případě pracovníků ve výkonu kryptografické ochrany. Rovněž je třeba usilovat o zajištění zastupitelnosti v klíčových rolích v bezpečnostní správě a správě certifikovaných informačních systémů.

Výzkumná a vývojová činnost Úřadu v oblasti ochrany utajovaných informací

Cíle a organizace výzkumu a vývoje

Základním cílem v oblasti výzkumu a vývoje byl neustálý rozvoj bezpečnostních technologií pro ochranu utajovaných informací v komunikačních a informačních systémech. V důsledku turbulentního rozvoje informačních technologií a nárůstu hrozeb kybernetických útoků se stále zvyšuje náročnost výzkumu a vývoje v oblasti bezpečnosti informačních technologií. S ohledem na kapacitní možnosti využívá Úřad pro řešení vývojových a výzkumných projektů osvědčený model – kromě vlastních odborných pracovišť zapojuje také externí subjekty a firmy specializované na vývoj bezpečnostních technologií případně jednotlivé externí odborníky.

Projekty realizované v roce 2020

V roce 2020 Úřad 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.

Úřad vývojové projekty realizoval na základě zjištěných poznatků při spolupráci s orgány státu, pilotním testování KP, 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 komunikačního i technologického prostředí a inovovat již vyvinuté produkty, případně vyvíjet nové prostředky.

V rámci odborného pracoviště OBIT-OKVKP byl v roce 2020 dokončen projekt střediska PCA, probíhaly vývojové projekty hlasových komunikátorů (iSacom, Sacom2, OSK) a výzkum technologií GNZ a biometrických senzorů. Uvedené projekty byly realizovány ve spolupráci s externími řešiteli. Návazně probíhal interní aplikovaný vývoj bezpečnostního SW a HW na odborném pracovišti Úřadu v předmětných oblastech a pilotní nasazení osobních KP a chráněné mobilní komunikace.

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

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

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

CIS3 C&I Partnership – SCIP + NINE Working Group Meeting, Work Package Board Meeting Partnership Committee Meeting

Setkání v rámci unikátního Partnerství států NATO, výborů a pracovních skupin SCIP a NINE. Účelem Partnerství je mezinárodní spolupráce při standardizaci chráněné hlasové a datové komunikace, vzájemné předávání informací o aktuálním stavu implementace protokolů SCIP a NINE i o jejich vývoji. Uskutečnilo se jedno prezenční zasedání a ostatní jednání byla realizována virtuálně kvůli COVID pandemii.

Security and Policing 2020

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).

EUROCRYPT 2020 (virtuálně)

Každoroční konference k získání aktuálních poznatků v kryptologii.

ICMC 2020 (virtuálně)

ICMC je významnou odbornou akcí zaměřenou na řešení aktuálních problémů vývoje, testování a provozování kryptografických modulů s důrazem na aplikaci příslušných standardů. Letos se z velké části věnovala tématu přechodu ze standardu FIPS 140-2 na FIPS 140-3.

PQCrypto 2020 (virtuálně)

Každoroční konference PQCrypto slouží k výměně informací o současných novinkách na poli kvantově odolné kryptografie.

Bar Ilan Winterschool 2020 (prezenčně)

Zimní škola informačně-teoretické kryptografie. Konala se v únoru 2020 v Tel Avivu, Izraeli.

PKC 2020 (virtuálně)

Každoroční konference na téma asymetrické kryptografie. V tomto ročníku se především věnovala tématům post-kvantové kryptografie.

Kurz Common Criteria (BSI)

Týdenní kurz hodnocení dle systému Common Criteria organizovaný pro NÚKIB a NBÚ-Slovensko. Konal se v únoru v Praze.

Matematická kryptologie a kvantové technologie relevantní pro bezpečnost informací

Matematická kryptologie

Úřad zajišťuje vývoj a analýzy bezpečnosti národních kryptografických algoritmů určených pro ochranu utajovaných informací. V roce 2020 Úřad analyzoval bezpečnostní vlastnosti národního kryptografického pseudonáhodného generátoru DRaCon1.

V reakci na bouřlivý rozvoj a výsledky veřejně publikované kryptografie v posledních letech bylo v rámci Úřadu diskutováno a analyzováno vhodné zaměření vývoje národních utajovaných kryptografických algoritmů do budoucna. Neutajovaná část těchto diskusí proběhla se zapojením renomovaných odborníků z akademické obce.

Reakce na kvantovou hrozbu a kvantové technologie relevantní pro informační bezpečnost

Jako reakci na kvantovou hrozbu (budoucí luštění šifrované komunikace pomocí kvantových počítačů) Úřad připravuje zajištění odolnosti kryptografických prostředků používajících asymetrickou kryptografii proti kvantové hrozbě. V roce 2020 byla dokončena a úspěšně obhájena studie proveditelnosti jejich odolnosti proti kvantové hrozbě a na rok 2021 je plánován návazný realizační projekt.

Úřad koordinuje zapojení ČR do iniciativy Euro QCI, jejímž cílem je postupné vybudování evropské komunikační kvantové infrastruktury. V blízké budoucnosti na bázi kvantové distribuce klíčů a ve vzdálenější budoucnosti se předpokládá realizace kvantového internetu.

Úřad v roce 2020 spolupracoval s českým šerpou pro Euro QCI a s českou akademickou obcí na přípravě Národního plánu rozvoje QCI ČR a je zapojen do Security Group Euro QCI.

Odborný rozvoj a spolupráce s akademickou obcí

V r. 2020 pracovníci Úřadu zajišťující výše zmíněné činnosti studovali problematiku:

- dokazatelné bezpečnosti vybraných kryptografických schémat,
- bezpečnostních, implementačních a provozních vlastností vybraných algoritmů kvantově odolné kryptografie,
- bezpečnosti kryptografických protokolů souvisejících s využitím kvantově odolné kryptografie,
- SW nástrojů pro hodnocení kryptografické bezpečnosti,
- bezpečnostních vlastností kvantové distribuce klíčů.

Dále spolupracovali s akademickou obcí formou diskuse výše zmíněných problematik (současný stav kvantové distribuce klíčů, Národní plán rozvoje QCI v ČR a další směřování vývoje národních kryptografických algoritmů). V r. 2020 zajišťovali výuku předmětu: Aplikovaná kryptografie 1 na MFF UK.

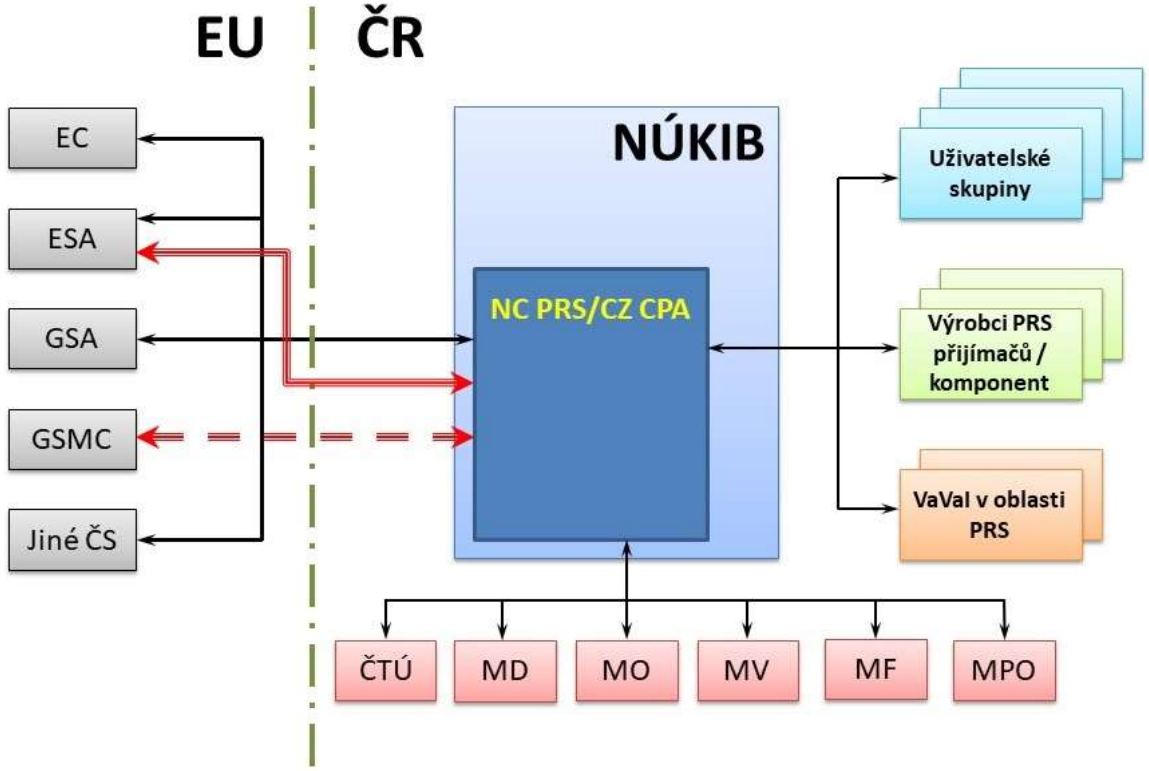
Výkon funkce příslušného orgánu PRS

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

Budování národního centra PRS

Implementace služby PRS v ČR probíhá na základě schváleného Akčního plánu implementace PRS v ČR. V souladu se schváleným finančním rámcem a personálními opatřeními Úřad pokračuje v budování Národního centra PRS (dále jen „NCPRS“), které je zodpovědné za organizační zabezpečení přístupu ke službě PRS a za výkon funkce CPA. Organizační schéma zabezpečení služby PRS v ČR je zobrazeno na následujícím obrázku.

Organizační schéma zabezpečení služby PRS v ČR



Jednou z hlavních činností, kterou vykonává NCPRS, je zastupování Úřadu, resp. ČR v pracovních skupinách EU pro řešení problematiky bezpečnosti programu Galileo a PRS. Účast pracovníků NCPRS na těchto jednáních pokračovala i v roce 2020. Vzhledem k nepříznivé epidemiologické situaci v EU v souvislosti s covid-19 se většina jednání uskutečnila on-line formou. V roce 2020 byl pro potřeby NCPRS akreditován a následně uveden do provozu komunikační systém umožňující výměnu utajovaných informací a v omezeném formátu i projednávání utajovaných informací agendy bezpečnostní akreditace a PRS.

Dalším důležitým úkolem NCPRS byla koordinace aktivit spojených s přístupem k informacím a technologiím PRS. NCPRS poskytovalo zájemcům informace o PRS autorizaci vydávané Radou pro bezpečnostní akreditaci Agentury pro evropský GNSS a zajišťovalo,

aby subjektům se sídlem v ČR, které se chtěly podílet na výrobě nebo vývoji přijímačů PRS, bezpečnostních modulů či technologií s integrovanou službou PRS, a které splňovaly požadavky fyzické a administrativní bezpečnosti a další stanovené podmínky, byla udělena bezpečnostní akreditace.

V roce 2020 dále pokračovala mezinárodní spolupráce pro přípravu testování služby PRS v rámci projektu společného testování „Joint Test Activities“, vyhlášeného Agenturou pro evropský GNSS. Časový harmonogram pro uskutečnění projektu byl prodloužen a koncem roku 2020 byly dodány PRS přijímače koordinátorovi konsorcia, kterého je ČR součástí. Podle dostupnosti přijímačů v ČR v závislosti na dohodě se zahraničními partnery bude realizace projektu uskutečněna pravděpodobně v roce 2021.

Zástupci NCPRS se rovněž zúčastnili testování nové GNSS „smart“ antény vyvinuté v rámci projektu oddělení TEMPEST NÚKIB v oblasti vědy, výzkumu a inovací s názvem „Vývoj antény pro signály GNSS Galileo a služby PRS odolné proti rušení“. Testování bylo realizováno ve spolupráci s Ministerstvem obrany ČR a jednoznačně prokázalo vyšší odolnost této nové antény proti rušení v porovnání se standardně využívanými GNSS anténami.

NCPRS se i v roce 2020 účastnilo pravidelného setkání CPA členských států EU, které vzhledem k epidemiologické situaci proběhlo pouze on-line formou a jehož hlavním cílem byla diskuze ohledně stavu a pokračování implementace PRS v členských státech EU, koordinace společného postupu při jednání s Evropskou komisí a vzájemná 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

Na plnění úkolů agendy PRS a aktivit NCPRS se podíleli čtyři zaměstnanci Úřadu. I vzhledem k očekávanému nárůstu agendy spojenému s transformací a rozšířením Agentury pro evropský GNSS na Agenturu Evropské unie pro kosmický program a blížícím se předsednictvím ČR v Radě EU bude nutné počet pracovníků zabývajících se touto agendou dále rozšiřovat.

Spolupráce s ostatními subjekty při implementaci PRS

Při řešení problematiky PRS NCPRS úzce spolupracuje zejména s Ministerstvem dopravy ČR coby národním koordinátorem pro správu a řízení evropských systémů družicové navigace. V roce 2020 nadále pokračovala spolupráce s Ministerstvem obrany ČR, zejména v oblasti zapojení do projektu společného testování PRS a také z důvodu potenciálního využití PRS Armádou ČR.

Odbor vzdělávání, výzkumu a projektů

Přínos Projektové kanceláře NÚKIB pro zajištění kybernetické bezpečnosti

Přínosu pro zajištění kybernetické bezpečnosti dosahuje NÚKIB pomocí projektového řízení, které uplatňuje zpravidla u komplexních a složitých záměrů se strategickým dopadem, obsažených nejenom v Akčním plánu k Národní strategii kybernetické bezpečnosti ČR 2015–2020. Projektová kancelář NÚKIB dále nově aplikuje nástroje portfolio managementu, podílí se dlouhodobě na metodické podpoře projektového řízení i jednotlivých projektů, podpoře financování relevantních projektů a na osvětě a vzdělávání v oblasti projektového řízení v úzkém vztahu s kybernetickou bezpečností.

Přímé řízení projektů

Projektová kancelář řídila v roce 2020 projekty namířené dovnitř Úřadu i mimo něj, případně se na jejich řízení podílela. Jde o tyto projekty:

- Neveřejný web – pokračování v koordinaci projektu, zajištění potřebné významné změny způsobu realizace projektu a následného předání k realizaci i projektovému řízení do rukou Vládního CERTu.
- Národní scrubbing centrum-Realizace projektu byla na základě analýzy změněné situace a nových variant vedením NÚKIB zastavena, aktuálně je projekt korektně ukončován. Byly dokončeny dílčí výstupy využitelné do budoucna a stanoveny požadavky na vytvoření projektem zamýšlených funkcionalit v rámci potenciálního širšího projektu. Další kroky na uvedeném projektu jsou připravovány se zapojením Projektové kanceláře.

- Databáze kontaktních údajů a ticketovacího systému – převzetí řízení projektu s významným dopadem na zajištění kybernetické bezpečnosti. Došlo k úspěšnému zajištění předpokladů pro budoucí realizační fázi formou dodávky v r. 2021.
- Mimo zmíněné projekty dochází k realizaci a přípravě dalších, zejména infrastrukturních projektů a projektů na zvýšení efektivity, které mají nepřímý pozitivní vliv na zajištění kybernetické bezpečnosti organizace s relevancí na celou ČR. Stejně tak dochází k asistenci s udržitelností a k vyhledávání a podpoře vhodných příležitostí a spolupráce.

Portfolio management a strategická koordinace

- Projektová kancelář připravila k využití nové nástroje portfolio managementu, které mají organizaci umožnit racionalizovat řízení projektů a programů ve vzájemných souvislostech a tím i pozitivně ovlivnit zajištění kybernetické bezpečnosti skrze řízení strategických projektů v kontextu potřeb a možností portfolia organizace.
- Na žádost MV ČR se Projektová kancelář a další relevantní útvary NÚKIB zapojily do systému hodnocení projektů v oblasti kyberbezpečnosti z programu Digitálního Česka (pouze na strategické úrovni, souvisí se spolufinancováním z fondů EU). Uvedená hodnocení budou probíhat v roce 2021.

Podpora financování kyberbezpečnostních projektů

- Zejména ze strany Projektové kanceláře proběhla řada jednání s MMR, Řídícím orgánem IROP, Centrem pro regionální rozvoj, MV ČR a dalšími orgány k nastavení programů a výzev v novém programovém období 2021-2027. Během července a srpna byly předloženy

  a zohledněny požadavky NÚKIB na podobu a alokaci výzvy kybernetická bezpečnost v IROP II.
- Na základě priorit ředitele NÚKIB bylo a je průběžně podporováno rozšíření spolufinancování v oblasti zdravotnictví. V září 2020 byl např. zaslán dopis na ŘO IROP s žádostí o rozšíření místní způsobilosti budoucí výzvy kybernetická bezpečnosti v IROP o území hlavního města Prahy tak, aby nemocnice na území Prahy byly způsobilým

příjemcem. Bohužel bylo obdrženo negativní stanovisko s odůvodněním, že tento typ projektů nesplňuje podmínku celoplošné působnosti.

- Pro zvýšení pravděpodobnosti úspěšného plánování a realizace spolufinancovaných projektů s dopadem na kyberbezpečnost z EU byly v r. 2020 vytvořeny interní pomůcky: „Odpovědnosti finančního řízení, spolufinancování“ „Možnosti financování – projekty“ – pro přehledné zhodnocení aktuálních příležitostí financování projektů mimo rozpočet NÚKIB, resp. s podílem mimo rozpočet NÚKIB.

Osvěta a vzdělávání v projektovém řízení

- Ve spolupráci s profesním sdružením projektových manažerů PMI.cz proběhla komunitní osvětová akce za hranice NÚKIB na téma „Kybernetická bezpečnost v životě projektového manažera“ s cílem předání zkušeností, informací a pomůcek, a tím i zvýšení dosahu témat kybernetické bezpečnosti. A to do této důležité, specifické skupiny projektových manažerů a podobných pracovníků, ovlivňujících přímo či nepřímo zajištění stavu kybernetické bezpečnosti v ČR.

Výzkum a evropská spolupráce

V roce 2020 byl Radou pro kybernetickou bezpečnost schválen Národní plán výzkumu a vývoje v kybernetické a informační bezpečnosti. Cílem Národního plánu je identifikovat prioritní výzkumná témata v oblasti kybernetické a informační bezpečnosti a dále definovat nástroje, které přispějí ke koordinaci výzkumných aktivit, spolupráci se soukromým a akademickým sektorem na vývoji a implementaci technologií v praxi.

NÚKIB podpořil několik projektů výzkumu a vývoje na národní i mezinárodní úrovni. V roli aplikačního garanta se zapojil do řešení dvou výzkumných projektů financovaných z programu „Strategická podpora rozvoje bezpečnostního výzkumu ČR 2019–2025“ Ministerstva vnitra České republiky. Prvním z nich je projekt zabývající se analýzou bezpečnostních rizik optických vláknových sítí. Druhý projekt je zaměřen na strategický výzkum a vývoj systémů pro zabezpečení moderních komunikačních sítí s využitím kvantového ustanovení klíčů a postkvantové kryptografie.

NÚKIB dále podpořil formou dopisu zájmu (Letter of intent) několik projektů v rámci národních programů podpory výzkumu a vývoje (programy Technologické agentury ČR, Ministerstva vnitra ČR, Ministerstva průmyslu a obchodu). Podobně tomu bylo i v případě vyjádření podpory mezinárodním konsorciím v rámci programů Horizont 2020 a Connecting Europe Facility (CEF). NÚKIB také podpořil připojení ČR k celoevropskému projektu EuroQCI, jehož cílem je vybudování celoevropské kvantové komunikační infrastruktury.

V oblasti společně prováděného výzkumu a vývoje v kybernetické bezpečnosti na úrovni EU se NÚKIB podílel na připomínkování nových evropských rámcových programů Horizont Evropa a Digitální Evropa. NÚKIB tak učinil prostřednictvím veřejných konzultací Evropské komise a dále také prostřednictvím poradní skupiny MPO k programu Digitální Evropa a Expertní skupiny pro mezinárodní spolupráci v oblasti bezpečnostního výzkumu MV ČR.

NÚKIB podnikl potřebné kroky pro zajištění implementace Aktu o kybernetické bezpečnosti[7] do českého právního řádu v oblasti EU certifikací kybernetické bezpečnosti. Smyslem certifikace kybernetické bezpečnosti je zvyšování důvěry v produkty, služby a procesy v oblasti informačních a komunikačních technologií skrze jejich bezpečnost. NÚKIB v tomto systému zastává klíčovou roli vnitrostátního orgánu certifikace kybernetické bezpečnosti, jehož úkolem bude mj. dohlížet na dodržování pravidel zahrnutých v evropských systémech certifikace kybernetické bezpečnosti a tato pravidla vymáhat.

V souvislosti s implementací Aktu o kybernetické bezpečnosti NÚKIB začal organizovat pravidelné setkání pro partnery s cílem informovat o evropském rámci pro certifikaci kybernetické bezpečnosti.

Vzdělávání a osvěta v kybernetické bezpečnosti

V roce 2020 se NÚKIB primárně zaměřoval na vzdělávání zaměstnanců veřejné správy a dále na další cílové skupiny, včetně pracovníků prevence a žáků základních škol prostřednictvím e-learningových kurzů. Za tímto účelem NÚKIB zrealizoval veřejnou zakázku

[7] https://eur-lex.europa.eu/eli/reg/2019/881/oj

na dodávku on-line vzdělávacího portálu na platformě Moodle s cílem umožnit tvorbu, správu, distribuci a evidenci on-line kurzů NÚKIB pro zástupce veřejných institucí a dalších uživatelů.

Vzdělávání uživatelů z veřejné správy probíhalo skrze online kurz NÚKIB *„Dávej kyber!“*, který představuje základy kybernetické bezpečnosti a ke konci roku 2020 jej absolvovalo 18 200 zaměstnanců veřejné správy, ale i profesních sdružení a soukromých firem. V oblasti odborného vzdělávání s preventivním přesahem absolvovalo 1 690 pracovníků prevence odborný online kurz *„Bezpečně v kyber!“,* který je seznamuje s tématy online bezpečnosti.

V rámci osvětových a vzdělávacích aktivit se mj. podařilo pro žáky 4. – 5. tříd základních škol zrealizovat projekt online interaktivního komiksu Digitální stopa: Příběh „Svůďáka“, který se zaměřuje především na téma kybergroomingu, a kterým prošlo 650 žáků. NÚKIB také distribuoval naučné deskové hry pro mateřské školy Městečko Kybernetov, které dětem nenásilnou formou představují mj. problémy kyberšikany.

Během druhého ročníku Festivalu bezpečného internetu NÚKIB do škol skrze školní informační systémy Bakaláři a Škola Online distribuoval videa, hry nebo podcasty, které tak byly nabídnuty až 280 000 uživatelům přímo na jejich homepage. Zároveň na Festivalu realizoval online panelovou diskuzi Efektivita kyberprevence, jež na různých online platformách zhlédlo 4 500 diváků, kteří se v rámci programu seznámili například s trendy a efektivními formami osvěty kybernetické bezpečnosti.

Vedle hlavních vzdělávacích produktů NÚKIB také vydal řadu podpůrných materiálů. Jednalo se například o aktualizovanou verzi Bezpečnostního doporučení NÚKIB pro administrátory[8], Základní bezpečnostní opatření pro vrcholové vedení organizace[9], Doporučení týkající se bezpečného používání videokonferencí[10] či Doporučení pro rodiče ohledně rizikového chování dětí na internetu a hraní on-line her[11].

[8] https://www.nukib.cz/cs/infoservis/doporuceni/1511-doporuceni-nukib-pro-administratory-verze-4-0/
[9] https://www.nukib.cz/cs/infoservis/doporuceni/1630-zakladni-bezpecnostni-opatreni-pro-vrcholove-vedeni/
[10] https://www.nukib.cz/cs/infoservis/aktuality/1599-predstavujeme-bezpecnostni-standard-pro-videokonference/
[11] https://www.nukib.cz/cs/infoservis/doporuceni/1559-hrejte-bezpecne/

4 Odbor Kabinet ředitele

Legislativa a vládní agenda NÚKIB

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

V roce 2020 NÚKIB v souladu s Plánem legislativních prací vlády zpracoval a předložil Legislativní radě vlády a vládě návrh novely zákona o kybernetické bezpečnosti, jehož cílem je precizovat kompetenci NÚKIB a národního CERT k vyhledávání zranitelností a provést adaptaci nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“). V adaptačních ustanoveních má být stanoveno, že tzv. vnitrostátním orgánem certifikace předvídaným aktem o kybernetické bezpečnosti je NÚKIB, a také mají být stanoveny přestupky za nedodržení povinností stanovených aktem o kybernetické bezpečnosti.

V roce 2020 také probíhaly intenzivní legislativní práce na přípravě zákona upravujícího využívání služeb cloud computingu orgány veřejné moci, na kterých se NÚKIB podílel. V závěru roku NÚKIB zahájil legislativní práce na přípravě tří vyhlášek provádějících uvedenou zákonnou právní úpravu. Dále byl v tomto roce zdárně dokončen legislativní proces vyhlášky č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, ve znění pozdějších předpisů, která bude nabývat účinnosti postupně, v různém rozsahu k 1. lednu 2021, 1. lednu 2022 a 1. lednu 2023. V druhé polovině roku byla také promptně provedena novelizace

vyhlášky č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby, jako reakce na zvýšené ohrožení českých nemocnic kybernetickými bezpečnostními incidenty.

Vedle přijetí výše uvedených vlastních právních předpisů NÚKIB v roce 2020 posoudil v meziresortním připomínkovém řízení více než 120 materiálů legislativní i nelegislativní povahy, přičemž k řadě z nich uplatnil z hlediska své působnosti připomínky.

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

Zahraniční pracoviště

USA

Spolupráce v oblasti kybernetické bezpečnosti s USA se nesla zejména v duchu výměny informací, posuzování rizik důvěryhodných dodavatelů 5G a koordinaci společných bezpečnostních politik s partnery na federální úrovni.

Významným krokem v této agendě byl podpis Memoranda o bezpečnosti sítí 5. generace mezi předsedou vlády ČR Andrejem Babišem a ministrem zahraničních věcí Mikem Pompeem.

Izrael

Spolupráce mezi ČR a Izraelem v oblasti kybernetické se rozvíjí od roku 2013 a její rámec upravují Společná deklarace vlády ČR a vlády Izraele o spolupráci v oblasti kybernetické bezpečnosti (listopad 2014) a dále memorandum o porozumění mezi příslušnými bezpečnostními úřady o spolupráci v oblasti kybernetické bezpečnosti (květen 2016). Hlavním gestorem této spolupráce za ČR je Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB).

Za účelem posílení spolupráce NÚKIB vyslal v září 2020 do Izraele cyber attaché. Jeho hlavním úkolem je posilování spolupráce a výměna informací s partnerským úřadem a dále s akademickou i soukromou sférou.

Mezi NÚKIB a izraelským partnerským úřadem probíhá strukturovaný dialog na několika úrovních (technická, kybernetická cvičení, právní úprava kybernetické bezpečnosti a regulace) za účelem výměny zkušeností, postupů a best practices.

Na druhé pololetí roku 2021 je plánováno společné kybernetické cvičení obou úřadů, které se díky pandemii nemohlo uskutečnit v roce 2020.

ENISA

S agenturou EU pro kybernetickou bezpečnost ENISA spolupracuje Úřad v rámci aktivit s dopadem na činnost NÚKIB, vybran organizační celk získávají shrnutí relevantních dokumentů a studií a jsou informovány o přípravě legislativy (např. novelizace NIS) nebo o vzniku pracovních skupin. Do vybraných aktivit ENISA jsou zapojovány české instituce, jsou rozvíjeny možnosti spolupráce organizačních celků NÚKIB s jejich protějšky v této agentuře.

Brusel – EU/NATO

NÚKIB se v roce 2020 prostřednictvím svého cyber attaché v Bruselu podílel na práci (EU) Horizontální pracovní skupiny pro kybernetické otázky, Skupiny pro spolupráci směrnice NIS a Evropské skupiny pro certifikaci kybernetické bezpečnosti. Koncem ledna se tak např. NÚKIB attaché podílel na přípravě tzv. 5G EU Toolboxu, obsahující soubor opatření, která by měla vést ke snížení rizik implementace 5G sítí v EU.

V kontextu pandemie covid-19 NÚKIB v rámci EU sdílel své zkušenosti s kybernetickými útoky proti nemocnicím. V druhé polovině roku EU projednávala zejména závěry Rady ke kybernetické bezpečnosti zařízení připojených k internetu, které byly přijaty v listopadu. Závěrem roku 2020 byla nalezena politická shoda mezi spolu zákonodárci k Nařízení o zřízení evropského centra kompetencí pro kybernetickou bezpečnost, které počínaje 2021 bude přerozdělovat evropské finanční granty pro podporu kybernetické bezpečnosti. V polovině prosince byl zveřejněn tzv. „kybernetický balíček“, obsahující návrh revize směrnice NIS a novou Strategii kybernetické bezpečnosti EU pro digitální dekádu. Na rozpracování výše

uvedeného „balíčku“ se bude NÚKIB prostřednictvím svého attaché při EU podílet také v roce 2021.

V roce 2020 Severoatlantická rada odsoudila veškeré destabilizující a škodlivé kybernetické útoky namířené proti zdravotnímu sektoru, jejichž obětí se stala i ČR. Stejně tak NATO a spojenci nejen na základě tohoto vývoje učinili v roce 2020 mnoho kroků k zajištění lepšího řízení rizik a zajištění kybernetické bezpečnosti národní či alianční infrastruktury. Vzhledem k závazku ze summitu ve Varšavě nadále docházelo k posilování kybernetické obrany národních infrastruktur. Úspěšně proběhlo také cvičení Cyber Coalition, které se s ohledem na epidemiologickou situaci spojenou s opatřeními proti šíření nemoci covid-19 uskutečnilo v online režimu.

CCDCOE

Příprava dalšího ročníku největšího kybernetického cvičeni Locked Shields, které bude poprvé v hybridním módu.

Komunikace

V roce 2020 bylo v NÚKIB zřízeno specializované oddělení komunikace, jehož náplní práce je budování vztahů s veřejností prostřednictvím správy sociálních sítí a webových stránek. V rámci oddělení také působí tiskový mluvčí úřadu odpovědný za mediální komunikaci. V roce 2020 oddělení spravovalo účty na sociálních sítích Facebook, Twitter, LinkedIn a Instagram. Náplní práce oddělení byla rovněž interní komunikace a organizace interních akcí Úřadu.

Oddělení v roce 2020 kromě své denní agendy participovalo na organizaci konferencí CyberCon a Prague 5G security konference. Mimo to zrealizovalo kampaň Bezpečně doma, jejímž cílem bylo šíření osvěty o možnostech zabezpečení vybavení domácnosti z pohledu kybernetické bezpečnosti.

Jeho činností je rovněž koordinace strategické komunikace napříč státní správou v tématech souvisejících s činností Úřadu. Mimo to se podílí na organizaci cvičení kybernetické bezpečnosti jako odborný garant u témat týkajících se komunikace s veřejností a poskytuje

dalším subjektům poradenství, jak komunikovat s veřejností v případě krizových situací týkajících se kybernetické bezpečnosti.

5 Interní auditor

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 (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 2020 byl vydám interní normativní akt 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 řízených organizačních celcích. Taktéž byla namátkově provedena průběžná kontrola realizace následných kontrol v pololetí, a i z této kontroly byla předložena zpráva řediteli NÚKIB.

V lednu roku 2020 byla odeslána Ministerstvu financí Zpráva o výsledcích finančních kontrol na NÚKIB.

Začátkem roku byl vypracován Plán auditu pro rok 2020, 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, z auditů pokladny a cestovních náhrad vykonaných v roce 2019.

Začátkem roku 2020 byl dokončen interní audit cestovních náhrad zahájený koncem roku 2019. Cílem auditu byla kontrola 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.

V průběhu roku 2020 byl proveden kromě následného auditu veřejných zakázek, pokladny a spisové služby audit vnitřní komunikace a byly zahájeny audity GDPR a oběhu účetních dokladů. Na základě pověření ředitele NÚKIB byl proveden mimořádný audit bezpečnosti.

Interní audit vnitřní komunikace byl zaměřen na analýzu vnitřní komunikace na NÚKIB a její zhodnocení. Při auditu bylo využito dotazníkového šetření, které bylo po dobu jednoho měsíce prováděno na NÚKIB. Respondenty byli zaměstnanci NÚKIB.

Cílem interního auditu GDPR je kontrola ochrany osobních údajů dle platné legislativy a interních normativních aktů NÚKIB, prověření institutu pověřence pro ochranu osobních údajů.

Interní audit oběhu účetních dokladů se věnuje prověření dodržování interních normativních aktů týkajících se oběhu účetních dokladů a souvisejících právních předpisů. Taktéž je pozornost zaměřena na kontrolu postupu předávání účetních dokladů od jejich příjmu až po archivaci, vymezení oprávnění a odpovědnosti jednotlivých zaměstnanců NÚKIB za ověření věcné i formální správnosti.

Mimořádný audit bezpečnosti byl na NÚKIB vykonán ve spolupráci interního auditu s Odborem kontroly, Odborem bezpečnosti informačních a komunikačních technologií, Odborem bezpečnosti a Oddělením penetračního testování. Mimořádný audit bezpečnosti zahrnoval oblast kybernetické bezpečnosti v kontextu zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, penetrační testování, oblast ochrany utajovaných informací v kontextu zákona č. 412/2005 Sb., o ochraně utajovaných informací

a o bezpečnostní způsobilosti, ve znění pozdějších předpisů včetně dodržování příslušných vyhlášek, fyzickou a personální bezpečnost.

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

Koncem roku 2020 byl zpracován Plán interního auditu pro rok 2021 a Zpráva o kvalitě a účinnosti vnitřního kontrolního systému, které byly předloženy řediteli NÚKIB. Mimo auditní činnost byla náplní interní auditorky také průběžná konzultační a poradenská činnost, plánování, a dále připomínkování a spolupráce při tvorbě interních normativních aktů.

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)
IROP – Integrovaný regionální operační program

IROP II – Navazující Integrovaný regionální operační program pro aktuální období 2021-2027¨

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

REACT– Recovery Assistance for Cohesion and the Territories of Europe

ŘO – řídící orgán

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