NÚKIB

ZPRÁVA O ČINNOSTI 2021

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST

Praha 2022

Obsah

Úvod

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

Hlavní oblasti činnosti NÚKIB:

- provoz Vládního CERT České republiky (GovCERT.CZ),
- spolupráce s ostatními národními CERT® týmy a CSIRT týmy,
- spolupráce s mezinárodními CERT® týmy a CSIRT týmy,
- stanovení kritérií pro určení klíčových informačních systémů z hlediska České republiky a jejich autoritativní určování v konkrétních případech,
- stanovení bezpečnostních standardů pro informační systémy kritické informační infrastruktury (dále jen „KII“), provozovatele základních služeb (dále jen „PZS“) a významné informační systémy (dále jen „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

Jednou z působností NÚKIB je projednávání přestupků stanovených zákonem o kybernetické bezpečnosti a ukládání správních trestů za jejich spáchání. Do působnosti NÚKIB přitom spadá nejen projednávání přestupků podle § 25 a násl. zákona o kybernetické bezpečnosti, ale zároveň vybírání pokut, které NÚKIB v rozhodnutí o spáchání přestupku pachateli uloží.

V roce 2021 NÚKIB pravomocně rozhodl ve věci přestupku na úseku zákona o kybernetické bezpečnosti spáchaného Ministerstvem práce a sociálních věcí (MPSV), kterému za závažné porušení zákona o kybernetické bezpečnosti udělil pokutu ve výši 800 000 Kč. Proti rozhodnutí nebyl podán opravný prostředek a pokuta byla uhrazena.

NÚKIB rovněž projednává některé přestupky podle části osmé zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů (dále jen „**zákon o ochraně utajovaných informací**“). Jedná se o přestupky proti bezpečnosti utajovaných informací v informačních a komunikačních systémech a proti bezpečnosti utajovaných informací při kryptografické ochraně. I podle zákona o ochraně utajovaných informací platí, že NÚKIB pokuty nejen ukládá, ale tyto zároveň i vybírá.

V roce 2021 zahájil NÚKIB tři přestupková řízení pro podezření ze spáchání přestupku stanoveného zákonem o ochraně utajovaných informací, z nichž v jednom případě bylo v roce 2021 ve věci i pravomocně rozhodnuto. NÚKIB dále pravomocně rozhodl dva další případy z minulého období a celkově tak v oblasti ochrany utajovaných informací v informačních a komunikačních systémech uložil a vybral pokuty v souhrnné výši 43 000 Kč. Jednalo se o přestupky fyzických osob spočívající v nakládání s utajovanou informací v necertifikovaném informačním systému.

NÚKIB dále prošetřoval pět dalších podnětů, podle nichž mohlo dojít ke spáchání přestupků upravených zákonem o ochraně utajovaných informací. Ve třech případech NÚKIB věc z části odložil a z části předal orgánu příslušnému k projednání daného skutku. Ve dvou případech neshledal důvody pro zahájení řízení o přestupku.

Ekonomické zabezpečení NÚKIB

NÚKIB je od 1. srpna 2017 samostatnou kapitolou státního rozpočtu pod číslem 378.

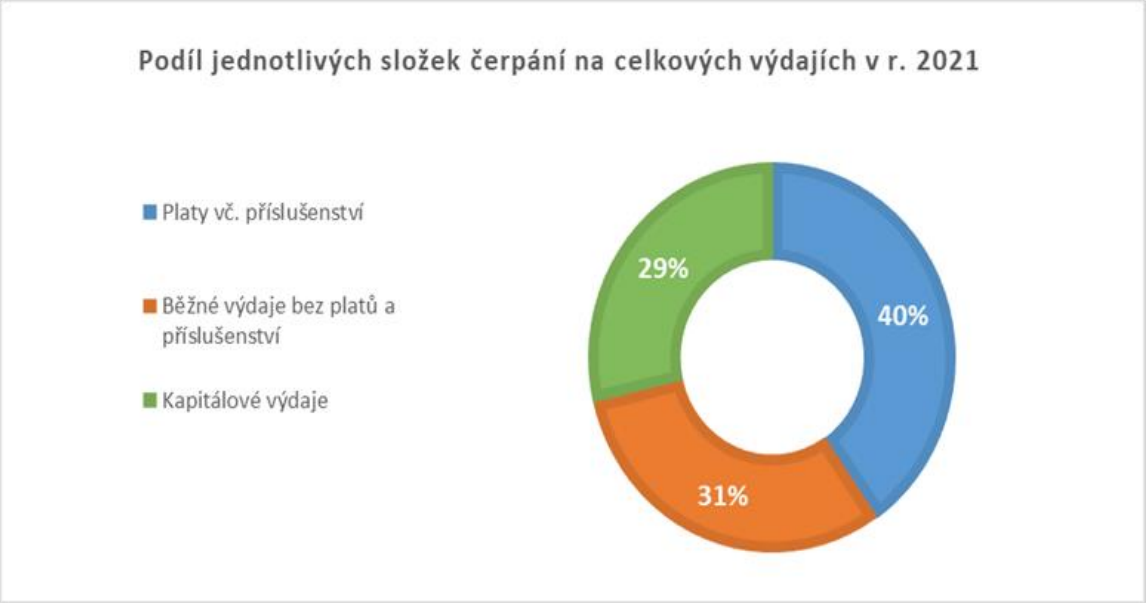
Rozpočet NÚKIB je tvořen příjmy a výdaji.

Celkové **příjmy** kapitoly za rok 2021 byly ve výši **1 042 990,54 Kč.** Tyto příjmy tvořily ostatní nedaňové příjmy, přičemž hlavní část představoval příjem pokuty ze správního řízení udělené MPSV ve výši 800 000 Kč. Dále se jednalo o sankce ve výši 43 000 Kč udělené několika fyzickým osobám. Významnou položkou byly také neplánované přijaté nekapitálové příspěvky a náhrady v objemu 173 626 Kč (vratky, dobropisy atd.).

Schválený **rozpočet celkových výdajů** NÚKIB byl v roce 2021 ve výši **427 932 108 Kč**.

Během roku 2021 byl schválený rozpočet upravován rozpočtovými opatřeními Ministerstva financí ČR (dále jen „MF“) na objem 433 662 332 Kč. Následně byl vázáním prostředků na platy a příslušenství za neobsazená pracovní místa v objemu 1 691 241 Kč snížen na 431 971 091 Kč. K 31. prosinci 2021 bylo z upraveného rozpočtu celkových výdajů vyčerpáno 406 582 295,52 Kč, tedy v relativním vyjádření 94,12 %. V průběhu roku 2021 bylo provedeno jedenáct rozpočtových opatření MF (v tom 4 rozpočtová opatření v rámci vázání prostředků státního rozpočtu za neobsazená pracovní místa).

Konečný rozpočet celkových výdajů kapitoly za rok 2021, tedy rozpočet včetně zapojených nároků z nespotřebovaných výdajů (dále jen „NNV“) ve výši 202 708 445,53 Kč, byl v objemu **634 679 536,53 Kč**. Čerpání konečného rozpočtu bylo v relativním vyjádření na **89,43 %**, v absolutním vyjádření ve výši **567 589 374,88 Kč**.



Výdaje na platy a příslušenství

Výdaje na platy, ostatní platby za provedenou práci a příslušenství byly rozpočtovány ve výši **231 106 275 Kč pro 269,5 pracovních míst**.

Vázáním prostředků na platy a příslušenství za neobsazená pracovní místa v objemu 1 691 241 Kč byl upravený rozpočet snížen na částku 229 415 034 Kč. Zapojením NNV byly upraveny výdaje na platy a příslušenství na konečný rozpočet ve výši **230 503 868,76 Kč**. Konečný rozpočet výdajů na platy, ostatní platby za provedenou práci a příslušenství byl čerpán ve výši **228 716 556,44 Kč**, tedy v relativním vyjádření na **99,22 %**.

V období od 1. ledna 2021 do 31. prosince 2021 nastoupilo na NÚKIB **60 nových zaměstnanců a 33 zaměstnanců ukončilo pracovní poměr**. Průměrný plat, k průměrnému ročnímu přepočtenému počtu 259,17 zaměstnanců, činil 53 942 Kč.

Běžné výdaje

Běžné výdaje (bez výdajů na platy, ostatní platby za provedenou práci a příslušenství) byly rozpočtovány ve výši 133 074 568 Kč.

Rozpočtovými opatřeními byly výdaje upraveny na 138 804 792 Kč. Zapojením nároků z nespotřebovaných výdajů byly upraveny na **konečný rozpočet ve výši 195 987 104,25 Kč**.

Konečný rozpočet běžných výdajů byl čerpán v objemu 175 992 320,22 Kč, v relativním vyjádření na 89,8 %.

Výdaje na opatření související s řešením epidemie COVID-19 činily objem 938 000 Kč. Jednalo se o výdaje na pořízení ochranných prostředků (mýdla, dezinfekce, antibakteriální gely, roušky, respirátory, ústenky), nákup antigenních testů pro zaměstnance, vynucené změny v informačních systémech NÚKIB a proplácení vybraných externích PCR testů zaměstnancům.

Kapitálové výdaje

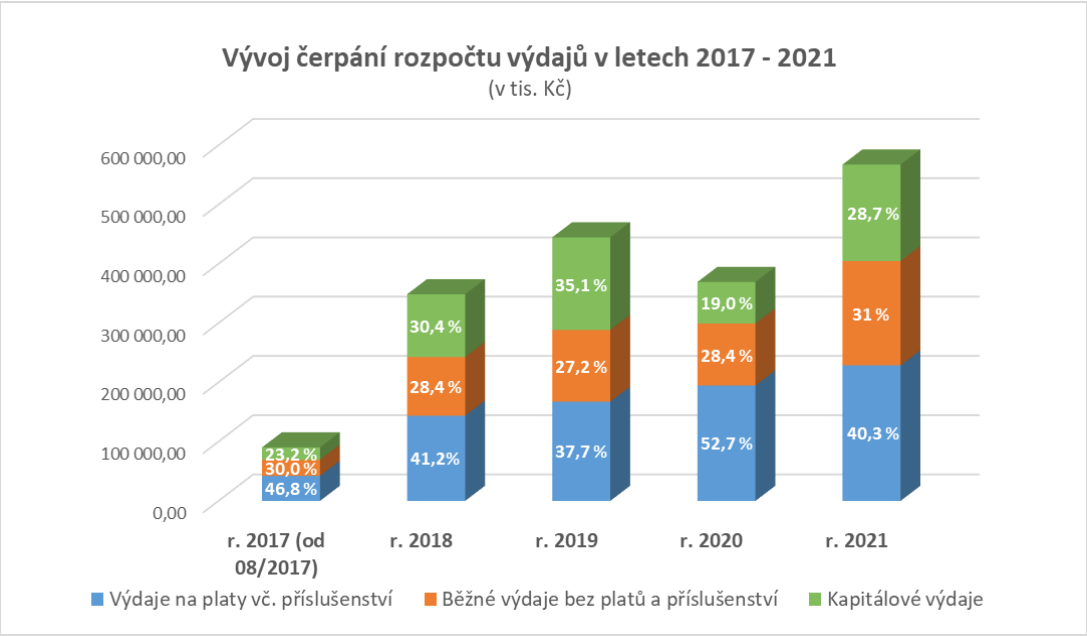
Kapitálové výdaje jsou evidovány v Informačním systému programového financování Správa majetku ve vlastnictví státu (dále jen „SMVS“) ve výdajovém titulu č. 37801 *„Rozvoj a obnova materiálně-technické základny Národního úřadu pro kybernetickou a informační bezpečnost“* pro období 2017-2022. V roce 2021 byl schválen nový program financování pro období 2021-2026 tj. výdajový titul č. 37802 *„Rozvoj a obnova materiálně-technické základny Národního úřadu pro kybernetickou a informační bezpečnost od r. 2021“*.

Kapitálové výdaje vedené v SMVS byly rozpočtovány v roce 2021 ve výši **63 751 265 Kč**.

Zapojením NNV pak byly kapitálové výdaje v roce 2021 upraveny na konečný rozpočet výdajů v SMVS v objemu 208 188 563,52 Kč. Z této částky bylo 40 000 000 Kč zapojeno z neprofilujících běžných NNV na profilující investiční NNV na základě usnesení vlády ze dne 17. května 2021 č. 461 za účelem financování rekonstrukcí, stavebních úprav a technického zhodnocení objektů NÚKIB.

Konečný rozpočet kapitálových výdajů byl čerpán v objemu **162 880 498,227 Kč, v relativním vyjádření 78,24 %.**

Nejvýznamnější objem finančních prostředků byl vynaložen na stavební úpravy a rekonstrukce objektů NÚKIB, a to téměř 90 000 000 Kč. Dále bylo vynaloženo téměř 58 000 000 Kč na dobudování, posílení a obnovu informačních a komunikačních technologii (dále jen „ICT“) infrastruktury NÚKIB a téměř 12 000 000 Kč na projekty v rámci výzkumu a vývoje, tj. kryptografické techniky, měřící techniky nebo nehmotných výsledků.



Evidence nároků z nespotřebovaných výdajů (dále „NNV“)

Počáteční stav nároků z nespotřebovaných výdajů k 1. lednu 2021 byl ve výši **202 912 132,68 Kč**. K 21. květnu 2021 došlo na základě usnesení vlády č.461 ze dne 17. května 2021 ke změně neprofilujících výdajů ve výši 40 000 000 Kč na výdaje profilující. Změna byla provedena za účelem posílení rozpočtu kapitálových výdajů NÚKIB, konkrétně na částečné financování rekonstrukce objektů Gorkého a Cejl v Brně a Paťanka v Praze. Dále došlo k 22. červnu 2021 ke snížení neprofilujících výdajů o částku 203 687,15 Kč z důvodu krytí nenaplněných příjmů rozpočtu NÚKIB za rok 2020. Nároky z nespotřebovaných výdajů se tak snížily na celkovou částku **202 708 445,53 Kč**, a to ve struktuře 149 187 992,62 Kč profilujících výdajů a 53 520 452,91 Kč neprofilujících výdajů.

Celkem za rok 2021 byly vyčerpány z NNV finanční prostředky v objemu **161 007 079,36 Kč**.

K 31. prosinci 2021 činí zůstatek nároků z nespotřebovaných výdajů částku **41 701 366,17 Kč**. Všechny nečerpané nároky z nespotřebovaných výdajů využije NÚKIB v roce 2022, a to včetně účelově určených finančních prostředků z roku 2021 na zapojení občanů České republiky (dále jen „ČR“), do civilních misí Evropské unie (dále jen „EU“) a dalších mezinárodních vládních organizací, účelově určených finančních prostředků z roku 2018 a 2019 na dobudování

pracoviště PRS a účelově určených finančních prostředků z roku 2018 na III. etapu oprav a vybavení objektu Cejl Brno.

Vnitřní finanční kontroly a interní audit

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

V průběhu roku 2021 byl zajišťován výkon řídící kontroly jednotlivými příkazci operací, hlavní účetní a správcem rozpočtu. V rámci své působnosti prováděly jmenované osoby finanční řídící kontroly při hospodaření s finančními prostředky na příslušných rozpočtových položkách NÚKIB v rámci jeho rozpočtové skladby. Mimo výkon řídící kontroly probíhala kontrolní činnost vedoucích zaměstnanců jednotlivých organizačních celků NÚKIB zaměřená na vyhodnocování již vyúčtovaných operací v jejich kompetenci z pohledu dosažení plánovaných cílů.

Uskutečněné řídící kontroly byly provedeny u finančních, statistických, účetních a jiných výkazů a operací v souladu a rozsahu stanoveném § 25 až § 27 zákona č. 320/2001 Sb., o finanční kontrole, ve znění pozdějších předpisů a vyhlášky č. 416/2004 Sb., kterou se zákon o finanční kontrole provádí. Výsledky finančních kontrol ukazují, že nastavený vnitřní kontrolní systém NÚKIB je plně funkční a zajišťuje jeho účinné a kvalitní řízení. Napomáhá včas odhalovat případné nedostatky a přijímat nápravná opatření.

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

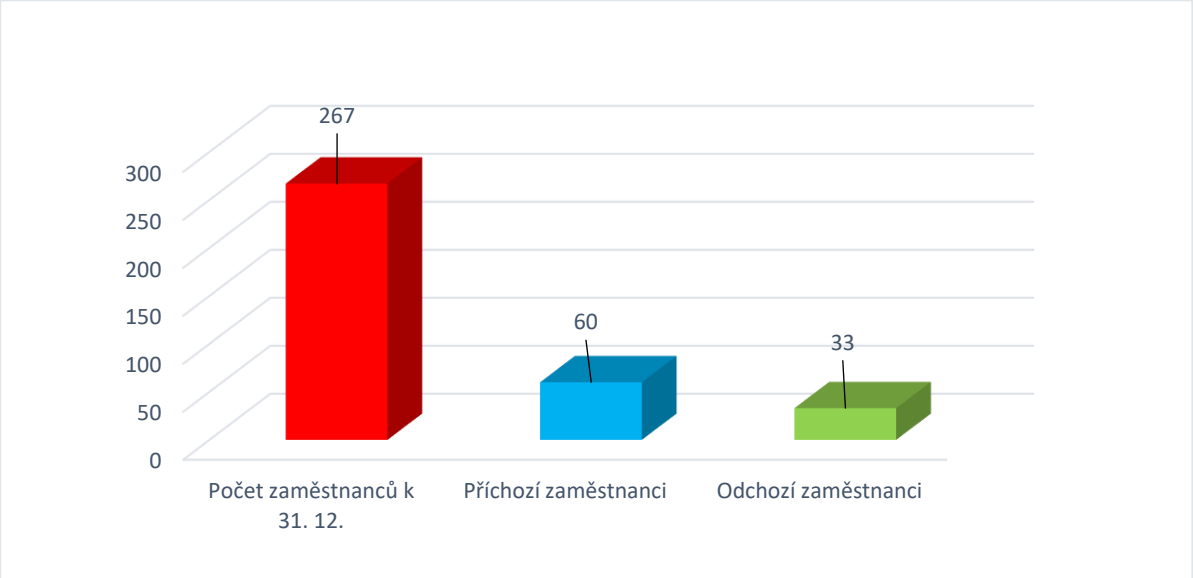
Personální zabezpečení NÚKIB

V souladu s Koncepcí rozvoje NÚKIB, kterou v roce 2020 schválila vláda, došlo od 1. ledna 2021 k navýšení počtu pracovních míst NÚKIB o 28. V polovině roku 2021 pak NÚKIB obdržel jedno pracovní místo na zajištění úkolů spojených s předsednictvím České republiky v Radě Evropské

unie. Všechna uvedená pracovní místa byla postupně obsazována novými zaměstnanci. Do pracovního poměru bylo v období od 1. ledna 2021 do 31. prosince 2021 **přijato 60 nových zaměstnanců.** Dalších 6 zaměstnanců vykonávalo činnost na základě uzavřených dohod o pracovní činnosti a se 16 osobami byla uzavřena dohoda o provedení práce.

Do konce roku 2021 **ukončilo** pracovní poměr **33 zaměstnanců**, tj. 12,58 % z počtu zaměstnanců evidovaných na systemizovaných pracovních místech. Z tohoto počtu **1** zaměstnanec ukončil pracovní poměr ve zkušební době, s **1** zaměstnancem ukončil ve zkušební době pracovní poměr zaměstnavatel, **8** zaměstnanců ukončilo pracovní poměr uplynutím doby určité, **12** zaměstnanců výpovědí ze strany zaměstnance a **11** pracovních poměrů bylo ukončeno dohodou na žádost zaměstnance. Nejčastější důvod ukončení pracovního poměru byla výpověď ze strany zaměstnance.

Nástupy a odchody zaměstnanců v roce 2021

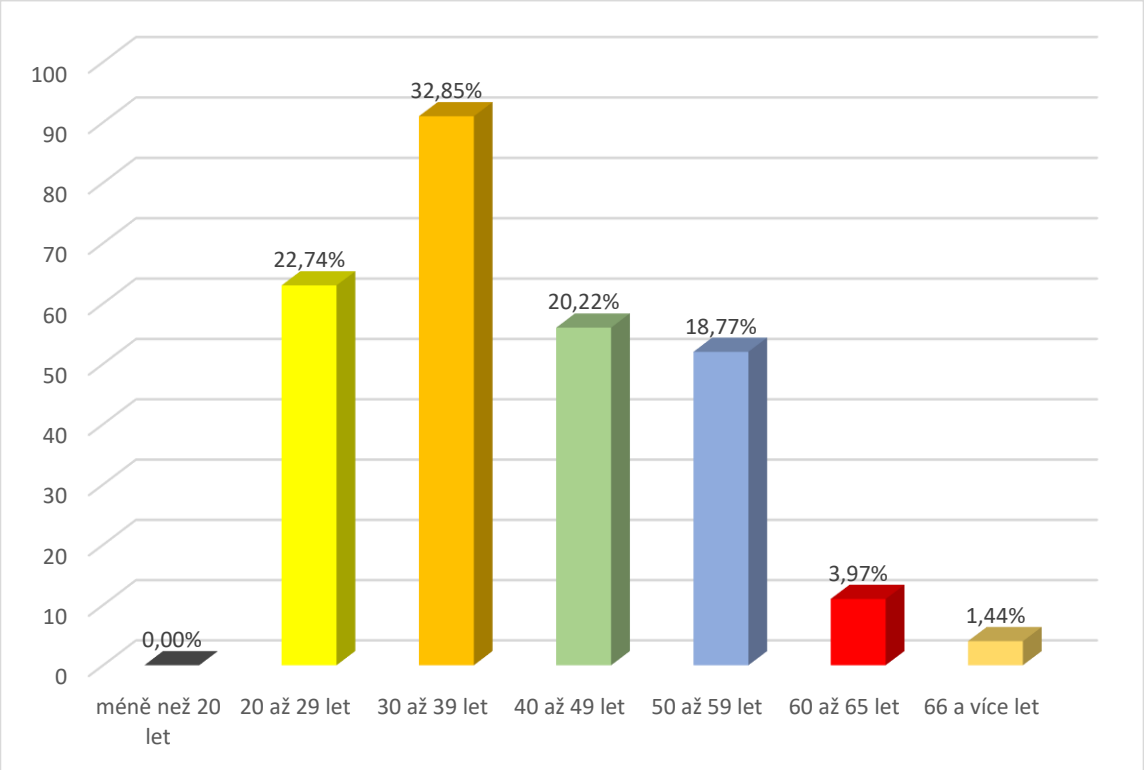


Struktura zaměstnanců k 31. prosinci 2021

V následující tabulce je uvedena věková struktura zaměstnanců (včetně zaměstnanců dočasně mimo systemizovaná pracovní místa):

Věková kategorie	Počet zaměstnanců k 31. 12. 2021	Podíl zaměstnanců v %	Z toho	
			muži	ženy
méně než 20 let	0	0,0 %	0	0
20 až 29 let	63	22,74 %	40	23
30 až 39 let	91	32,85 %	55	36
40 až 49 let	56	20,22 %	36	20
50 až 59 let	52	18,77 %	34	18
60 až 65	11	3,97 %	9	2
66 a více let	4	1,44 %	3	1
Celkem	**277**	**100,00 %**	**177**	**100**

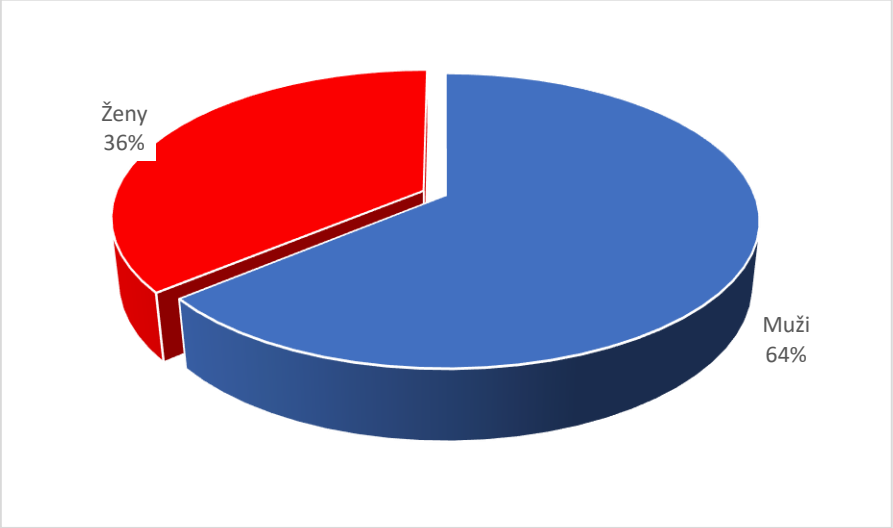
Struktura zaměstnanců NÚKIB podle věku (%)



Struktura zaměstnanců – ženy/muži

K 31. prosinci 2021 evidoval NÚKIB celkem 277 zaměstnanců (267 na systemizovaných pracovních místech a 10 dočasně mimo systemizovaná pracovní místa), z toho bylo 63,9 % mužů a 36,1 % žen.

Struktura zaměstnanců NÚKIB – ženy/muži

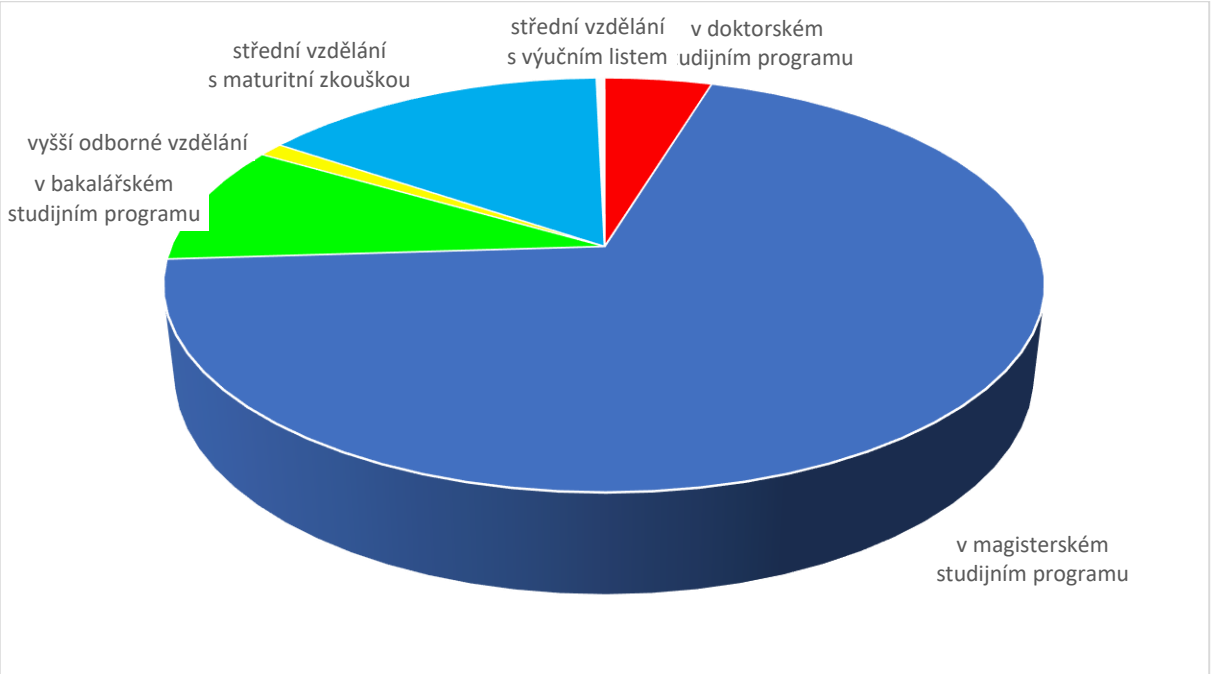


Kvalifikační struktura zaměstnanců

Systemizovaná pracovní místa ve struktuře NÚKIB mají stanovena požadované kvalifikační předpoklady a požadavky. Plnění potřebného vzdělání se pak promítá v kvalifikační struktuře zaměstnanců NÚKIB.

Dosažené vzdělání k 31. 12. 2021 (zahrnuti jsou též zaměstnanci dočasně na MD, RD a uvolnění k výkonu veřejné funkce)	**Počet zaměstnanců k 31. 12. 2021**	**Procentní struktura**
v doktorském studijním programu	13	4,69 %
v magisterském studijním programu	192	69,31 %
v bakalářském studijním programu	26	9,39 %
vyšší odborné vzdělání	3	1,08 %
střední vzdělání s maturitní zkouškou	42	15,16 %
střední vzdělání s výučním listem nebo střední vzdělání	1	0,36 %
základní vzdělání	0	0,00 %
Celkem	**277**	**100 %**

Struktura zaměstnanců podle vzdělání



Vzdělávání a rozvoj zaměstnanců

Osobnostní a profesní rozvoj zaměstnanců prostřednictvím soustavného rozvíjení, zvyšování a prohlubování dovedností, znalostí a kompetencí znamená udržení profesionality NÚKIB. Zabezpečujeme odborný rozvoj zaměstnanců, zajišťujeme prohlubování a zvyšování jejich odborné kvalifikace a umožňujeme zaměstnancům skupinové i individuální jazykové vzdělávání.

Vzdělávání je zabezpečováno formou individuálních i hromadných vzdělávacích akcí. V roce 2021 byla realizována školení převážně v oblasti programování, projektového řízení, řízení rizik, strategického řízení, IT bezpečnosti a hackingu a prostředí Windows, dále také školení zaměřená na prohloubení znalostí v oblasti kancelářských programů MS Excel, MS Word, PowerPoint apod. Další školení byla zaměřena na změny v legislativě, veřejných zakázkách, novinkách v oblasti ekonomiky, personalistiky a právní oblasti. Zaměstnanci se také účastnili různých odborných konferencí, například konference Cyberspace 2021 nebo České právo a informační technologie 2021. Také v roce 2021 převažovalo z důvodu nepříznivé pandemické situace vzdělávání online formou.

Zaměstnávání osob se zdravotním postižením

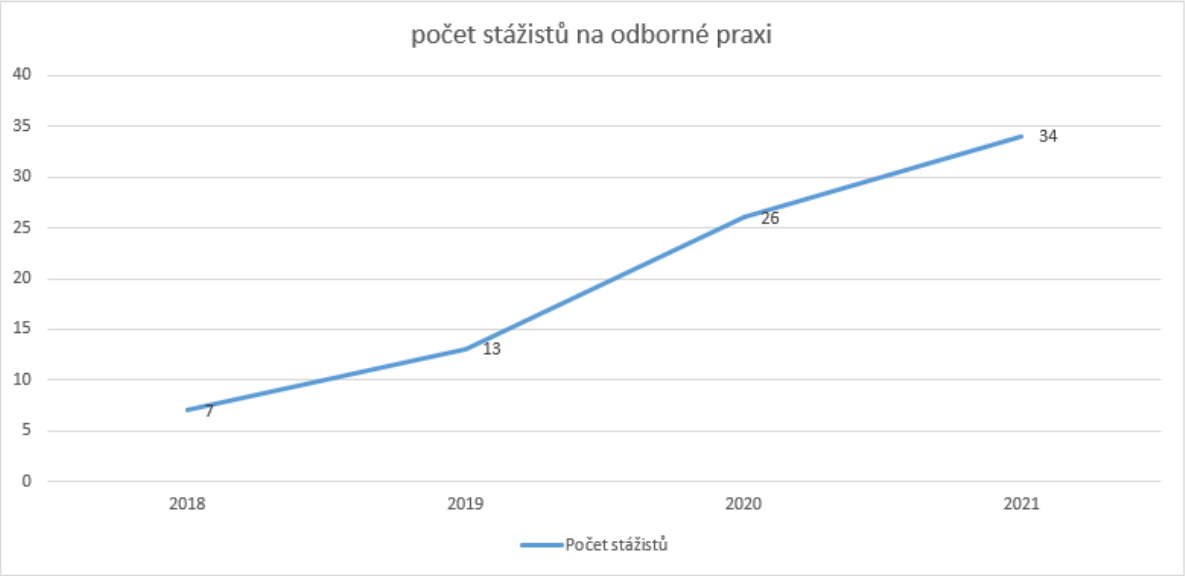
NÚKIB je v souladu s § 83 zákona č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů, povinen plnit **stanovený podíl osob se zdravotním postižením**. Naplňování podílu je možno realizovat zaměstnáváním osob se zdravotním postižením, nebo odběrem výrobků a služeb od zaměstnavatelů, kteří zaměstnávají více než 50 % osob se zdravotním postižením.

V roce 2021 měl NÚKIB naplnit povinný podíl v zaměstnávání osob se zdravotním postižením ve výši **10,37 osob**. Plnění povinného podílu bylo splněno zaměstnáváním osob se zdravotním postižením ve výši **1,02 osob a odběrem výrobků a služeb v hodnotě 3 543 173 Kč**, což odpovídá v přepočtu zaměstnání **13,66 osob**.

Spolupráce s vysokými školami a odborné praxe studentů škol

Vedle pracovních příležitostí NÚKIB rovněž poskytuje za účelem přípravy na budoucí povolání praktické stáže pro vysokoškolské studenty a nově také umožňuje absolvování odborné praxe žákům Střední školy informatiky, poštovnictví a finančnictví Brno. Stáže NÚKIB poskytuje studentům nejen v rámci povinné praxe podle studijních osnov, ale i těm studentům, kteří o stáž požádají z důvodu vlastního zájmu o získání pracovních a odborných zkušeností pro svou budoucí kariéru.

V roce 2021 absolvovalo stáž 34 studentů, což bylo o 8 více než v roce 2020. Stáže byly technického i politicko-bezpečnostního zaměření. Součástí spolupráce se studenty byly také pravidelné odborné konzultace diplomových a seminárních prací. Přednáškové činnosti a spolupráci s vysokými školami bude věnována mimořádná pozornost i v budoucnu. V roce 2021 byly nově uzavřeny **smlouvy o spolupráci** s Univerzitou obrany Brno, CEVRO Institutem, z. ú. a Diplomatickou akademií s.r.o. Dále byla uzavřena smlouva o spolupráci se Střední školou informatiky, poštovnictví a finančnictví Brno, přičemž v rámci této smlouvy na NÚKIB vykonávalo odbornou praxi **5 studentů** oboru Kybernetická bezpečnost.



Investice a rozvoj

V roce 2021 oddělení investic a rozvoje realizovalo několik investičních akcí, které přispěly zejména k rozšíření kancelářských prostor NÚKIB.

Na pracovišti Cejl proběhla stavební rekonstrukce za účelem rozšíření kancelářských prostor a kapacita objektu tímto vzrostla o 35–38 kancelářských míst.

Na pracovišti Gorkého v Brně byla po výběrovém řízení na dodavatele stavebních prací a předání staveniště zahájena rekonstrukce celého činžovního domu, tím dojde k navýšení o přibližně 90 kancelářských míst. Plánované dokončení rekonstrukce se předpokládá koncem roku 2022. Tento objekt bude určen zejména pro zaměstnance, kteří jsou aktuálně umístěni v nájemních prostorách objektu Vysoké učení technické (dále jen „VUT“).

V Brně NÚKIB realizoval rekonstrukci služebního bytu v ul. Čápkova, který je určen pro zaměstnance cestující služebně do Brna.

V Praze pokračovaly práce spojené s rekonstrukcí prostor objektu na Praze 6, které budou určeny zejména pro zaměstnance dislokované v prostorách Národního bezpečnostního úřadu (dále jen „NBÚ“) a rozšíření kancelářských prostor v objektu Olšanská. Dokončení těchto rekonstrukcí se předpokládá do července 2022.

Nová administrativní budova NÚKIB v Brně – Černých Polích

V lednu 2021 byly aktualizovány podklady pro jednací řízení bez uveřejnění, které navazovalo na architektonickou soutěž proběhlou v roce 2019. S vybraným uchazečem byla uzavřena

smlouva na zpracování všech stupňů projektové dokumentace, vyřízení stavebního povolení a služeb autorského dozoru.

Do konce roku 2021 zhotovitel zpracoval první fázi/stupeň projektové dokumentace *„studii stavby“*. Následně se bude počátkem roku 2022 pokračovat zpracováním *„dokumentace pro stavební povolení“*. Studie stavby obsahuje zejména:

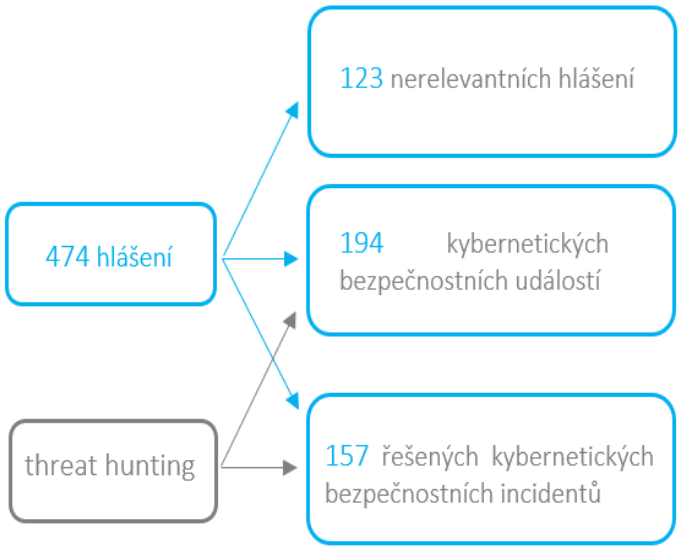
- rozpracování zadání, tj. návrh objektu a jeho zasazení na stávající pozemek. Objekt je určen pro cca 320 zaměstnanců, dále vybudování víceúčelového kyberpolygonu pro 150 lidí, technické a provozně speciální místnosti určené pro činnost NÚKIB, aj.,
- řešení návrhu objektu vzhledem k plánované změně územního plánu (rok 2022),
- bezpečností řešení, tj. řešení fyzické bezpečnosti a režimového opatření pro denní provoz NÚKIB ve všech jeho činnostech,
- řešení rozložení jednotlivých zón v okolí objektu v návaznosti na bezpečnostní řešení,
- terénní a zahradní úpravy podle možností, které umožňuje bezpečnostní opatření,
- průzkumy a měření (např. řešení návaznosti inženýrských sítí, geologický a dendrologický průzkum, měření radonu, měření spodní vody apod.),
- dispoziční řešení typických (2.NP - 4.NP) a netypických (suterén, 1.NP, střecha) pater s vysokou možností variability, návrh pro možnost nástavby 5.NP v provedení shell and core,
- návrh objektu jako objektu s vyšším energetickým standardem nebo jako pasivní objekt s max. využitím obnovitelných zdrojů a záchytem vody, využitím fotovoltaiky, tepelného čerpadla apod.

2 Sekce Národní centrum kybernetické bezpečnosti

Vládní CERT (GovCERT.CZ)

Počet kybernetických bezpečnostních incidentů v roce 2021

NÚKIB v roce 2021 obdržel 474 hlášení, z nichž 157 vyhodnotil jako kybernetické bezpečnostní incidenty a ty následně řešil.



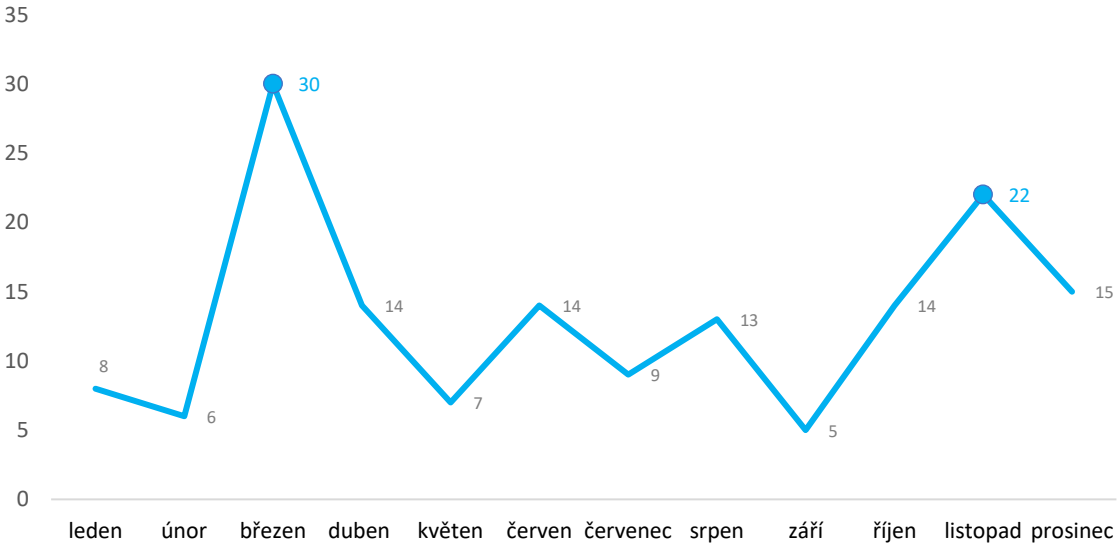
NÚKIB přijal 474 hlášení, u kterých vyhodnocoval jejich povahu a potřebu danou věc řešit. Ve 131 případech nebyl jeho zásah potřebný.

Kybernetická bezpečnostní událost je taková událost, která může vést ke kybernetickému incidentu. Typickým příkladem je zranitelný stroj v infrastruktuře organizace. Ten představuje slabé místo, jehož zneužitím by došlo ke kybernetickému incidentu.

Kybernetický bezpečnostní incident je případ, kdy dojde k narušení důvěrnosti, integrity nebo dostupnosti informací a služeb.

Rekordním měsícem se stal březen se 30 incidenty. V té době probíhalo masivní zneužívání zranitelnosti ProxyLogon, která cílí na kompromitaci široce využívané služby Microsoft Exchange Server. Druhým rušným měsícem byl listopad, kdy byla napříč ČR aktivně zneužívána zranitelnost ProxyShell ve stejné službě a došlo k nárůstu ransomwarových útoků.

Počet incidentů v průběhu roku 2021



Počet incidentů, které GovCERT řeší, se každým rokem zvyšuje. Během roku 2021 to bylo 157 incidentů, což představuje **59% nárůst oproti předchozímu roku**, kdy bylo řešeno 99 incidentů.

Do klasifikace incidentů se promítly trendy uplynulého roku, a to především v podobě ransomwarových útoků a zneužívání zranitelností:

- **Dostupnost (34 % řešených incidentů)**: Nejvíce incidentů minulého roku negativně ovlivnilo dostupnost služeb. Promítly se do toho DDoS útoky, technické chyby i ransomwarové útoky, které kvůli špatně řešeným zálohám omezily fungování napadených organizací,
- **Škodlivý kód (25 % řešených incidentů)**: Druhou nejčastější kategorií se staly škodlivé kódy. Stojí za nimi především ransomwarové útoky. Ty nicméně nenapáchaly větší škody, jelikož napadené organizace měly své zálohy dobře vyřešené. Po zašifrování infrastruktury se jim tedy podařilo provoz rychle obnovit a dostupnost jejich služeb nebyla narušena. Vedle ransomwarových útoků NÚKIB v této kategorii řešil také případy malwaru, které na našem území hostovaly své kontrolní servery, především TrickBot, Emotet nebo Dridex,
- **Průniky (22 % řešených incidentů)**: K výraznému nárůstu oproti roku 2020 došlo v incidentech, které NÚKIB klasifikoval jako průnik. Loni tvořily průniky 9 % všech incidentů, letos se číslo navýšilo na 22 %. Zatímco se škodlivé kódy a incidenty s dostupností objevovaly stabilně v průběhu celého roku, průniky přicházely skokově při zveřejnění nových zranitelností, jako např. v případě březnové kampaně zneužívání zranitelností MS Exchange Server.

Další aktivity GovCERT v roce 2021

GovCERT v roce 2021:

- spustil Neveřejný web, na kterém sdílí informace a data s partnery,
- provedl penetrační testování deseti organizací,
- otestoval 73 institucí na zranitelnost Log4Shell,
- zapojil 15 institucí do průběžného skenování zranitelností,
- ukončil testovací fázi Honeypotů a začal aktivně zájemcům nabízet zapojení se do projektu,
- upozornil na 26 hrozeb a zranitelností,
- podílel se na přípravě reaktivních opatření ke zranitelnostem MS Exchange Server a Log4Shell,
- vydal ochranné opatření k zabezpečení e-mailových schránek pro správce a provozovatele informačních systémů nezbytných pro fungování státu,
- začal publikovat pravidelný veřejný report ke kybernetickým incidentům.

Odbor kybernetických bezpečnostních politik

Oddělení národních strategií a politik

Při zajišťování kybernetické bezpečnosti na národní úrovni je zásadní spolupráce dotčených subjektů, a to i při 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.

Pracovníci NASTAPO během první poloviny roku 2021 zpracovali Akční plán k Národní strategii kybernetické bezpečnosti pro období let 2021 až 2025 (dále jen „Akční plán“). Na jeho vzniku se významně podílely všechny veřejné instituce v ČR, které sehrávají relevantní úlohu při zajišťování kybernetické bezpečnosti. Akční plán, který byl vládou ČR schválen v červenci 2021, představuje implementační část k Národní strategii kybernetické bezpečnosti ČR. Akční plán stanovuje na období let 2021 až 2025 celkově 105 úkolů, vč. zodpovědných subjektů a termínů plnění. Některé z úkolů jsou nastaveny jako průběžné (např. v oblasti vzdělávání nebo organizaci cvičení), jiné vyžadují komplexnější změny (např. zpracování návrhu národní politiky koordinovaného zveřejňování zranitelností). Vyhodnocení úkolů z Akčního plánu každoročně provádí NASTAPO. Za rok 2021 bylo vyhodnocováno 76 úkolů, přičemž 71 je v režimu průběžného plnění. Drtivá většina hodnocených úkolů byla splněna/plněna průběžně. Pouze 8 úkolů bylo naplněno částečně, jako nesplněný nebyl shledán žádný z úkolů.

I v roce 2021 pracovníci NASTAPO prohlubovali spolupráci při zajišťování a implementaci kybernetické bezpečnostní politiky. Úzká součinnost probíhala například nad zpracováním Národní strategie pro čelení hybridnímu působení, jejímž gestorem je Ministerstvo obrany (dále jen „MO“) a která byla vládou ČR schválena v dubnu 2021. Strategii implementuje Akční plán, zpracovaný během léta a schválený vládou ČR v listopadu 2021 usnesením č. 1 047. Pracovníci NASTAPO rovněž připomínkovali četné resortní dokumenty (např. Koncepci rozvoje schopností Policie České republiky v oblasti trestné činnosti páchané v kyberprostoru), aktivně se účastnili různorodých jednání (např. k implementaci Koncepce Smart Cities), během nichž akcentovali téma kybernetické bezpečnosti. NASTAPO taktéž zorganizovalo setkání české

komunity kybernetické bezpečnosti (tzv. C2S2), které proběhlo v říjnu 2021 a na kterém byly diskutovány především praktické aspekty zajišťování kybernetické bezpečnosti vyplývající z praxe účastníků.

Samostatnou kapitolu v oblasti spolupráce bylo nastavování pravidel kybernetické bezpečnosti 5G sítí, a to zejména prostřednictvím přípravy návrhů zavedení některých opatření EU 5G Toolboxu do českého právního řádu. Kromě NÚKIB, za který tuto aktivitu koordinovalo NASTAPO, se na ní podíleli také zástupci dalších státních institucí, do jejichž působnosti spadá bezpečnost sítí elektronických komunikací a ochrana bezpečnostních zájmů ČR, a zástupci akademického i soukromého sektoru z oblasti elektronických komunikací. Po většinu roku probíhal na úrovni Bezpečnostní rady státu (dále jen „BRS“) proces přípravy možných přístupů k posuzování a omezování rizik spojených s dodavateli 5G sítí, kdy NÚKIB spolu s dalšími orgány státní správy předkládal koncepční varianty a řešení. V říjnu 2021 zvolila BRS jednu z variant a uložila NÚKIB spolu s dalšími orgány státní správy rozpracovat vybranou variantu do podoby věcného záměru zákona. NÚKIB po celý rok 2021 také pravidelně organizoval jednání pracovní skupiny pro kybernetickou bezpečnost 5G Aliance, kde byli zástupci soukromého sektoru informováni o nejnovějším vývoji v oblasti národní regulace a politik kybernetické bezpečnosti 5G sítí. V roce 2022 budou tato jednání a spolupráce pokračovat, a to především v souvislosti s přípravou zmíněného věcného záměru zákona.

Pracovníci NASTAPO dále koordinovali přípravy a organizaci již sedmého ročníku konference CyberCon Brno, která se uskutečnila v září 2021 v Univerzitním kině Scala v Brně. Změnou oproti minulým ročníkům bylo rozšíření konference o mezinárodní den probíhající v anglickém jazyce. Ten zahrnoval debaty o kybernetické bezpečnosti ve zdravotnictví, přípravě revize Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (dále jen “směrnice NIS“[1]), Cyber Law Toolkitu či problematice kvantové výpočetní techniky. Druhý den v příspěvcích rezonovaly současné a budoucí výzvy pro kybernetickou bezpečnost, jimiž jsou např. přelomové technologie. Konferenci uzavřel seminář k zákonu o kybernetické bezpečnosti, jehož cílem bylo předat publiku novinky v oblasti legislativy a regulace. Každý den

1 Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii.

si tak přes 300 účastníků z řad odborné i široké veřejnosti mohlo poslechnout rozličné příspěvky v podání 37 domácích i zahraničních řečníků. Součástí konference byl i doprovodný program, např. veletrh studijních příležitostí Studuj kyber!, technický workshop či ukázka table-top cvičení kybernetické bezpečnosti.

Při NASTAPO působí právní poradce (LEGAD) CERT, který poskytuje právní poradenství Vládnímu CERT a koordinuje některé průřezové právní otázky v rámci Odboru kybernetických bezpečnostních politik a Sekce Národního centra kybernetické bezpečnosti. Mezi jeho hlavní úkoly v roce 2021 patřila aktualizace procesů Vládního CERT, příprava pravidel spolupráce CERT a dalších organizačních celků NÚKIB. Dále se LEGAD CERT podílel na přípravě opatření podle zákona o kybernetické bezpečnosti, revizi a přípravě smluv upravujících činnost Vládního CERT nebo připomínkování legislativních materiálů.

Oddělení cvičení

Organizace a realizace cvičení kybernetické bezpečnosti je důležitou aktivitou NÚKIB, kterou se zabývá Oddělení cvičení. V roce 2021 proběhlo v porovnání s 2020 více cvičení, a to jak těch nových, tak těch dříve přesunutých. Připravovaná i uskutečněná cvičení se zaměřovala mimo jiné na ověřování technických, strategických i komunikačních dovedností účastníků. Uvedený přehled obsahuje souhrn relevantních tuzemských a zahraničních cvičení.

Aktivity v ČR

Cvičení pro platformu MO pro spolupráci se strategickými subjekty obranného průmyslu

Cvičení zorganizovalo MO spolu s NÚKIB a cílilo na firmy účastnící se platformy MO pro kooperaci strategických společností obranného průmyslu ČR a státu. Akce si kladla za cíl prověřit připravenost klíčových firem obranného průmyslu na hrozby související s kyberprostorem. Účastníci z řad top managementu i zaměstnanců těchto firem, pracovníci MO, NÚKIB a dále Ministerstva průmyslu a obchodu (dále jen „MPO“) museli řešit nejen samotné kybernetické útoky, ale také jejich právní či mediální aspekty a provázanost s krizovým managementem. Scénář cvičení, připravený na míru zúčastněným firmám, byl koncipován jako hybridní kampaň zahrnující širokou škálu hrozeb.

Cvičení pro ČEPS

Cvičení vycházelo z demo ukázky pro profesní sdružení ISACA a jeho cílem bylo procvičit reakci účastníků na krizovou situaci způsobenou kybernetickým útokem. Cvičení bylo koncipováno jako předstupeň komplexního interního cvičení společnosti ČEPS. Scénář pracoval s reálným prostředím ČR pohledem fiktivního provozovatele elektroenergetické přenosové soustavy.

Cvičení pro Státní pokladnu Centrum sdílených služeb

Cílovou skupinou cvičení uspořádaného NÚKIB a Státní pokladnou Centrem sdílených služeb (dále jen „SPCSS“) byli pracovníci organizací spadajících pod MF. Cílem cvičení bylo prověřit možnosti spolupráce těchto organizací na půdě SPCSS, která mimo jiné slouží jako platforma pro spolupráci jednotlivých institucí pod MF s cílem zlepšit jejich celkové zabezpečení. Účastníky této akce byli zástupci MF, Generálního finančního ředitelství, Generálního ředitelství cel, Úřadu pro zastupování státu ve věcech majetkových, akciové společnosti ČEPRO, Kanceláře finančního arbitra a Státní tiskárny cenin. Samotné cvičení probíhalo formou moderované diskuse. Během ní účastníci navrhovali řešení různých předem připravených scénářů, které kombinovaly jak každodenní provozní záležitosti, tak i cílené kybernetické útoky či dezinformační kampaně. Cílem takového cvičení je ukázat na komplexnost kybernetických incidentů, které mimo technické roviny zasahují také do oblasti krizového plánování, komunikace s veřejností, práva a exekutivy.

Health Czech 2021

Jednalo se o historicky první sektorové cvičení kybernetické bezpečnosti pro sektor zdravotnictví. Cvičení bylo zaměřeno na nemocnice, které spadají pod regulaci zákona o kybernetické bezpečnosti a jejichž vyřazení z provozu by mělo za následek ohrožení velkého množství pacientů a obecně významně negativní dopad na ČR. Mezi cvičícími byli zástupci z celkem 16 nemocnic, jejichž týmy byly složené z pracovníků IT, odborníků na (kybernetickou) bezpečnost, ale také právníků, tiskových mluvčí a pracovníků léčebně preventivní péče. Cílem cvičení bylo zahrnout všechny tyto rozdílné role a přispět ke vzájemné spolupráci a společnému přístupu ke kybernetické bezpečnosti. Cvičení bylo dvoudenní, přičemž první den odpoledne proběhlo samotné cvičení, druhý den pak workshopy. Během nich experti NÚKIB a zástupci dalších relevantních institucí s účastníky sdíleli dobrou praxi, doporučené postupy a praktické rady. Komplexní povaha cvičení umožnila prověřit reakci napadených nemocnic po všech stránkách – technické, organizační, právní a mediální. Poznatky získané při konání Health Czech

budou uplatněny také při dalším cvičení určeném pro zdravotnický sektor, které se bude konat v roce 2022.

Cvičení pro Český statistický úřad

Table-top cvičení pro Český statistický úřad bylo součástí tzv. komplexního auditu, jehož cílem bylo celostně prověřit systém zajišťující zpracování a prezentaci výsledků voleb. Hlavním cílem cvičení bylo především procvičit okamžitou reakci a rozhodovací procesy v časové tísni během krize způsobené kybernetickým útokem. Scénář se zaměřoval jak na technická opatření a organizační řešení, tak na komunikační strategii v reakci na předložené situace. Přínosem celého cvičení byla rovněž podnětná diskuse, během které cvičící předkládali různá řešení vyvstanuvších problémů.

Cvičení v rámci konference CyberCon Brno 2021

Součástí NÚKIB organizované a již popsané konference bylo i krátké, formou workshopu konané cvičení. Cvičení mělo za cíl zdůraznit komplexnost krizového managementu a obecně zvýšit povědomí v oblasti kybernetické bezpečnosti. Účastníkům poskytlo příležitost vyzkoušet si roli cvičícího a zažít si všechny aspekty takového cvičení.

Cvičení v rámci kurzu Kybernetická bezpečnost na FSS

Table-top cvičení mělo za cíl přiblížit studentům reálnou podobu kybernetických cvičení. Bylo vedené formou moderované diskuse, aby podnítilo aktivitu studentů a poskytlo jim možnost se maximálně vžít do děje a řešit situace, které by v souvislosti s kybernetickými útoky mohly nastat. Scénář cvičení byl založen na potenciální krizové situaci, která by vznikla napadením a nedostupností různých univerzitních systémů. Otázky se týkaly zejména netechnických aspektů, například povinnosti správce a provozovatele systémů, mediální komunikace či role NÚKIB a Policie ČR v obdobných situacích.

Zahraniční aktivity

Locked Shields 2021

Ve dnech 12. – 16. dubna 2021 proběhl další ročník největšího a nejkomplexnějšího mezinárodního cvičení kybernetické bezpečnosti Locked Shields, konaného pod záštitou expertního centra NATO CCD COE v estonském Tallinnu. Kvůli pandemii COVID-19 se celé

cvičení odehrálo distančně. Tým ČR se umístil na třetím místě. Cvičení Locked Shields představuje simulované série útoků tzv. Červeného týmu na systémy a sítě tzv. Modrých týmů, které jsou složeny z expertů chránící IT systémy i v reálném světě. Český Modrý tým, stejně jako v předchozích letech, reprezentovali zástupci NÚKIB, sdružení CESNET a CZ.NIC, MO, Armády ČR, Vojenského zpravodajství (dále jen „VZ"), Národní agentury pro komunikační a informační technologie (dále jen „NAKIT"), Masarykovy univerzity a předních firem z oblasti IT. Součástí cvičení byla i strategická hra, které se účastnili i představitelé klíčových bezpečnostních institucí. ČR měla své zástupce i v organizačních týmech, což přináší významnou zkušenost uplatnitelnou pro vývoj a přípravu národních cvičení.

Cyber Coalition 2021

Cvičení Cyber Coalition je mezinárodní cvičení kybernetické bezpečnosti pořádané Severoatlantickou aliancí (dále jen „NATO") a uskutečnilo se od 29. listopadu do 3. prosince 2021 v estonském středisku pro kybernetickou bezpečnost. Cyber Coalition 2021 se zúčastnily všechny členské země NATO, jakož i partneři Finsko, Irsko, Švédsko a Švýcarsko spolu s účastníky z průmyslového sektoru a akademické sféry. Celkově se tak uplynulého ročníku zúčastnilo asi 1 000 osob, a to jak přímo v Estonsku, tak i vzdáleně z jednotlivých států. Na úrovni ČR koordinoval NÚKIB civilní část, Velitelství kybernetických sil a informačních operací (dále jen „VeKySIO") pak tu vojenskou. Cílem cvičení je utužení spojenectví a vzájemné spolupráce mezi zúčastněnými státy. Scénář se zaměřuje jak na řešení technických výzev, tak i na podnícení spolupráce a vytvoření společného situačního povědomí mezi členskými státy. Připravené scénáře zahrnovaly kybernetické útoky na plynovody, útoky narušující rozmístění vojenských jednotek a jejich logistiku i ransomwarový útok navázaný na pandemii COVID-19.

Cvičení s Izraelem

V říjnu 2021 proběhlo procesní cvičení s izraelským protějškem Vládního CERT, Israel National Cyber Directorate. Cvičení si kladlo za cíl procvičit reálné procesy, postupy a komunikaci s cílem dále prohloubit (nejen) operační spolupráci obou CERT týmů a dalších relevantních celků. Scénář cvičení a v něm obsažené události byly vybrány tak, aby vytvořily co nejlepší prostředí pro naplnění cílů cvičení a zároveň byly realistické. Záměrem bylo podnítit a ověřit vzájemnou koordinaci a komunikaci při řešení událostí a incidentů s mezinárodním přesahem a vytvoření

společného situačního povědomí. Cvičení potvrdilo důležitost mezinárodní spolupráce a s ní spojené výměny informací.

Cvičení pro ELSA v rámci Summer Law School

Cvičení bylo organizováno v rámci mezinárodní ELSA Summer Law School, přičemž proběhlo v anglickém jazyce. Jeho scénář byl zasazen do mezinárodního prostředí a řešené otázky kladly důraz na právní rovinu kybernetických incidentů. Studenti měli možnost aplikovat mezinárodní právo v situacích, které by reálně mohly nastat, a seznámit se blíže s klíčovými materiály, jako jsou například Tallinnský manuál či tzv. Budapešťská úmluva aj.

Cvičení v rámci finále European Cyber Security Challenge

V roce 2021 hostila ČR poprvé v historii finále evropské soutěže European Cyber Security Challenge, kterou každoročně pořádá Agentura Evropské unie pro kybernetickou bezpečnost (dále jen „ENISA“). Akce je koncipována jako soutěž týmů mladých talentů do 25 let v otázkách kryptografie, reverzního inženýrství nebo forenzní analýzy. V roce 2021 se soutěže účastnilo celkem 19 týmů ze zemí EU a jeden tým z Kanady. NÚKIB jako jeden z partnerů akce připravil pro doprovod soutěžících, zástupce médií a další partnery workshop s ukázkou table-top cvičení. Účastníci měli možnost řešit v rámci realisticky připraveného scénáře krizové situace mající původ v kybernetickém prostoru a nahlédnout na různé přístupy k mezinárodněprávním otázkám kybernetické bezpečnosti. Právě mezinárodní složení jednotlivých cvičících týmů přispělo k plodné a aktivní diskusi a také ke vzájemné výměně zkušeností, znalostí a poznatků.

Oddělení strategických informací a analýz

Pro NÚKIB je rovněž důležité disponovat potřebnou kapacitou pro monitoring a analýzu hrozeb. Toto zajišťuje Oddělení strategických informací a analýz. Jeho činnost směřuje jednak k analytické podpoře dalších organizačních celků v rámci NÚKIB, ale i partnerských institucí ve státní správě, veřejném i soukromém sektoru. Oddělení každoročně zpracovává Zprávu o stavu kybernetické bezpečnosti České republiky, která přináší komplexní pohled na vývoj kybernetické bezpečnosti v ČR. Dalšími důležitými produkty jsou Měsíční souhrn dění v kybernetické bezpečnosti pro partnery NÚKIB nebo automatizovaný monitoring zranitelností zdravotnických přístrojů pro nemocnice a další zdravotnická zařízení. V roce 2021 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 ČR závisí do velké míry na vývoji situace v zahraničí a rozhodnutích přijímaných na evropské a mezinárodní úrovni. Zájmy ČR v oblasti kybernetické bezpečnosti v mezinárodních organizacích a integračních uskupeních, zejména pak v EU, Organizace spojených národů (dále jen „OSN“), NATO, ale i Organizace pro hospodářskou spolupráci a rozvoj (dále jen „OECD“), Organizace pro bezpečnost a spolupráci v Evropě (dále jen „OBSE“) a Mezinárodní telekomunikační unie (dále jen „ITU“), zastupuje NÚKIB společně s Ministerstvem zahraničních věcí (dále jen „MZV“), MO a dalšími partnery. V rámci NÚKIB se touto agendou zabývá Oddělní mezinárodních organizací a práva. Následující přehled je souhrnem toho nejdůležitějšího, co se na poli uvedených institucí během roku 2021 odehrálo a na čem pracovníci oddělení participovali.

Evropská unie

ČR se v roce 2021 zapojila do naplňování konkrétních iniciativ Strategie kybernetické bezpečnosti EU. Strategie spolu s návrhem revize Směrnice NIS představují klíčové dokumenty ukotvující politické a legislativní směrování kybernetické bezpečnosti v EU. V Radě EU se NÚKIB i nadále podílel na činnosti Horizontální pracovní skupiny pro kybernetické otázky (dále jen „HWPCI“), která se zabývá aspekty spolupráce na poli kybernetické bezpečnosti v rámci EU a je odpovědná za koordinaci práce Rady v této oblasti. NÚKIB v roce 2021 pokračoval v účasti na jednáních k návrhu revize Směrnice NIS, který má zásadním způsobem rozšířit sektory regulovaných subjektů, přičemž by mělo dojít rovněž ke sjednocení způsobu jejich identifikace. Mělo by také dojít ke stanovení nových povinností v oblasti řízení rizik a hlášení incidentů, a to s cílem dosažení větší harmonizace právních předpisů a přístupu. V druhé polovině roku 2021 došlo k přijetí obecného přístupu Rady EU k návrhu revize Směrnice NIS, stejně jako zprávy Evropského parlamentu k tomuto návrhu. Pozornost NÚKIB se na unijní úrovni soustředila také na sondážní rozhovory k možné revizi opatření ze Cyber Diplomacy Toolboxu či na prvotní jednání k iniciativě Společné kybernetické jednotky (Joint Cyber Unit). Ta by na základě nezávazného doporučení Komise z června 2021 měla usilovat o posílení spolupráce mezi orgány, institucemi a členskými státy v případech závažných přeshraničních

kybernetických incidentů nebo hrozeb. V rámci krizového řízení EU byl NÚKIB také aktivně zapojen do pokračujících jednání ohledně plné operacionalizace Sítě styčných organizací pro řešení kybernetických krizí (CyCLONe), v níž jsou na dobrovolné bázi zastoupené všechny členské státy EU. Mimoto se zástupci NÚKIB účastnili pravidelných jednání pracovních skupin v rámci Skupiny pro spolupráci zřízené Směrnicí NIS.

Rok 2021 se také nesl ve znamení příprav historicky druhého předsednictví ČR v Radě EU, které ČR převezme po Francii v červenci roku 2022. V průběhu roku 2021 se proto zástupci ČR účastnili přípravných a koordinačních jednání, která jsou stěžejní pro úspěšnou organizaci i průběh samotného předsednictví. Tato jednání probíhala nejen vnitrostátně, ale také s unijními institucemi a v neposlední řadě i s Francií a Švédskem, s nimiž ČR tvoří tzv. předsednické trio. Pro NÚKIB bude předsednictví konkrétně znamenat mj. jak předsedání HWPCI a CyCLONe, tak organizaci několika předsednických akcí v ČR.

Organizace Severoatlantické smlouvy

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. V roce 2021 byla pro NATO připravena již pátá zpráva o stavu kybernetických schopností ČR. NÚKIB pokračoval v úzké spolupráci s NATO CCD COE, jehož je aktivním členem a přispívá do jeho činnosti.

Organizace spojených národů

V OSN v roce 2021 vyvíjely činnosti dvě skupiny, které se věnují otázkám odpovědného chování států v kyberprostoru. První z nich je Open-Ended Working Group (dále jen „OEWG“), která je aktuálně nejvýznamnější platformou v rámci OSN ke kybernetické bezpečnosti a na jejíž činnosti se NÚKIB spolu s MZV aktivně podílí. 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. V roce 2021 se NÚKIB účastnil třetího a posledního substantivního jednání první iterace OEWG (2019-2021) konaného v březnu 2021 v New Yorku, v jehož rámci došlo k přijetí konsenzuální závěrečné zprávy. Ve zbytku roku se pak již vyjednávaly organizační aspekty druhé iterace OEWG a první

substantivní zasedání proběhlo na konci roku 2021. Toho se NÚKIB rovněž zúčastnil a spolu s MZV a zahraničními partnery (Microsoft a CyberPeace Institute) připravili na jeho okraj side-event k ochraně zdravotního sektoru v rámci projektu Protecting the Healthcare Sector from Cyber Harm.

Vedle OEWG monitoroval NÚKIB na úrovni OSN také vývoj ve druhé pracovní skupině, UN Group of Governmental Experts (dále jen „UN GGE“). UN GGE se skládá z 25 členů vybraných podle spravedlivého geografického rozložení, přičemž ČR mezi členy není. NÚKIB však vývoj v této skupině dlouhodobě sledoval, a to zejména s ohledem na souvislost s paralelním formátem OEWG a možnými důsledky jednání UN GGE v oblasti uplatnitelnosti mezinárodního práva v kyberprostoru. V květnu 2021 došlo k přijetí závěrečné zprávy a ukončení této iterace UN GGE. K zahájení další iterace (narozdíl od OEWG) v roce 2021 však již nedošlo.

V roce 2021 probíhala jednání Ad Hoc Committee on Cybercrime (dále jen „AHC“), jejímž cílem je posílit stávající regionální a mezinárodní mechanismy v oblasti kyberzločinu, resp. vytvořit a přijmout novou mezinárodní úmluvu. NÚKIB spolu s MZV a Ministerstvem spravedlnosti (dále jen MS) vývoj příprav a organizačních jednání AHC sledoval a nadále sleduje, a to zejména s cílem zajistit soulad výstupů se stávající Úmluvou Rady Evropy o počítačové kriminalitě (tzv. Budapešťskou úmluvou), kterou ČR ratifikovala v roce 2013.

Organizace pro hospodářskou spolupráci a rozvoj

V OECD v roce 2021 pokračovala v činnosti Working Group on Security in the Digital Economy (dále jen „SDE“). Stěžejní pro NÚKIB byla aktivita expertních podskupin SDE, jejichž analytické výstupy mohou posloužit jako vodítko při zavádění nebo revizi národních politik, strategií a legislativy v oblasti digitální bezpečnosti. Pracovníci NÚKIB se tak účastnili jednání expertních skupin k bezpečnosti internetu věcí, ke koordinovanému zveřejňování zranitelností a k přístupu vlád vůči údajům drženým soukromým sektorem. Výstupem ze skupin jsou expertní zprávy OECD, které mapují stávající úpravu napříč členskými státy OECD, doporučují ověřené postupy a navrhují možná opatření. ČR se v roce 2021 stala členem elitního klubu Global Partnership on Artificial Intelligence, jehož smyslem je propojovat experty z veřejné správy a akademického i soukromého sektoru za účelem implementace umělé inteligence (dále jen „AI“) do praxe. V průběhu roku 2021 rovněž vznikla na úrovni OECD nová pracovní skupina k AI, která by měla sdružovat regulátory zodpovědné za nastavení národních AI strategií.

Organizace pro bezpečnost a spolupráci v Evropě

V rámci OBSE v roce 2021 pokračovala v činnosti Informal Working Group (dále jen „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 (dále jen „CBM“). NÚKIB se v roce 2021 účastnil ve spolupráci s MZV zasedání IWG (vzdáleně i osobně) a i nadále se podílel na implementaci zejména CBM 16 (Koordinované zveřejňování zranitelností) a realizoval bilaterální výměnu informací s vybranými státy v rámci CBM 8 (Výměna informací mezi styčnými pracovníky). V roce 2021 proběhla i za účasti NÚKIB dvě komunikační cvičení pro styčné pracovníky, která sloužila k zajištění funkčních komunikačních kanálů a k výměně informací mezi jednotlivými členskými státy a příslušnými celky. Pracovníci NÚKIB se rovněž zúčastnili řady virtuálních workshopů na téma kybernetické bezpečnosti, které OBSE připravilo.

Mezinárodní telekomunikační unie

Problematika správy internetu, tzv. Internet Governance, a kybernetické bezpečnosti jako takové se v agendě ITU v posledních letech objevuje čím dál častěji. NÚKIB tak v roce 2021 sledoval a analyzoval dění zejména v oblasti standardizace telekomunikačních technologií, kybernetické bezpečnosti a AI, konkrétně pak v pracovních skupinách. V roce 2021 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 internetu bude nadále sílit. Takové snahy mohou mít negativní důsledky na stávající model správy internetu a kybernetickou bezpečnost jako takovou. NÚKIB se problematice na úrovni ITU, společně s dalšími národními partnery, nadále věnuje a úzce spolupracuje s MPO, ČTÚ a MZV. V listopadu roku 2021 se v Ženevě uskutečnily meziresortní konzultace české delegace složené ze zástupců výše uvedených resortů, jejichž součástí byly i schůzky se zástupci ITU (sektorů i sekretariátu).

V roce 2021 se NÚKIB i nadále angažoval virtuální formou v aktivitách Global Forum on Cyber Expertise (dále „GFCE“), ke které se ČR připojila v roce 2018. NÚKIB se angažoval v pracovní skupině k normám a kybernetické diplomacii a v pracovní skupině k ochraně kritické infrastruktury.

Prague 5G Security Conference

NÚKIB uspořádal ve spolupráci s MZV a pod záštitou Úřadu vlády ČR na přelomu listopadu a prosince 2021 The Prague 5G Security Conference. Třetí ročník konference, konající se kvůli pandemickým opatřením hybridní formou, se zaměřil na otázky spojené s bezpečností 5G sítí a přelomových technologií (Emerging Disruptive Technologies, dále jen „EDTs“). V průběhu konference vystoupilo téměř sedmdesát řečníků z Evropy i celého světa (např. z Izraele, Jižní Koreje, Japonska, Austrálie, USA, Kanady či Indie). Na konferenci nechyběli zástupci veřejného, akademického, neziskového, ani soukromého sektoru. Dvoudenní konference byla rozdělena na několik tematických panelů, kterých se virtuálně zúčastnily stovky mezinárodních posluchačů.

Na závěr konference byly představeny tzv. Pražské návrhy týkající se kybernetické bezpečnosti přelomových technologií (Prague Proposals on Cyber Security of EDTs). Zúčastněné země se v nich shodly na možných principech budoucího přístupu k EDTs. Dokument zmiňuje například důležitost zohlednění technických i netechnických rizik, bezpečnosti dodavatelského řetězce, transparentnosti, důvěryhodnosti a diverzifikace i demokratických a etických hodnot při rozvoji nových technologií. Výstupem třetího ročníku konference jsou ještě druhé Pražské návrhy, které se týkají diverzity dodavatelů telekomunikací (Prague Proposals on Telecommunications Supplier Diversity).

Odbor kontroly

Rok 2021 byl z pohledu kontrolní a auditní činnosti NÚKIB ovlivněn zejména mapováním stavu kybernetické bezpečnosti v nejvýznamnějších zdravotnických zařízení v ČR. Počet kontrol či auditů podle zákona o kybernetické bezpečnosti, respektive jeho prováděcí vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (o kybernetické bezpečnosti) (dále jen „VKB“) se v roce 2021 zvýšil z 8 na 22. Kontrola či audit u povinných orgánů a osob podle § 3 ZKB ověřuje plnění povinností plynoucích ze zákona o kybernetické bezpečnosti a VKB. V rámci každé kontroly nebo auditu je rámcově ověřováno cca 150 kontrolních bodů.

Kromě sektoru zdravotnictví se NÚKIB v roce 2021 zaměřil i na další subjekty jako například na prověření systému zajišťujícího zpracování a prezentaci výsledků voleb u Českého statistického úřadu. NÚKIB provedl tzv. komplexní audit zahrnující cvičné phishingové kampaně, skenování zranitelností, provedení interních a externích penetračních testů či zátěžových testů. Součástí komplexního auditu bylo také table-top cvičení, díky kterému měl Český statistický úřad možnost procvičit svoji připravenost na krizové situace při zpracování a prezentaci výsledků voleb vč. mediální linky. V neposlední řadě také proběhl audit souladu systému s požadavky VKB.

NÚKIB dále i v roce 2021 rozvíjel spolupráci v kontrolní činnosti s dalšími regulátory. Jmenovitě například s Úřadem pro civilní letectví, se kterým bylo v lednu podepsáno memorandum o spolupráci nejen v oblasti kontroly. Praktická spolupráce v oblasti kontroly se rozvinula i s Českou národní bankou (dále jen ČNB) při společné kontrole, kde byli zaměstnanci NÚKIB součástí kontrolní skupiny v pozici přizvané osoby. 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 sítě,
- příliš krátká doba uchovávání log záznamů,
- používání zastaralého hardware a software, který již jeho výrobce nepodporuje, a neřízení souvisejících rizik.

Odbor regulace

Určování a přezkum kritické informační infrastruktury

Určování KII provádí NÚKIB na základě zmocnění uvedeného v zákoně o kybernetické bezpečnosti a v zákoně č. 240/2000 Sb. Zákon o krizovém řízení a o změně některých zákonů, ve znění pozdějších předpisů, v souladu s nařízením vlády č. 315 o kritériích pro určení prvku KII, a to již od roku 2015. Zákon o kybernetické bezpečnosti také ukládá NÚKIB povinnost ověřovat každé 2 roky aktuálnost určení prvků KII. Správci prvků KII jsou jak organizační složky státu (OSS), tak i soukromé subjekty. NÚKIB ke konci roku 2021 evidoval celkem 60 subjektů, které spravují 131 prvků KII.

Zároveň byly přezkoumány již určené prvky KII u 28 správců KII. Jednalo se o 15 správců z řad organizačních složek státu a 13 soukromoprávních subjektů.

Významné informační systémy

S účinností od 1. ledna 2021 proběhla novela vyhlášky č. 317/2014 Sb., o významných informačních systémech. U organizačních složek státu a krajů byly zavedeny tzv. typové významné informační systémy, které jsou uvedeny ve výčtu v § 2 odst. 1 zmíněné vyhlášky. Tento paragraf má tzv. dělenou účinnost, a tedy bude nabíhat postupně a každý rok budou přidávány nové typové systémy, dokud v roce 2023 vyhláška nenaběhne do cílového stavu. K 1. lednu 2021 výčet typových systémů obsahoval systémy elektronické pošty a systémy využívané ke kontrolní nebo inspekční činnosti anebo státního dozoru. NÚKIB ke konci roku 2021 evidoval celkem 162 subjektů, které spravují 372 významných informačních systémů.

Kromě vydání podpůrných materiálů a individuálních konzultací s orgány veřejné moci proběhly také workshopy k problematice identifikace významných informačních systémů, kterých se zúčastnilo 246 osob z 68 státních organizací.

Provozovatel základní služby v roce 2021

Určování provozovatelů základní služby, které NÚKIB provádí od roku 2018, pokračovalo také v průběhu roku 2021. Správní řízení v rámci některých odvětví – především železniční a silniční dopravy – pokračovala ještě z roku 2020 a byla v roce 2021 dokončena. S ohledem

na novelizaci vyhlášky č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby a rozšíření kritérií v odvětví zdravotnictví došlo ihned po její účinnosti k zahájení určovacích správních řízení s relevantními subjekty, tj. nemocnicemi. Díky připravenosti na obou stranách proběhla daná řízení velmi rychle a bezproblémově. Následně se NÚKIB v průběhu roku zaměřil také na dokončení určování v odvětví energetika – teplárenství, a také zahájil určování zcela nového odvětví – vodního hospodářství. Jak se již stalo zvykem, před každou novou vlnou určování byl pro potenciální povinné osoby, se kterými bude řízení vedeno, uspořádán online workshop, na kterém byly tyto společnosti seznámeny s celým procesem.

V roce 2021 bylo zahájeno nebo vedeno 153 určovacích správních řízení. Z nich bylo ukončeno 84 správních řízení – 45 subjektů bylo nově určeno a 39 správních řízení bylo ukončeno rozhodnutím o neurčení.

Celkový počet určených provozovatelů základní služby, resp. správců informačních systémů základní služby, je 124 se 147 informačními systémy základní služby.

Podpůrné materiály

NÚKIB i nadále pokračuje ve vydávání veřejných podpůrných materiálů určených povinným osobám spadajícím pod zákon o kybernetické bezpečnosti i odborné veřejnosti. V průběhu roku 2021 došlo především k vydání souhrnného materiálu Pravidla určování kritické informační infrastruktury a Co si připravit na jednání, které souvisí především s tím, že NÚKIB v roce 2021 zahájil velkou vlnu přezkumů určení těchto povinných osob. Dále NÚKIB vydal podpůrný materiál Práva a povinnosti subjektů KII podle krizového zákona, který obsahuje shrnutí práv a povinností správců KII, které jim podle krizového zákona vyplývají a pohled NÚKIB na způsob plnění zákonných povinností a soulad s požadavky zákona o kybernetické bezpečnosti. Vedle kritické informační infrastruktury došlo k vydání podpůrného materiálu také v oblasti významných informačních systémů, kdy došlo k upřesnění této problematiky pro odvětví školství – podpůrný materiál Významné informační systémy ve školství. S ohledem na vydání ochranného opatření k zabezpečení e-mailu ze dne 11. října 2021 došlo také k vydání metodiky k tomuto opatření. Ke konci roku také došlo k vydání několika podpůrných materiálů v oblasti cloud computingu – Průvodce zařazením poptávaného cloud computingu do bezpečnostní úrovně a Požadavky na zprávy z penetračních testů v souvislosti se zápisem cloud computingu do katalogu cloud computingu. Tyto

dokumenty poskytují orgánům veřejné moci metodickou podporu pro zařazení informačního nebo komunikačního systému, který si přejí provozovat prostřednictvím služeb cloud computingu, do odpovídající bezpečnostní úrovně podle vyhlášky č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci, a poskytovatelům cloud computingu mají pomoci správně doložit požadované skutečnosti. Aktualizací se dočkaly také velmi důležité podpůrné materiály Požadavky na smlouvy s dodavateli a Provozovatel informačního systému. K poměrně velké aktualizaci došlo také v oblasti FAQ na internetových stránkách NÚKIB, které nyní obsahují více informací a odpovědí na dotazy, se kterými se NÚKIB setkává.

Konzultace

V roce 2021 proběhla řada konzultací týkajících se implementace zákona o kybernetické bezpečnosti. Typicky konzultovanými oblastmi jsou analýza rizik, zahrnutí bezpečnostních požadavků do veřejných zakázek, požadavky na smlouvy s dodavateli, technické aspekty bezpečnostních opatření, budování bezpečnostního povědomí v organizaci a nastavení bezpečnostních politik. Vedle toho NÚKIB s ohledem na účinnost nové právní úpravy reagoval na řadu dotazů směřujících na obsah požadavků kladených na poskytovatele cloud computingu a samotnou službu cloud computingu.

Opatření

V průběhu roku 2021 využil NÚKIB třikrát svou pravomoc vydat opatření v souladu s § 11 zákona o kybernetické bezpečnosti. Prvním takto vydaným opatřením bylo reaktivní opatření ze dne 11. března 2021, jehož cílem bylo zvýšení zabezpečení informačních systémů nebo sítí a služeb elektronických komunikací před kybernetickým bezpečnostním incidentem v souvislosti se zranitelnostmi Microsoft Exchange Server. Obsahem reaktivního opatření byla sada především technických opatření, které měly povinné subjekty za úkol provést. Druhým opatřením bylo ochranné opatření – historicky první využití institutu ochranného opatření podle zákona o kybernetické bezpečnosti – které ukládá povinným osobám zavést sadu technických opatření k většímu zabezpečení elektronické pošty, a to na základě poznatků z proběhlého kybernetického bezpečnostního incidentu. Ke konci roku, krátce po upozornění

na závažnou zranitelnost v komponentě Apache Log4j, která postihovala napříč různými odvětvími veškeré aplikace využívající ji k logování, přistoupil NÚKIB k vydání dalšího reaktivního opatření. Toto opatření obsahovalo povinné úkony a metodické pokyny k zabezpečení systémů před kybernetickým bezpečnostním incidentem, který zranitelnost mohla způsobit.

Cloud computing

Ministerstvo vnitra (dále jen „MV“) od srpna 2020 posuzuje poskytovatele a služby cloud computingu. Do tohoto posuzování je NÚKIB výrazně zapojen. NÚKIB v této oblasti provádí posouzení splnění bezpečnostních kritérií, která musejí poskytovatelé cloud computingu splnit, aby mohli dodávat služby veřejné správě. Do konce roku 2021 v této oblasti NÚKIB vydal již celkem 145 stanovisek.

Dne 1. září 2021 vstoupila v účinnost novela zákona č.365/2020 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů (dále jen „zákon o informačních systémech), která podstatně upravila a zpřesnila proces posuzování poskytovatelů cloud computingu a jednotlivých služeb cloud computingu v případě, že jsou poskytovány orgánům veřejné správy. Spolu s novelou zákona o informačních systémech veřejné správy vstoupila v účinnost vyhláška č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu, která blíže rozvádí požadavky na poskytovatele a služby cloud computingu. V této oblasti NÚKIB nově vydává závazná stanoviska k zápisu poskytovatelů cloud computingu do katalogu cloud computingu.

Kromě výše uvedeného tedy NÚKIB v roce 2021 posoudil ještě 4 poskytovatele podle požadavků stanovených vyhláškou č. 316/2021 Sb. V roce 2021 nebyl podle požadavků stanovených touto vyhláškou posouzen žádný cloud computing, protože NÚKIB neobdržel žádnou žádost o posouzení cloud computingu oproti požadavkům stanovených touto vyhláškou. To je dáno zejména tím, že nejprve musí dojít k posouzení poskytovatele cloud computingu a až následně je možné podat žádost o posouzení cloud computingu. S regulací cloud computingu souvisí ještě jeden právní předpis účinný od roku 2021, a sice vyhláška č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci, která definuje kritéria pro zařazování státních informačních systémů

do bezpečnostních úrovní, což je základní prerekvizita pro funkčnost celého rámce regulace cloud computingu.

Legislativa

Legislativní změny týkající se zákona o kybernetické bezpečnosti byly v roce 2021 spojeny především s problematikou cloud computingu. Podstatnou změnou prošlo s účinností od 1. září 2021 ustanovení § 4 odst. 5 zákona o kybernetické bezpečnosti. Tato úprava vedla k rozšíření okruhu jeho adresátů. Původně byla povinnost zajistit splnění bezpečnostních pravidel vztažena pouze na orgány veřejné moci, které byly zároveň jeho povinnými osobami. Nově tato povinnost dopadá na všechny orgány veřejné moci bez bližší specifikace. Nad to byla zavedena rovněž povinnost zařadit poptávaný cloud computing do bezpečnostní úrovně. V návaznosti na to byla také upravena související ustanovení zákona o kybernetické bezpečnosti. Ke stejnému datu, tedy 1. září 2021, rovněž vstoupila v účinnost vyhláška č. 315/2021 Sb. o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci. Tato vyhláška navazuje na § 4 odst. 5 zákona o kybernetické bezpečnosti a rozvíjí povinnost zařadit poptávaný cloud do bezpečnostní úrovně.

S účinností od 1. ledna 2021 došlo také ke změnám vyhlášky č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby, kde došlo k rozšíření kritérií pro odvětví zdravotnictví, a vyhlášky č. 317/2014 Sb., o významných informačních systémech, jejíž novelizace změnila obsah celé této vyhlášky a jejíž znění NÚKIB připravoval.

S ohledem na to, že Evropská komise zveřejnila na konci roku 2020 celou řadu návrhů nových právních předpisů týkajících se kybernetické bezpečnosti na úrovni Evropské unie nebo revizí stávajících, byly práce nad těmito návrhy i podstatnou součástí legislativních prací v roce 2021. Toto je případ především revize směrnice NIS, jejíž revize je označována jako NIS2. Vydání této revize je očekáváno v roce 2022. NÚKIB se také aktivně zapojoval především do formování národních pozic týkajících se směrnice Evropského parlamentu a Rady o posílení odolnosti kritických subjektů a nařízení Evropského parlamentu a Rady o digitální provozní odolnosti finančního sektoru a o změně nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014 a (EU) č. 909/2014, kde spolupracoval s národními gestory těchto předpisů.

3 Sekce informační bezpečnosti

Bezpečnost informačních a komunikačních systémů a kryptografická ochrana

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

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

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

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

Certifikační a akreditační činnost

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

Certifikace a akreditace informačních systémů

V roce 2021 probíhalo řízení o certifikaci 207 informačních systémů. K 50 žádostem o certifikaci informačního systému, jejichž zpracování bylo zahájeno v předchozím roce (2020), přibylo v roce 2021 dalších 157 žádostí, a to 62 ze státní správy nebo samosprávy a 95 ze soukromé sféry. Ve většině případů se jednalo o žádosti o opakovanou certifikaci již provozovaných informačních systémů. Ve 21 případech byla podána žádost o certifikaci nově budovaného informačního systému, přičemž pouze 6 z těchto žádostí pochází ze státní správy.

V uvedeném roce bylo vydáno celkem 151 certifikátů informačních systémů, z toho 58 pro žadatele ze státní správy nebo samosprávy a 93 ze soukromé sféry.

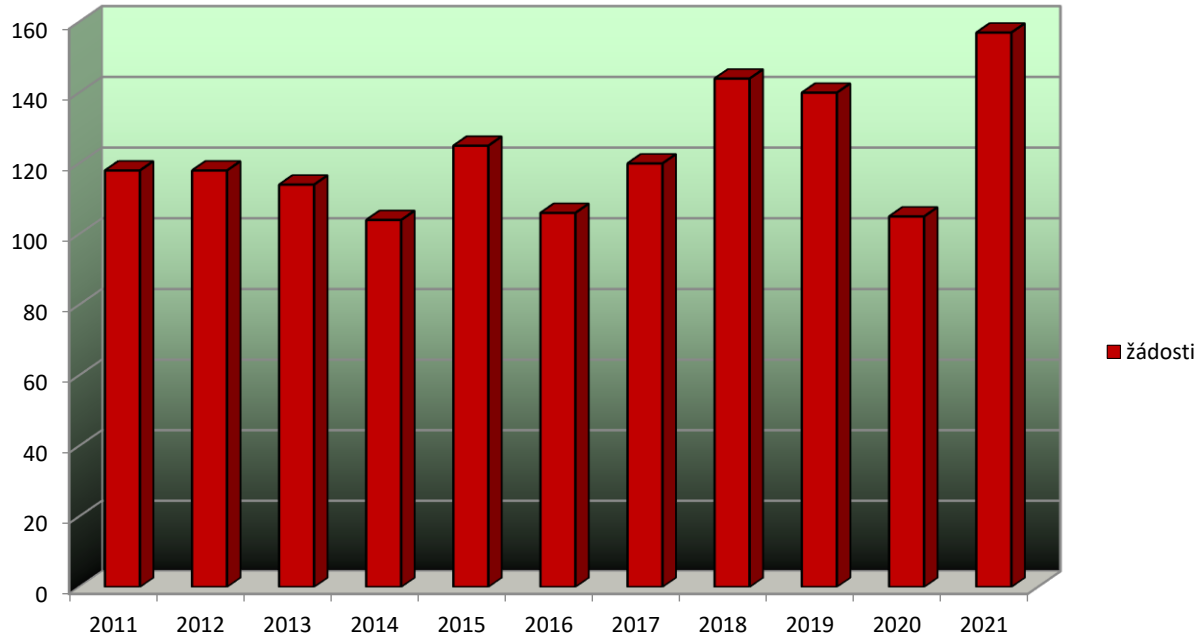
Celkem 102 certifikátů informačních systémů bylo vydáno na žádost podanou v roce 2021.

V celkem deseti případech provozovatel informačního systému s certifikátem platným do data spadajícího do roku 2021 nepožádal o opakovanou certifikaci a platnost certifikátu automaticky skončila.

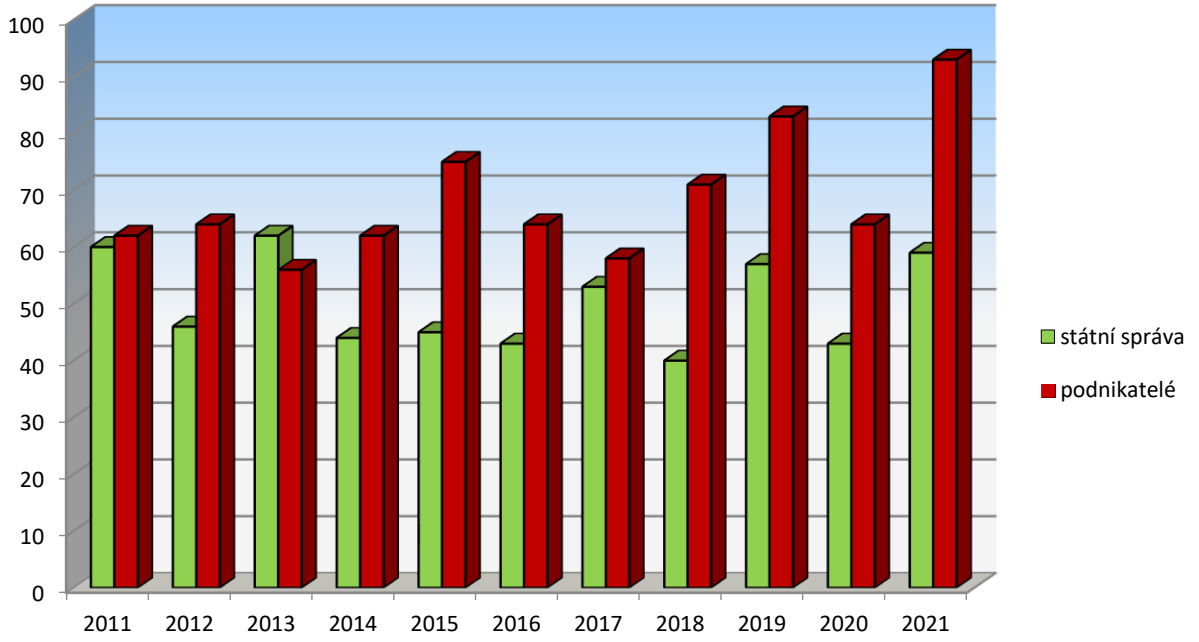
Certifikace informačních systémů v roce 2021

Řešené žádosti v roce 2021	Vydané certifikáty podle stupně utajení				Vydané certifikáty	
	Vyhrazené	Důvěrné	Tajné	Přísně tajné	státní správa	podnikatelé
207	26,30 %	45,40 %	26,30 %	2,00 %	59	93

Přijaté žádosti o certifikaci informačního systému v letech 2011 až 2021



Vydané certifikáty informačních systémů v letech 2011 až 2021



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

Lze konstatovat, že v roce 2021 přibylo šest žádostí o certifikaci nově budovaného informačního systému ze státní správy a 15 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 dva roky, stupně utajení Důvěrné nejvýše tři roky a stupně utajení Vyhrazené nejvýše pět let, 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 šest měsíců před koncem platnosti jeho certifikátu.

V roce 2021 proběhla kromě certifikace menších informačních systémů podnikatelů, několika ministerstev a úřadů (Ministerstvo financí, Ministerstvo pro místní rozvoj, Ministerstvo dopravy, Ústavní soud, Úřad vlády České republiky, Kancelář poslanecké sněmovny, Kancelář Senátu, Generální ředitelství cel, Národní bezpečnostní úřad, Česká národní banka, Vězeňská služba ČR a několik krajských a městských úřadů) opakovaná nebo nová certifikace řady rozsáhlých informačních systémů resortu MV a Policie ČR, resortu Ministerstva obrany (MO) včetně Vojenského zpravodajství (VZ), Ministerstva zahraničních věcí (MZV) a Úřadu pro zahraniční styky a informace.

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

V roce 2021 NÚKIB provedl pro resorty MO a MV národní akreditaci čtyř 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 2021 byl připravován interní normativní akt „Pracovní postup Certifikace informačního systému malého rozsahu určeného pro nakládání s utajovanými informacemi do stupně utajení Vyhrazené včetně, který sjednocuje postup certifikace informačních systémů malého rozsahu určených pro nakládání s utajovanými informacemi do stupně utajení Vyhrazené včetně. V rámci přípravy této směrnice vznikly dokumenty, které popisují celý postup certifikace včetně všech potřebných podkladů (dokumentace, vzory administrativních pomůcek, vzor žádosti, skript umožňující nastavení a kontrolu bezpečnostních atributů operačního systému). Postup má sloužit zejména pro podnikatele, kteří chtějí provozovat informační systém malého rozsahu určený pro nakládání s utajovanými informacemi do stupně utajení Vyhrazené včetně.

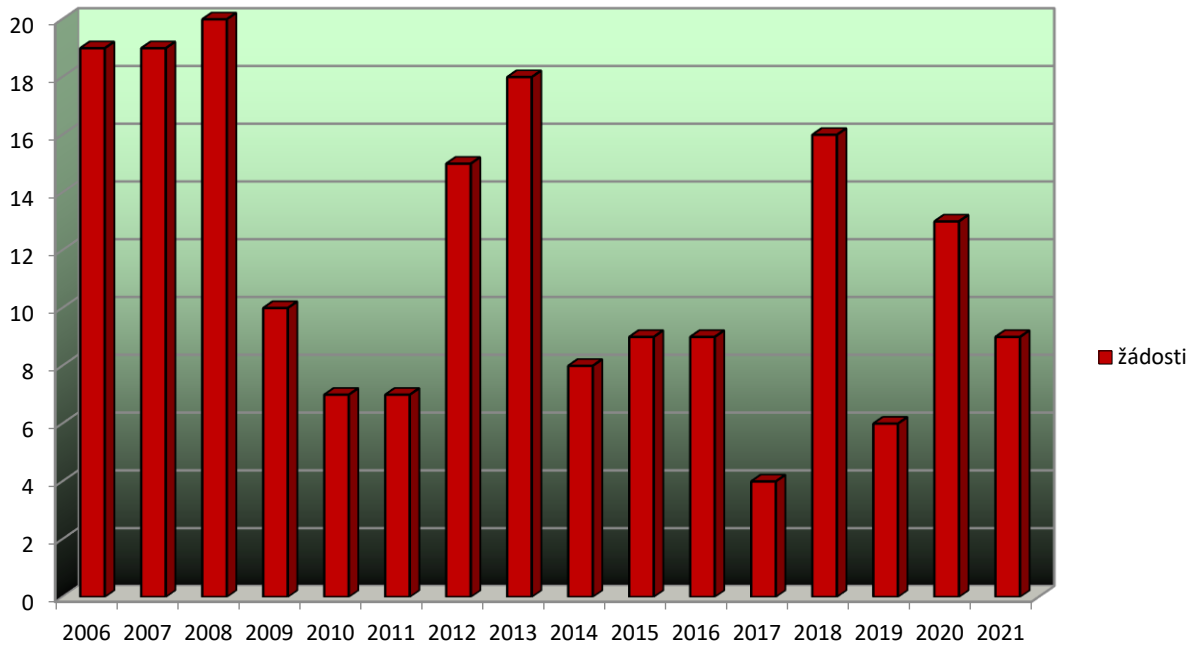
Certifikace kryptografických prostředků

V roce 2021 bylo NÚKIB podáno celkem devět žádostí o certifikaci kryptografického prostředku, z toho jedna na nový kryptografický prostředek. V řízeních k certifikaci kryptografického prostředku bylo vydáno 9 certifikátů, žádné řízení nebylo ukončeno bez vydání certifikátu. Stav řízení je shrnut v následující tabulce.

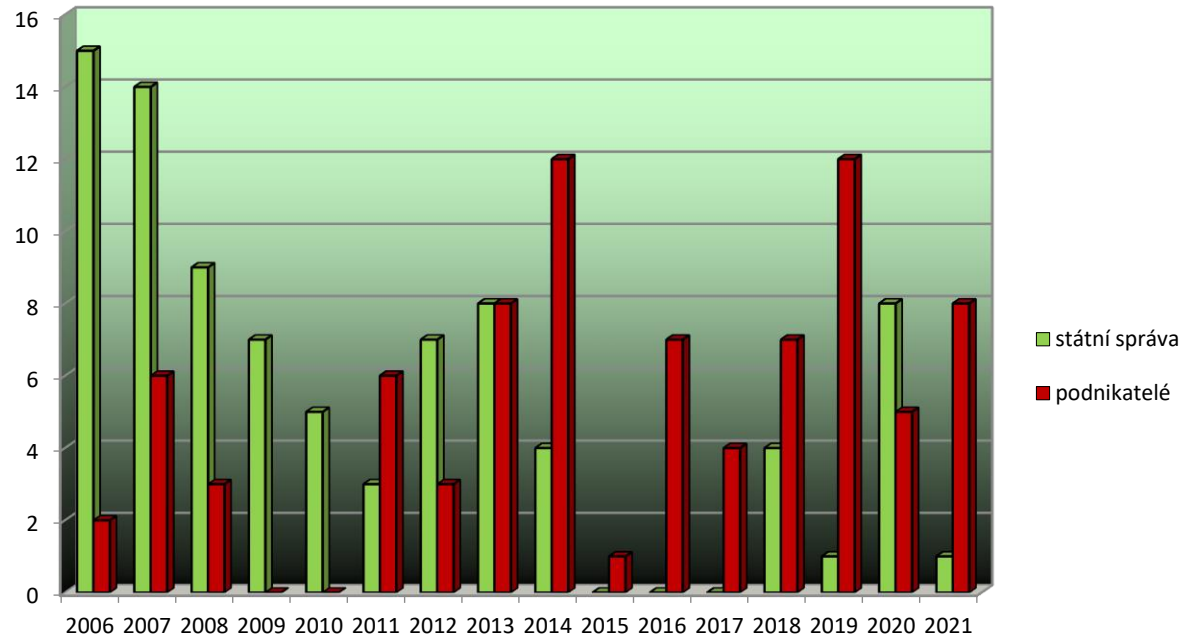
Certifikace kryptografických prostředků v roce 2021

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
9	0	0	0	0	1	8	8	5

Přijaté žádosti o certifikaci kryptografického prostředku v letech 2006 až 2021



Vydané certifikáty kryptografických prostředků v letech 2006 až 2021



Nově byl certifikován kryptografický prostředek TCE 811, ostatní žádosti se týkaly opakované certifikace. V návaznosti na dílčí změny v podmínkách provozování kryptografických prostředků současně probíhaly aktualizace příslušných certifikačních zpráv kryptografických prostředků.

Do seznamu NÚKIB materiálu „kontrolovaná kryptografická položka“ byly nově zařazeny dva kryptografické prostředky.

Schvalování projektů bezpečnosti komunikačních systémů

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

V roce 2021 byly podány dvě žádosti o schválení projektu bezpečnosti nového komunikačního systému RKS MO a Stratus MO. Projekt systému Stratus MO byl schválen, schválení projektu RKS MO proběhne v roce 2022.

Nadále byl provozován komunikační systém v Bezpečnostní informační službě (dále jen „BIS“), komunikační systém MODUS a komunikační systém RETIS.

Podporu pro provoz komunikačního systému MODUS využívajícího certifikovaných kryptografických prostředků SECTRA Tiger XS (přídavný kryptografický modul k mobilnímu telefonu), umožňujících mobilní telefonii pro utajované informace do stupně utajení Tajné, v roce 2021 nadále zajišťoval NÚKIB.

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 NÚKIB.

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

Certifikace kryptografických pracovišť

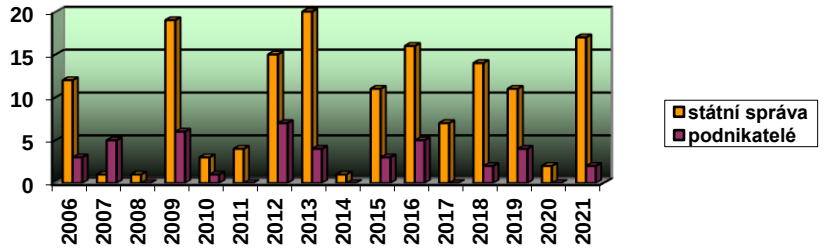
V roce 2021 bylo podáno celkem 19 žádostí o certifikaci kryptografického pracoviště. Většina žádostí o certifikaci spadá do kategorie opakovaných žádostí. Tři žádosti jsou ve stádiu posuzování. Z provedené certifikace vyplynulo, že umístění kryptografických pracovišť a provoz na nich je v souladu s reálnými potřebami příslušných organizací. V tomto rámci

ovšem dochází k rozšiřování nebo ke změnám schválených činností jednotlivých pracovišť, navýšení o další kryptografické prostředky a systémy a ke změnám jejich umístění. Všechny změny musí být předem posouzeny a schváleny NÚKIB. Stav řízení je shrnut v následující tabulce:

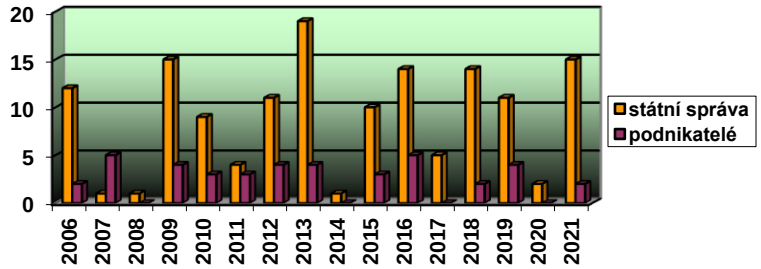
Certifikace kryptografických pracovišť v roce 2021

	Přijaté žádosti	Rozpracováno	Certifikováno	Zamítnuto	Zastaveno
Státní správa	17	3	15	0	0
Podnikatelé	2	0	2	0	0
Celkem	**19**	**3**	**17**	**0**	**0**

Přijaté žádosti o certifikaci kryptografického pracoviště v letech 2006 až 2021



Vydané certifikáty kryptografických pracovišť v letech 2006 až 2021



Další odborná činnost

Výroba kryptografického materiálu

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

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

V roce 2021 bylo v NÚKIB vygenerováno celkem 89 841 kryptografických klíčů a hesel uložených na 7 932 nosičích různých typů a dalších 35 ks jiného kryptografického materiálu (paměti, provozní dokumentace ke kryptografickým prostředkům, instalační a provozní software a firmware).

Omezené cestování, z důvodů epidemiologické situace v ČR a ve světě, omezilo v roce 2021 dovoz nakoupeného kryptografického materiálu a také přepravu kryptografických prostředků na servis v zahraničí. NÚKIB vzal do evidence a provedl distribuci celkem 700 ks nového kryptografického a CCI materiálu a dále zajistil servis a opravy na území ČR u 129 ks kryptografických prostředků a mimo ČR u 33 ks kryptografických prostředků.

NÚKIB zajistil výrobu, vzal do evidence a provedl distribuci celkem 135 ks kryptografického materiálu EU.

Dále NÚKIB zajistil pro tři pracovníky z Oddělení šifrové služby ve Francii školení na obsluhu zařízení Black Box Key Management Equipment (dále jen „BBKME“) a pro toto zařízení zpracoval provozní dokumentaci „Návod pro používání BBKME“ a „Pravidla pro používání BBKME“. Pro možnost komunikace v utajované síti SPIDER, kterou provozuje Agentura pro evropský globální navigační satelitní systém (dále jen „EUSPA“) pomocí software kryptografického prostředku Filkrypto, zajistil NÚKIB nákup software kryptografického prostředku Filkrypto a zpracoval provozní dokumentaci „Pravidla pro používání Filkrypto“ a „Rychlý návod pro používání Filkrypto“. Nadále NÚKIB zajišťoval speciální balení a distribuci kryptografického materiálu, vedení ústřední evidence certifikovaných kryptografických prostředků provozovaných u orgánů státu, jakož i centrální databáze pracovníků

kryptografické ochrany, pracovníků provozních obsluh kryptografického prostředku a kurýrů kryptografického materiálu v působnosti NÚKIB.

Měření kompromitujícího vyzařování (TEMPEST)

TEMPEST měření elektronických zařízení

NÚKIB prováděl v roce 2021 TEMPEST měření podle standardů NATO řady SDIP, EU řady IASG 7 a podle metodiky bezpečnostních standardů NBÚ. Objektem měření byla především zařízení orgánů státu. Jednalo se jak o měření komerčních zařízení (většinou pro účely výběrových řízení), tak speciálních informačních systémů (zejména vojenských).

Celkem bylo v roce 2021 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. ÚVČR, MZV, MO, MV, MPO, zpravodajské služby aj.), nebo pro podnikatele. Z celkového počtu hodnocených zařízení byla většina vyžádána Ministerstvem obrany. Bylo provedeno měření a hodnocení pro Ured vlade Republike Slovenike za varovanje tajnih podatkov.

Zónové měření, instalační záznamy, obranné prohlídky

NÚKIB dále prováděl ohodnocování prostorů metodou zónového měření. Jednalo se o prostory, ve kterých se nacházela zařízení zpracovávající utajované informace. Tento druh měření byl především použit u objektů NÚKIB, BIS, MO a MV. Další zónová měření byla prováděna pro státní správu i pro soukromé subjekty v rámci certifikace informačních systémů. Prováděno bylo rovněž zónové hodnocení prostorů na základě podkladů dodaných akreditovanými pracovišti MO, BIS a VZ.

Bylo provedeno hodnocení instalace informačních systémů zpracovávajících utajované informace stupně utajení Důvěrné a Tajné a v rámci certifikace těchto systémů byly zpracovány instalační záznamy z více než 20 lokalit. Dále byly posouzeny instalační záznamy z akreditovaných pracovišť (MO, BIS, VZ, MV).

V roce 2021 byly provedeny obranné prohlídky v několika objektech v ČR i 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 2021 je uveden v následující tabulce.

Měřená zařízení a objekty v roce 2021

Typ měření[2]	Počet
Zónové měření	8 lokalit
Kryptografické prostředky	2 typy
Komponenty ICT	41 systémů
Audiotechnika	2 typy zařízení
Obranné prohlídky i v rámci certifikace IS	10 objektů
Mobilní systémy	8 systémů
Instalační záznamy	> 20 lokalit
Stínicí komory	27 certifikátů

Školení pracovníků kryptografické ochrany a zkoušky odborné způsobilosti

V roce 2021 nadále platila opatření vlády související s COVID-19, která značně omezovala činnosti spojené s prováděním zkoušky zvláštní odborné způsobilosti pracovníků kryptografické ochrany. Proto NÚKIB prodloužil možnost, aby u pracovníků kryptografické ochrany, kterým platnost osvědčení o zvláštní odborné způsobilosti skončila, byla tato doba platnosti osvědčení na nezbytně nutnou dobu prodloužena.

NÚKIB v roce 2021 v rámci ČR organizačně zajistil a uskutečnil celkem 14 školení pro pracovníky kryptografické ochrany a po úspěšné zkoušce vydal 124 osvědčení o zvláštní odborné způsobilosti pracovníka kryptografické ochrany. Dále provedl pro pracovníky, kteří se budou

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

seznamovat s informacemi z oblasti COMSEC EU poučení a vydal jim 14 Crypto Authorisation. Současně provedl zaškolení pracovníka provozní obsluhy a vydal jedno potvrzení o odborném zaškolení pracovníka provozní obsluhy kryptografického prostředku. Školení, která jsou v neutajovaném režimu, proběhla také korespondenční formou.

V roce 2021 byla provedena aktualizace rozsahu (z hlediska typů kryptografických prostředků) smlouvy k provádění odborné zkoušky a vydávání osvědčení o zvláštní odborné způsobilosti pracovníků kryptografické ochrany uzavřené mezi NÚKIB a MO. Dále byla provedena aktualizace rozsahu (z hlediska typů kryptografických prostředků) smlouvy o zajištění činnosti k provádění části zkoušky zvláštní odborné způsobilosti pracovníka kryptografické ochrany a vydávání potvrzení o jejím absolvování uzavřené mezi NÚKIB a S.ICZ a.s.

Kontroly ochrany utajovaných informací (státní dozor)

V roce 2021 provedl NÚKIB ve smyslu § 143 odst. 6 zákona o ochraně utajovaných informací 17 kontrol v oblasti bezpečnosti informačních nebo komunikačních systémů, případně kryptografické ochrany. Z tohoto počtu byly tři kontroly provedeny v rámci státní správy a 14 kontrol u podnikatelů.

Oblasti bezpečnosti informačních a komunikačních systémů a kryptografické ochrany

Zákonem stanovené činnosti NÚKIB v oblasti bezpečnosti informačních systémů nakládajících s utajovanými informacemi a kryptografické ochrany byly v roce 2021 zajištěny.

- Stálou výzvou je rychlý rozvoj ICT a s ním spjaté bezpečnostní problémy. Některé nové technologie nelze nasadit bez jejich důkladného testování, anebo bez podkladů vzniklých jejich kvalifikovaným hodnocením z hlediska bezpečnosti podle uznávaných mezinárodních kritérií. Zároveň mají subjekty vedoucí útoky proti důvěrnosti, integritě a dostupnosti utajovaných nebo citlivých informací k dispozici stále sofistikovanější nástroje. Informace o skrytých zranitelnostech ICT produktů jsou obtížně dosažitelné a jejich objevení zpravidla vyžaduje vysoce nadstandardní technické vybavení.
- V oblasti certifikace informačních systémů, kryptografických prostředků a pracovišť jsou pracovní místa v NÚKIB aktuálně přidělená pro tyto činnosti kvalitně obsazena. Vzhledem k malému počtu pracovníků, kteří řeší jednotlivá certifikační řízení, má výpadek každého

pracovníka (mateřská dovolená, dlouhodobé onemocnění, odchod pracovníka) znatelný vliv na již tak vysoké pracovní vytížení odborných pracovníků. Nová pracovní místa jsou potřebná rovněž pro testování bezpečnostních technologií a analýzu rizik pro informační a komunikační systémy.

- V oblasti kryptologie je získání nových odborníků obtížné, neboť se jedná o specializované činnosti, které jsou v soukromé sféře vyhledávané. Pro tyto pozice v NÚKIB je vyžadována bezpečnostní prověrka pro přístup k utajovaným informacím stupně utajení Tajné nebo Přísně tajné.
- 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, zejména u mobilních komunikací. Vývoj národních kryptografických prostředků probíhá v podmínkách odborných pracovišť NÚKIB a ve spolupráci se specializovanými subjekty ze soukromého sektoru v rámci externích vývojových projektů. Vzhledem k 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 NÚKIB (tedy státu). Zájem privátních subjektů také negativně ovlivňuje malý národní trh kryptografických prostředků (počty kusů kryptografických prostředků uplatnitelných v ČR).
- Z hlediska zajištění praktické ochrany utajovaných informací v informačních nebo komunikačních systémech a zajištění kryptografické ochrany všeobecně ve státní správě je potřebné také personální posílení pracoviště NÚKIB zajišťujícího výrobu, evidenci a distribuci kryptografického materiálu národního a EU v ČR. V rámci resortů je třeba mít stále na zřeteli nedostatek odborníků v oboru informačních technologií a kryptografické ochrany, kteří by zároveň splňovali podmínky pro přístup fyzické osoby k utajované informaci stupně utajení Důvěrné, Tajné nebo Přísně tajné. Stabilizované obsazení pracovních míst je potřebné zejména v případě pracovníků ve výkonu kryptografické ochrany.

Výzkumná a vývojová činnost NÚKIB v oblasti ochrany utajovaných informací

Cíle a organizace výzkumu a vývoje

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

Projekty realizované v roce 2021

V roce 2021 NÚKIB zajišťoval vývoj na základě schváleného Výzkumného záměru vědy a výzkumu, zpracoval výzkumnou zprávu a dále rozvíjel výzkum a vývoj v oblasti kryptografické ochrany a ochrany proti úniku utajovaných informací kompromitujícím vyzařováním tak, aby mimo jiné reflektoval požadavky resortů státní správy, pro které jsou tyto druhy ochrany utajovaných informací nezbytné.

NÚKIB vývojové projekty realizoval na základě zjištěných poznatků při spolupráci s orgány státu, z informací získaných pilotním testování kryptografických prostředků, z certifikační a konzultační činnosti se zástupci orgánů státní správy a při výkonu státního dozoru.

Některé realizované projekty navazovaly na projekty řešené v minulých letech. Důvodem této skutečnosti je již výše zmíněný rychlý technologický pokrok, kvůli němuž je nutné neustále reagovat na změny komunikačního i technologického prostředí, rozvíjet a inovovat již vyvinuté produkty, případně vyvíjet nové prostředky.

V rámci odborného pracoviště Oddělení kryptologie a vývoje kryptografických prostředků/Odbor bezpečnosti informačních a komunikačních technologií – byly v roce 2021 úspěšně realizovány vývojové projekty hlasových komunikátorů: Studie proveditelnosti – demonstrátor iSaCom, Studie proveditelnosti – demonstrátor OSK a SaCom pro verzi OS Android 11/2021. Dále byl realizován projekt výzkumu technologií GNZ a projekt výzkumu Biometrických senzorů mobilních telefonů. Uvedené projekty byly realizovány na základě smluv o dílo ve spolupráci s externími řešiteli. Návazně na odborném pracovišti NÚKIB probíhal interní aplikovaný vývoj a testování výsledků výše zmíněných hardware projektů a také interní

vývoj bezpečnostního software. V předmětných oblastech také probíhalo pilotní nasazení a testování osobních KP a chráněné národní mobilní komunikace. Pozitivní výsledky výše zmíněných projektů ukázaly potenciál národního vývoje kryptografických prostředků při naplnění strategických plánů NÚKIB.

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

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

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

V rámci odborného pracoviště Oddělení TEMPEST (dále jen „OT OBIT“) byly v roce 2021 zahájeny projekty týkající se měření kompromitujícího vyzařování na radiových vysílačích (202101) a zaměřování rušících signálů v pásmech GNSS (202104). V roce 2021 dále pokračoval projekt týkající se měření akustických signálů šířených po konstrukcích budov (202001). OT se podílel jako aplikační garant na projektu týkajícího se rizik použití optických vláken (řešitel VUT Brno). V roce 2021 byly zahájeny administrativní práce nutné k řešení projektu zónových měření (v rámci projektů MV).

Přehled zahraničních pracovních cest za rok 2021

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

V důsledku COVID-19 pandemie probíhala v roce 2021 jednání CIS3 Partnerství pouze virtuálně. Partnerství je unikátní společenství dnes 13 států NATO skládající se z příslušných

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, a také o vývoji interoperabilních kryptografických prostředků.

EUROCRYPT 2021 (virtuálně)

Každoroční konference k získání aktuálních poznatků v kryptologii.

MILIPO 2021

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. (Paříž, Francie)

Pracovní návštěva na NSA Albánie

Na žádost albánské strany se uskutečnilo několik pracovních jednání týkajících se oblasti měření kompromitujících signálů, hodnocení prostorů, v kterých dochází ke zpracovávání utajovaných informací, bezpečnostních standardů NATO a přístupu NÚKIB k ochraně národních a NATO utajovaných informací.

ICMC 2021 (virtuálně)

ICMC je významnou odbornou akcí zaměřenou na řešení aktuálních problémů vývoje, testování a provozování kryptografických modulů s důrazem na aplikaci příslušných standardů. V roce 2021 se tato akce konala začátkem září a hodně se věnovala standardu FIPS 140-3 a obecně PQC.

Bar Ilan Winterschool 2021 (virtuálně)

Zimní škola informačně-teoretické kryptografie. Konala se v únoru 2021 formou online přenosu z Tel Avivu, Izrael.

MKB 2021 (prezenčně)

Významná konference pořádaná každý rok, kde se setkává česká a slovenská kryptologická scéna. Konference se v roce 2021 konala v září.

Cyber Week 2021 (virtuálně)

V roce 2021 byly tématy konference PQC a kryptografie na mřížkách. Konference se konala v červenci v Tel Avivu.

Matematická kryptologie a kvantové technologie relevantní pro bezpečnost informací

Matematická kryptologie pro podporu vývoje a hodnocení bezpečnosti národních kryptografických prostředků

NÚKIB zajišťuje expertní analytickou podporu pro vývoj národních kryptografických prostředků a pro jejich hodnocení. V oblasti matematické kryptologie provádí zejména činnosti v oblasti vývoje a analýz bezpečnosti a efektivnosti kryptografických algoritmů. Od roku 2018 jsou tyto analýzy zaměřeny zejména na analýzy algoritmů vhodných pro zajištění odolnosti kryptografických prostředků proti kvantové hrozbě, zejména algoritmů post-kvantové kryptografie a kryptografických protokolů, které umožňují její začlenění. V této souvislosti NÚKIB připravil a řídil projekt, jehož náplní bylo zajištění odolnosti kryptografického prostředku proti kvantové hrozbě na bázi post-kvantové kryptografie.

NÚKIB se průběžně zabývá problematikou software nástrojů pro hodnocení kryptografické bezpečnosti, přičemž tyto nástroje NÚKIB využil i při hodnocení bezpečnosti kryptografických protokolů navržených pro začlenění post-kvantové kryptografie. Kromě těchto oblastí se NÚKIB v minulém roce blíže zabýval dokazatelnou bezpečností kryptografických schémat v modelu náhodného orákula a dále problematikou tzv. nefyzikálních náhodných generátorů, zejména v prostředích Windows a Linux.

Dále NÚKIB připravil a řídí projekty, jejichž cílem je realizace mechanismu bezpečné vzdálené výměny FW kryptografického prostředku a získání znalostní báze umožňující posuzovat bezpečnostní vlastnosti obdobných mechanismů.

Expertní a hodnotitelská činnost

NÚKIB hraje v projektech IMPAKT roli aplikačního garanta. V roce 2021 se podílel formou konzultací na přípravě obsahu projektu IMPAKT zaměřeného na využití software nástrojů a umělé inteligence při hodnocení kryptografických implementací a dále poskytoval odbornou zpětnou vazbu v projektu NESPOQ, pro který mimo jiné analyzoval možnosti volby funkce pro hybridní kombinaci post-kvantově a kvantově ustanovených klíčů.

V rámci Security Group Euro QCI se NÚKIB zúčastnil konzultací bezpečnostních aspektů budování evropské kvantové infrastruktury na bázi kvantové distribuce klíčů (dále jen „QKD“). Mimo jiné poskytl doporučení možností volby funkce pro odvozování klíčů pro případy příliš pomalého ustanovování QKD klíčů.

Spolupráce s akademickou obcí

V roce 2021 zajišťovali pracovníci NÚKIB sérii seminářů: „Modelování kryptografické bezpečnosti“ (součást předmětu „Modelování bezpečnosti“) na MFF UK a pro studenty FJFI ČVUT prezentovali veřejně dostupnou přednášku: „Principy a realita kryptografické bezpečnosti“.

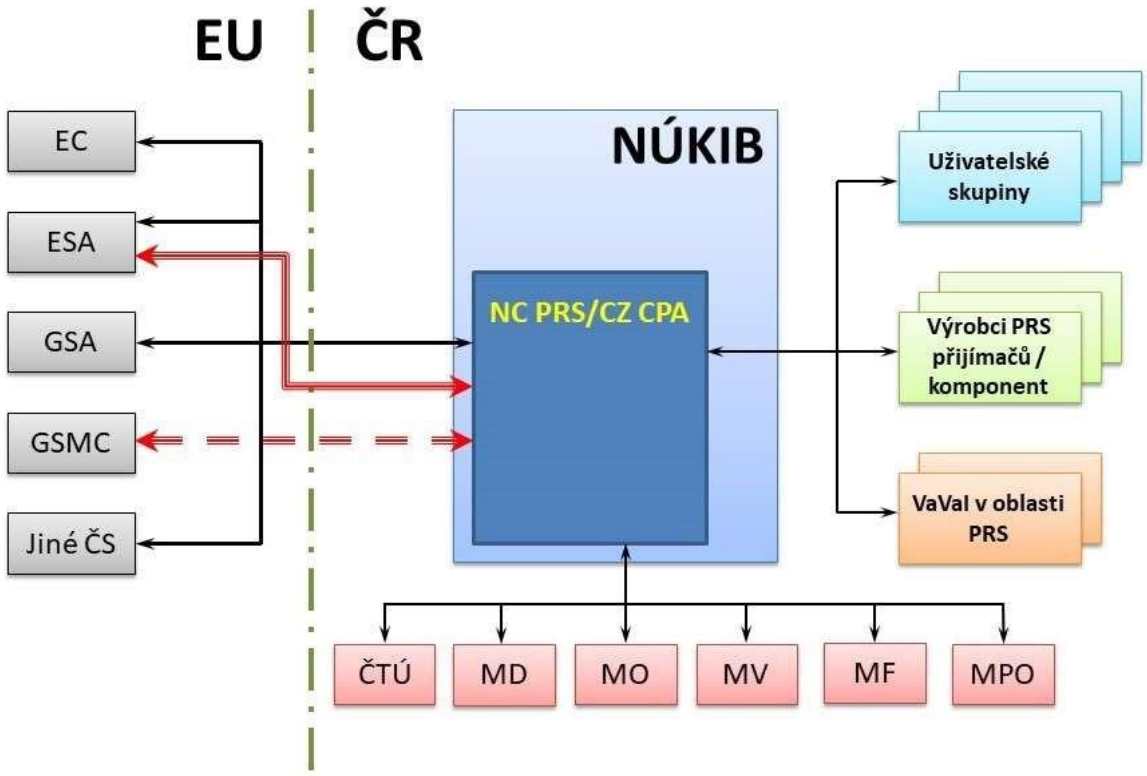
Výkon funkce příslušného orgánu PRS

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 resortu MD na NÚKIB. Ředitel NÚKIB byl, v souladu s čl. 5 Rozhodnutí Evropského Parlamentu a Rady č. 1104/2011/EU ze dne 25. října 2011, o podmínkách přístupu ke službě PRS nabízené globálním navigačním družicovým systémem na základě programu Galileo, pověřen výkonem funkce Příslušného orgánu PRS (Competent PRS Authority, dále jen „CPA“).

Budování národního centra PRS

Implementace služby PRS v ČR probíhá na základě schváleného Akčního plánu implementace PRS v ČR. V souladu se schváleným finančním rámcem a personálními opatřeními NÚKIB pokračuje v budování Národního centra PRS (dále jen „NCPRS“), které je zodpovědné

za organizační zabezpečení přístupu ke službě PRS a za výkon funkce CPA. Organizační schéma zabezpečení služby PRS v ČR je zobrazeno na následujícím obrázku.



Koncem roku 2021 byly zahájeny práce na aktualizaci Akčního plánu implementace PRS v ČR, který má zohlednit aktuální poznatky a potřeby související s implementací PRS pro dosažení počátečních a následně i plných operačních schopností. Aktuální informace byly získány aktivní účastí a zastupováním ČR na jednáních pracovních skupin EU pro řešení problematiky bezpečnosti programu Galileo a PRS, což představovalo i v roce 2021 jednu z důležitých činností, kterou vykonávalo NCPRS. Získané informace umožní již v předstihu realizovat potřebná a nutná opatření, která umožní využití technologie GNSS pro kritické aplikace vyžadující garantovaný přístup k polohovým a časovým službám poskytovaných systémem Galileo. Vzhledem k nepříznivé epidemiologické situaci v EU v souvislosti s COVID-19 se většina jednání uskutečnila v limitovaném online formátu. Jednání v režimu utajení probíhala prostřednictvím akreditovaného komunikačního systému, který umožňuje výměnu utajovaných informací a v omezeném formátu i projednávání utajovaných informací agendy bezpečnostní akreditace a PRS. Těchto jednání se ovšem zúčastňoval omezený počet členských států, ve kterých byla tato technologie již instalována, což negativně ovlivnilo proces schvalování klíčových dokumentů.

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 2021 se mělo NCPRS podílet na realizaci mezinárodní spolupráce pro testování služby PRS v rámci projektu společného testování „Joint Test Activities“ vyhlášeného Agenturou pro evropský GNSS. Z důvodů restrikcí souvisejících s platnými epidemiologickými opatřeními k zamezení šíření COVID-19 nebyl tento projekt v roce 2021 realizován a časový harmonogram pro uskutečnění projektu byl prodloužen. Testy na území ČR proběhnou až v průběhu roku 2022, kdy má být tento projekt ukončen.

Zástupci NCPRS se i v roce 2021 účastnili pravidelných setkání CPA členských států EU, jejichž hlavním cílem byla diskuse ohledně stavu a pokračování implementace PRS v členských státech EU, koordinace společného postupu při jednání s Evropskou komisí a vzájemná výměna zkušeností. Proběhlo i bilaterální jednání se zástupci slovenského CPA, jehož cílem byla výměna informací ohledně budování počátečních operačních schopností PRS a posílení vzájemné spolupráce v oblasti národních strategií bezpečnostní správy provozu a implementace PRS.

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

Bohužel se ani v roce 2021 nepodařilo navýšit personální obsazení Odboru PRS. Tato situace představuje vzhledem k očekávanému nárůstu agendy spojenému s transformací a rozšířením Agentury pro evropský GNSS na Agenturu Evropské unie pro kosmický program a blížícímu

se předsednictvím ČR v Radě EU problém, který bude muset být v nejbližším období řešen. Vzhledem k nedostupnosti personálu s požadovanou kvalifikací, bude muset NÚKIB patrně přistoupit i k náboru ne zcela kvalifikovaného personálu a následnému zaškolení.

Spolupráce s ostatními subjekty při implementaci PRS

NCPRS úzce spolupracuje při řešení problematiky PRS zejména s MD, které plní úlohu hlavního koordinátora pro správu a řízení národních aktivit souvisejících s evropským kosmickým programem. V roce 2021 i nadále pokračovala spolupráce s MO, zejména v oblasti přípravy a zapojení do realizace připravovaných scénářů projektu společného testování PRS a také z důvodu plánovaného využití PRS AČR.

Odbor vzdělávání, výzkumu a projektů

Vzdělávání a osvěta v kybernetické bezpečnosti

Stejně jako v roce 2020 i v roce 2021 se NÚKIB zaměřoval na vzdělávání zaměstnanců veřejné správy, zdravotnického personálu a na vzdělávání svých cílových skupin (pedagogové, pracovníci prevence, žáci základních a středních škol). Ke vzdělávání všech skupin byly v maximální míře využívány online e-learningové kurzy zveřejněné na vzdělávacím portálu NÚKIB (osveta.nukib.cz).

Byla ukončena spolupráce s Institutem pro veřejnou správu Praha, který zajišťoval studium ve vybraných kurzech NÚKIB. Nově NÚKIB poskytuje všechny online e-learningové kurzy vlastní produkce bez dalších prostředníků.

NÚKIB v roce 2021 rozšířil nabídku na **13 kurzů** zaměřených na různé cílové skupiny. Mezi základní kurzy NÚKIB patří zejména tyto:

1. Základy kybernetické bezpečnosti (Dávej kyber!)
2. Kurz pro manažery kybernetické bezpečnosti (Šéfuj kyber!)
3. Kurz základů rizikového chování (Bezpečně v kyber!)

Kurz „Dávej kyber!“ je využívaný jako primární vzdělávací aktivita pro vzdělávání zaměstnanců veřejné správy a představuje základy kybernetické bezpečnosti pro běžného uživatele. Ke konci roku 2021 jej absolvovalo **20 546 uživatelů**. Tento kurz je od roku 2021 nabízen

i v akreditované verzi podle § 30 zákona č. 312/2002 Sb., o úřednících územních samosprávných celků a o změně některých zákonů, ve znění pozdějších předpisů. Kurz dobrovolně absolvovali také členové některých profesních sdružení a zástupci firem soukromého sektoru. Stejně jako v roce 2020, je ponechána možnost absolvování kurzu ze strany široké veřejnosti a je možné jej absolvovat v režimu bez přihlášení (podobně jako u dalších kurzů NÚKIB). Počet zobrazení od neregistrovaných uživatelů u tohoto kurzu dosáhl **498 561 zobrazení**.

Odborný **kurz „Šéfuj kyber“**, který je určen především manažerům kybernetické bezpečnosti a dalším bezpečnostním rolím podle vyhlášky č. 82/2018 Sb., (dále jen „vyhláška o kybernetické bezpečnosti) úspěšně absolvovalo **374 zájemců**. Kurz je přístupný jako otevřená učebnice a slouží jako pomůcka pro aplikaci požadavků vyhlášky o kybernetické bezpečnosti v praxi. Díky tomu dosáhl tento kurz **18 569 zobrazení** nepřihlášenými uživateli. I tento kurz je nově nabízen také v akreditované verzi podle § 30 zákona č. 312/2002 Sb., o úřednících územních samosprávných celků a o změně některých zákonů, ve znění pozdějších předpisů.

Odborné vzdělávání s preventivním přesahem zajišťuje NÚKIB prostřednictvím e-learningového **kurzu „Bezpečně v kyber“**, který absolvovalo **2 848 pracovníků prevence** a počet zobrazení nepřihlášenými uživateli dosáhl hranice **192 300.** Odborný kurz seznamuje pracovníky prevence se sociálními tématy kybernetické bezpečnosti, jako je například kyberšikana, a je k dispozici ve dvou verzích. Základní verze seznamuje zájemce s úvodem do problematiky rizikových jevů v kyberprostoru. Rozšířená verze pak umožňuje proniknout do problematiky ve větší hloubce, v širších souvislostech a s tematicky bohatším obsahem.

NÚKIB v reakci na kybernetické útoky zaměřené na sektor zdravotnictví připravil kurz Základy kybernetické bezpečnosti pro nemocnice a zdravotnická zařízení, který je upravený speciálně pro toto prostředí. Tento kurz byl zveřejněn na jaře 2021 a do konce roku jím prošlo **4 892 pracovníků** ze sektoru zdravotnictví.

V rámci šíření osvěty mezi dětmi a mládeží NÚKIB v roce 2021 nabízel i své vlastní nástroje pro jejich vzdělávání, které mohou využít učitelé ve výuce od mateřské po střední školu. Jedná se například o interaktivní příběh Vanda a Eda v Onl@jn světě, který měl přes **11 100 zobrazení**, interaktivní komiks Digistopa: Příběh Svůďáka, který zaznamenal **76 500 zobrazení,** a komiks Digistopa: Příběh Báry, u kterého je zaznamenáno **177 000 zobrazení**. Aktivita pro starší žáky s názvem „Jsem netvor, tvor, který žije na netu“ byla zobrazena **105 000x**. NÚKIB tyto aktivity

také propagoval. V lednu 2021 byly aktivity rozposlány přes informační systémy škol Bakaláři a Škola Online. V součtu se **podařilo oslovit 4 710 českých škol a 279 000 unikátních uživatelů**.[3]

NÚKIB se také tradičně zapojil do **Dne bezpečnějšího internetu (Safer Internet Day)**, který v České republice koordinuje sdružení CZ.NIC, konkrétně do jeho projektu Bezpečně na netu.[4] Propagoval výše uvedené aktivity. NÚKIB byl také **součástí Evropského měsíce kybernetické bezpečnosti (ECSM)**, pro který připravil sérii speciálních osvětových příspěvků na instagramovém účtu @petr.vytrzny.[5]

V průběhu roku 2021 byl zprovozněn **rozcestník vzdělávacích a osvětových aktivit NÚKIB**, kde zejména pedagogové a pracovníci prevence najdou inspiraci a metodickou pomoc pro výuku.[6]

Všechny kurzy z produkce NÚKIB jsou standartně přístupné nejenom cílovým skupinám, ale celé veřejnosti a lze je v rámci lepšího šíření osvěty procházet i bez registrace. Jejich reálný dopad na zvyšování povědomí o kybernetických hrozbách a zvyšování odolnosti společnosti je tak mnohem vyšší, než napovídají počty absolventů, kteří jako registrovaní obdrželi certifikáty. Z pozice garanta oblasti kybernetické bezpečnosti koncipujeme naše kurzy formou online příručky, kterou je možné kdykoliv využít.

NÚKIB se podílel i na osvětových akcích s jinými ústředními orgány státní správy. Například společně s Ministerstvem školství, mládeže a tělovýchovy (dále jen „MŠMT“) pořádal online panelovou diskusi „Digitalizace vzdělávání a kybernetické bezpečnosti“[7] a další panelovou diskusi k otázkám kyberbezpečnosti ve vzdělávání. Cílem bylo podpořit řešení aktuálních problémů, které vyvstávají především v souvislosti s distanční online výukou a kyberbezpečností ve vzdělávání. Účastníci panelových diskusí se zabývali například otázkami, jak bezpečně vyučovat na dálku, jak efektivně eliminovat rizika při používání digitálních technologií, kam směřovat pozornost a obezřetnost rodičů i dětí při každodenním virtuálním školním i mimoškolním setkávání.

3 https://www.nukib.cz/cs/infoservis/aktuality/1678-nukib-distribuoval-vyukove-materialy/
4 https://www.nukib.cz/cs/infoservis/aktuality/1686-nukib-se-opet-zapoji-do-osvetovych-aktivit-v-ramci-dne-bezpecnejsiho-internetu/
5 https://www.nukib.cz/cs/infoservis/aktuality/1753-jsme-soucasti-evropskeho-mesice-kyberneticke-bezpecnosti-2021/
6 https://osveta.nukib.cz/course/view.php?id=105
7 https://www.nukib.cz/cs/infoservis/aktuality/1700-digitalizace-vzdelavani-a-kyberneticke-bezpecnosti/

Díky nepříznivé epidemiologické situaci v České republice v roce 2021 nebyl organizován Festival bezpečného internetu, který je hlavní osvětovou událostí NÚKIB v oblasti kybernetické bezpečnosti.

Vedle hlavních vzdělávacích produktů NÚKIB také vydal řadu podpůrných materiálů včetně článků a další publikační činnosti. Jednalo se například o odborný článek „K vybraným otázkám výuky kybernetické bezpečnosti“[8] nebo články pro Svaz měst a obcí. Jednou z doplňkových činností byla také průběžná přednášková činnost.

V červnu roku 2021 se NÚKIB ve spolupráci s MV, Národní agenturou pro komunikační a informační technologie (dále jen „NAKIT“), AFCEA a dalšími partnery podílel na vytvoření „Doporučení pro bezpečné nakládání s e-identitou“, kde mimo jiné NÚKIB připravil přehledový diagram „Stávající prostředky pro e-identitu“. Cílem této spolupráce bylo pomoct široké veřejnosti zorientovat se v problematice eGovernmentu.

Výzkum a evropská spolupráce

NÚKIB se v roli aplikačního garanta zapojil do řešení několika výzkumných projektů financovaných z programů „Strategická podpora rozvoje bezpečnostního výzkumu ČR 2019-2025“ a „Bezpečnostní výzkum 2021-2026: vývoj, testování a evaluace nových bezpečnostních technologií“ MV. Příklady podpořených projektů jsou vytvoření testovacího prostředí pro výzkum a vývoj kyberbezpečnostních technologií využívajících umělou inteligenci či výzkum nástrojů pro verifikaci bezpečnosti kryptografických zařízení s využitím umělé inteligence.

V oblasti společně prováděného výzkumu a vývoje v oblasti 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.

NÚKIB v roce 2021 podnikal potřebné kroky pro zajištění implementace Aktu o kybernetické bezpečnosti do českého právního řádu v oblasti EU certifikací kybernetické bezpečnosti.

8 https://clanky.rvp.cz/clanek/c/Z/22993/K-VYBRANYM-OTAZKAM-VYUKY-KYBERNETICKE-BEZPECNOSTI.html

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 pokračoval v organizaci pravidelného setkání pro partnery s cílem informovat je o evropském rámci pro certifikaci kybernetické bezpečnosti. Současně se NÚKIB aktivně podílel na činnosti Evropské skupiny pro certifikaci kybernetické bezpečnosti a také působil v ad-hoc working groups agentury ENISA pro návrh certifikačních systémů EUCC (Common Criteria based European candidate cybersecurity certification scheme) a EUCS (European Union Cybersecurity Certification Scheme on Cloud Services).

Na základě nařízení Evropského parlamentu a Rady č. 887/2021 bylo v ČR vytvořeno Národní koordinační centrum kybernetického výzkumu a vývoje (dále jen „NKC“). Entitou zaštiťující činnost NKC je NÚKIB. Zástupci NÚKIB se pravidelně aktivně účastní jednání správní rady Evropského kompetenčního centra, které činnost jednotlivých NKC zastřešuje; přispívají k formulovaní politik a priorit kybernetického výzkumu a vývoje na evropské úrovni; a slouží jako hlavní bod komunikace mezi orgány EU (Evropská komise, Evropské kompetenční centrum, ENISA) a národní výzkumnou komunitou v dané oblasti.

Na národní úrovni NÚKIB zastřešuje činnost Platformy pro výzkum a vývoj v kybernetické bezpečnosti, jejímiž členy jsou orgány státní správy, akademické a výzkumné instituce a zástupci soukromého sektoru. Cílem platformy je sdílet napříč jednotlivými sektory informace o vývoji v oblasti kybernetické bezpečnosti, stávajících a nových trendech a výzvách (například kvantum a post-kvantum, umělá inteligence, vzdělávání atd.) a rovněž o možnostech posílení spolupráce mezi institucemi na národní i mezinárodní úrovni včetně zapojení do evropských programů. Platforma byla vytvořena v první polovině roku 2021; doposud proběhla dvě expertní jednání.

Přínos Projektové kanceláře NÚKIB pro zajištění kybernetické bezpečnosti

Přínosu pro zajištění kybernetické bezpečnosti dosahujeme mj. pomocí projektového řízení, které aplikujeme zpravidla u komplexních a složitých záměrů se strategickým dopadem.

Zdrojem podnětů je Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2021 až 2025, Koncepce rozvoje NÚKIB a další relevantní strategické dokumenty. Oddělení projektového řízení („Projektová kancelář“) zajišťuje přímé řízení některých projektů organizace, stejně jako integraci celého systému projektového řízení. Pracoviště vykonává celou paletu služeb (podrobnosti na oficiálním webu NÚKIB), zde popisujeme výsledky vybraných z nich:

Portfolio management, strategická koordinace

- V průběhu roku 2021 jsme implementovali a nově využíváme vybrané nástroje portfolio managementu, které organizaci umožňují racionalizovat řízení projektů a programů ve vzájemných souvislostech (časové, technologické, kapacitní ad.).
- Na základě iniciativy MV jsme byli nadále zapojeni do hodnocení projektů v oblasti kybernetické bezpečnosti z programu Digitálního Česka – ze strategického hlediska.
- Společně s partnery z projektových kanceláří veřejné správy se podílíme na tvorbě minimálního standardu projektového řízení pro státní správu.

Přímé řízení projektů a metodická podpora

Projektová kancelář přímo řídila nebo asistovala v roce 2021 na těchto projektech (s přínosem dovnitř NÚKIB i mimo něj):

- **Neveřejný web** – po předání řízení projektu do rukou vládního CERTu v roce 2020 dále zajišťovala projektová kancelář metodickou podporu v závěrečné fázi projektu. Projekt je nyní úspěšně dokončen – zejména díky specialistům ze SecOps CERT. Nyní dochází k jeho rozvoji a rozšiřování okruhu cílových uživatelů.
- **Databáze kontaktních údajů a systém pro řešení incidentů –** řízení projektu pokračuje s významným dopadem na zajištění kybernetické bezpečnosti. V roce 2021 došlo k úspěšnému výběru dodavatele a k samotné implementaci systému. K finalizaci prací dochází v souladu s harmonogramem na začátku roku 2022.
- Pilotní projekt **Vytvoření komunikačního IS** připravil architekturu pro vytvoření důvěryhodného prostředí vnitřní infrastruktury při práci mj. i s utajovanými informacemi nižšího stupně. Následně byla zajištěna implementace zabezpečené platformy.

- Mimo uvedené realizujeme a připravujeme další, zejména infrastrukturní projekty a projekty na zvýšení efektivity, které mají zpravidla přímý i nepřímý pozitivní vliv na zajištění kybernetické bezpečnosti organizace. Stejně tak asistujeme s udržitelností ukončených projektů a vyhledáváme a podporujeme vhodné příležitosti a spolupráci na mnoha úrovních. V neposlední řadě poskytujeme metodickou podporu řadě dalších projektů NÚKIB.

Podpora financování kyberbezpečnostních projektů z fondů EU

- Jsme členy pracovního týmu IROP, pro SC 1.1 eGovernment a kybernetickou bezpečnost, v rámci, kterých se účastníme různých aktivit.
- Zajišťujeme také přípravu kofinancování vybraných projektů NÚKIB v oblasti kybernetické bezpečnosti, a i v dalších oblastech EU fondů.
- Vypracovali jsme množství pomůcek, šablon, provedli jsme řadu konzultací směřujících k maximální podpoře realizace projektů kofinancovaných ze SF EU. Podpora probíhá směrem dovnitř i směrem vně organizace. Konkrétními kroky se snažíme zvýšit i podpořit možnost kofinancování kybernetické bezpečnosti z EU pro oblast zdravotnictví.

Osvěta a vzdělávání v projektovém řízení

- V předmětném období jsme nadále velice aktivně spolupracovali s externí profesní komunitou projektových manažerů.
- Vytvořili jsme nová školení, např. školení projektového řízení pro pokročilé a k řízení rizik.
- Podporujeme vzdělávání v oblasti projektového řízení pro ostatní kolegy, poskytujeme doporučení ke konkrétním kurzům a metodikám.

4 Odbor Kabinet ředitele

Legislativa a vládní agenda NÚKIB

NÚKIB je gestorem zákona č. 181/2014 Sb. zákon o kybernetické bezpečnosti, 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 v informačních systémech kritické informační infrastruktury, významných informačních systémech, informačních systémech základních služeb a dalších systémech, ve kterých jsou zpracovávány neutajované informace, a také zajištění bezpečnosti informací zpracovávaných v informačních a komunikačních systémech nakládajících s utajovanými informacemi.

V roce 2020 předložila vláda Poslanecké sněmovně Parlamentu ČR návrh novely zákona o kybernetické bezpečnosti vypracovaný NÚKIB, jehož cílem bylo 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 bylo stanoveno, že tzv. vnitrostátním orgánem certifikace předvídaným aktem o kybernetické bezpečnosti je NÚKIB, a také měly být stanoveny přestupky za nedodržení povinností stanovených aktem o kybernetické bezpečnosti. Jelikož do konce 8. volebního období Poslanecké sněmovny Parlamentu ČR nebyl návrh novely zákona Sněmovnou projednán, musel být v roce 2021 opakovaně předložen nově jmenované vládě ke schválení.

V roce 2021 také pokračovaly intenzivní legislativní práce na přípravě zákona upravujícího využívání služeb cloud computingu orgány veřejné moci, na kterých se NÚKIB podílel. NÚKIB zároveň pracoval na přípravě tří vyhlášek provádějících uvedenou zákonnou úpravu. Práce na dvou z těchto vyhlášek se podařilo zdárně dokončit a byly vydány ve Sbírce zákonů ČR. Jedná se o vyhlášku č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci a vyhlášku č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu. Dokončení třetí vyhlášky upravující tuto problematiku se očekává v průběhu roku 2022. K 1. lednu 2021 rovněž nabyla účinnost vyhláška č. 573/2020 Sb., kterou se mění vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby, kterou došlo ke změně odvětvových kritérií v odvětví zdravotnictví.

Vedle legislativních prací na výše uvedených právních předpisech NÚKIB v roce 2021 posoudil v meziresortním připomínkovém řízení 115 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 (dále jen „VKB“), aktualizací výkaznictví souladu právních předpisů v gesci NÚKIB s právními předpisy EU a řízením gescí NÚKIB k dokumentům legislativní i nelegislativní povahy EU apod. V této souvislosti lze za rok 2021 zmínit především přijetí Akčního plánu k Národní strategii kybernetické bezpečnosti na období let 2021 až 2025. Akční plán navazuje na Národní strategii kybernetické bezpečnosti České republiky. Strategií představené vize transformuje Akční plán do konkrétních úkolů, definuje gestory a časově terminuje jejich plnění v horizontu do roku 2025. Přijetí Akčního plánu byl další nezbytný krok k účinnému zajišťování kybernetické bezpečnosti ČR.

NÚKIB dále zabezpečuje fungování VKB, který je stálým pracovním orgánem Bezpečnostní rady státu. NÚKIB plní funkci sekretariátu VKB, zabezpečuje svolávání schůzí VKB a v neposlední řadě zajišťuje koncepční směřování VKB. V roce 2021 se NÚKIB podařilo zefektivnit činnost VKB, a to novelou jeho Jednacího řádu a Statutu. Touto novelou došlo k zakotvení institutu mimořádného situačního jednání k aktuálním bezpečnostním hrozbám, kterým lze v případě ohrožení kybernetické bezpečnosti ČR rychle a operativně svolat schůzi členů VKB.

Zahraniční pracoviště

USA

V roce 2021 pokračovala blízká spolupráce mezi NÚKIB a partnery v USA v otázce zabezpečení 5G sítí a důvěryhodnosti dodavatelů technologií. Výsledkem je mj. i přijetí Pražských návrhů k diverzifikaci dodavatelů telekomunikačních sítí.

V druhé polovině roku se Česká republika prostřednictvím NÚKIB a MZV připojila ke Counter Ransomware Initiative, jako jedna ze 30 zakládajících zemí inciativy amerického National Security Council.

Izrael

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

Dne 24. února 2021 se uskutečnil Executive Cyber Workshop pro kritickou informační infrastrukturu, který zorganizoval NÚKIB ve spolupráci s Israel Electric Corporation – izraelskou státní společností, která vyrábí, přenáší a distribuuje elektřinu. Cílem workshopu byla výměna zkušeností se zvládáním kybernetických incidentů v sektoru energetiky. Za českou stranu se účastnili zástupci různých společností kritické infrastruktury, zejména za sektor energetiky a některých státních úřadů.

NÚKIB dále v červenci zorganizoval návštěvu delegace Poslanecké sněmovny Parlamentu ČR a vedení NÚKIB na prestižní konferenci Cyber Week 2021. Česká delegace kromě účasti na konferenci měla také jednání s řadou místních institucí, s nimiž NÚKIB dlouhodobě a úspěšně spolupracuje.

Na konci října proběhlo historicky první společné cvičení NÚKIB a INCD s názvem CRISIS-X.

ENISA

V roce 2021 pracovník NÚKIB českým aktérům zasílal shrnutí a analýzy relevantních veřejných výstupů ENISA. Pomáhal vybraným českým subjektům v kontaktu s ENISA. Propagoval české akce typu Prague 5G Security Conference a naopak akce ENISA v ČR.

Brusel – NATO

V roce 2021 se NÚKIB ve spolupráci s národními partnery a všemi spojenci podílel na vytvoření nové komplexní politiky kybernetické obrany NATO. Tato politika byla schválena na červnovém summitu a nadále podporuje tři základní úkoly NATO, jimiž jsou kolektivní obrana, krizové řízení a kooperativní bezpečnost. Zároveň tato nová politika podporuje celkové odstrašení a obranný postoj NATO. Všichni spojenci v loňském roce rovněž zahájili diskusi k přípravě akčního plánu, který má zajistit plnohodnotnou implementaci nové politiky.

Na alianční půdě také ČR spolu s dalšími spojenci hojně diskutovali jednotlivé případy a dopady škodlivých kybernetických činností na kritickou infrastrukturu. Hlavními trendy v této oblasti,

které ostatně zmiňuje např. summitové communiqué, byly útoky na dodavatelský řetězec software či incidenty spojené se škodlivým (vyděračským) kódem – ransomware. Některé případy pak Severoatlantická rada přímo adresovala ve svých veřejných prohlášeních. Jednalo se o odsouzení útoků na produkty Solarwinds či kompromitace serveru Microsoft Exchange.

V roce 2021 také proběhl další ročník Cyber Coalition, jednoho z největších cvičení kybernetické obrany NATO. Vedle všech spojenců NATO se účastnily i vybrané partnerské země: Finsko, Irsko, Švédsko a Švýcarsko. Cvičení opět prověřilo kybernetické experty z těchto zemí a jejich schopnosti bránit národní i aliančí sítě.

Brusel – EU

NÚKIB se v roce 2021 prostřednictvím svého cyber attaché na Stálém zastoupení ČR při EU podílel zejména na práci (EU) Horizontální pracovní skupiny pro kybernetické otázky. Zásadním tématem této skupiny v roce 2021 byla revize směrnice o opatřeních pro vysokou společnou úroveň kybernetické bezpečnosti v celé Unii (směrnice NIS), která byla vydána 16. prosince 2020. Cílem NÚKIB bylo, aby systém zajišťování kybernetické bezpečnosti nastavený směrnicí NIS byl efektivní, zbytečně nezatěžoval regulované subjekty, dovoloval pružné nakládání s kapacitami členských států a umožňoval jejich vzájemnou spolupráci založenou na důvěře. Závěrem roku byl v rámci Rady EU přijat tzv. Obecný přístup k této směrnici, který následně založil mandát pro francouzské předsednictví Rady EU pro vyjednávání s Evropským parlamentem dle standardního legislativního procesu EU.

Z nelegislativních spisů se v druhé polovině roku NÚKIB podílel zejména na přijetí závěrů Rady o prozkoumání potenciálu iniciativy Joint Cyber Unit. Samotná substantivní práce na této iniciativě bude probíhat také v období českého předsednictví Radě EU, v druhé polovině roku 2022.

CCDCOE

Zástupci NÚKIB se úspěšně podíleli na realizaci největšího kybernetického cvičení Locked Shields, které se z pandemických důvodů muselo konat v hybridním módu. Dále se titíž zástupci podíleli na realizaci ofenzivního cvičení Crossed Swords a Cyber Coalition. Výraznou měrou se naši lidé zasloužili o uskutečnění výroční konference CCDCOE – CyCon.

Komunikace

Hlavní náplní práce oddělení komunikace v roce 2021 bylo budování vztahů s veřejností prostřednictvím správy sociálních sítí a webových stránek. V roce 2021 oddělení spravovalo účty na sociálních sítích Facebook, Twitter, LinkedIn, Instagram a YouTube. Realizovalo rozličné komunikační aktivity a kampaně. Náplní práce oddělení byla rovněž interní komunikace a organizace interních akcí NÚKIB. V rámci oddělení také působí tiskový mluvčí NÚKIB odpovědný za mediální komunikaci.

Oddělení v roce 2021 kromě své denní agendy participovalo na organizaci konferencí CyberCon a Prague 5G Security Conference. Mimo to zrealizovalo studijní veletrh Studuj Kyber!, jehož cílem je představit žákům a široké veřejnosti školy a obory, které úzce souvisejí s kybernetickou a informační bezpečností a informačními technologiemi.

Mezi činnosti oddělení komunikace spadá rovněž koordinace strategické komunikace napříč státní správou v tématech souvisejících s činností NÚKIB. 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, ve znění pozdějších předpisů (dále jen „zákon o finanční kontrole“). Postavení interního auditu je nezávislé na organizační struktuře NÚKIB a interní audit je administrativně a funkčně podřízen řediteli NÚKIB.

Činnost interního auditu je upravena Statutem interního auditu. Pro výkon činnosti jsou využívány Manuál interního auditu a Program pro zabezpečení a zvyšování kvality 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 bylo zpracovaní Mapy 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.

Začátkem roku 2021 byly dokončeny interní audity GDPR a oběhu účetních dokladů, které byly zahájeny koncem roku 2020.

Cílem interního auditu GDPR byla 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 věnoval prověření dodržování interních normativních aktů týkajících se oběhu účetních dokladů a souvisejících právních předpisů. Taktéž byla 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.

V průběhu roku byl proveden audit procesu nákupu a audit bezpečnosti a ochrany zdraví při práci (dále jen „BOZP“) a požární ochrany (dále jen „PO“). Při auditu procesu nákupu bylo prověřeno dodržování interních normativních aktů vztahujících se k procesu nákupu a souvisejících právních předpisů. Taktéž proběhla kontrola plánování procesu nákupu, požadavků na objednávku, výběru a hodnocení dodavatelů, uzavírání smluv, vystavení a potvrzení objednávky, příjmu zboží či poskytnutí služby.

Audit BOZP a PO se zaměřil především na kontrolu shody s legislativními požadavky, s interními normativními akty, realizaci školení v dané problematice, záznamy o školeních, pracovních úrazech, zprávy o revizích, bezpečnostní značení.

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.

V roce 2021 byl taktéž zahájen následný audit zaměřený na prověření realizace opatření k odstranění nedostatků zjištěných v průběhu auditů vykonaných v roce 2020 a audit dodržování zákona č. 340/2015 Sb., o registru smluv, ve znění pozdějších předpisů.

Cílem auditu dodržování zákona č. 340/2015 Sb., o registru smluv je prověření shody s legislativními požadavky, interními normativními akty, vztahu k zákonu č. 106/1999 Sb. o svobodném přístupu k informacím, ve znění pozdějších předpisů a k obecnému nařízení o ochraně osobních údajů. Taktéž zmapování povinných subjektů/smluvních stran, rozbor jednotlivých výjimek z povinnosti uveřejnit smlouvu, kontrola provádění případných oprav zveřejněné smlouvy a prověření praktického postupu při uveřejňování smlouvy v registru smluv.

Na základě pověření ředitele NÚKIB byl zahájen mimořádný audit organizace příprav a realizace Prague 5G Security Conference 2021. Pozornost auditu je zaměřena na soulad dokumentace související s organizací příprav a realizace Prague 5G Security Conference 2021 s interními normativními akty NÚKIB a právními předpisy (zejména se zákonem č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů a s § 26 a § 27 zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů, ve znění pozdějších předpisů).

V únoru roku 2021 byla odeslána MF Zpráva o výsledcích finančních kontrol na NÚKIB za předchozí kalendářní rok.

Koncem roku 2021 byl zpracován Plán interního auditu pro rok 2022, střednědobý plán interního auditu pro období 2022–2024 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, připomínkování a spolupráce při tvorbě interních normativních aktů.

Seznam zkratek

AČR – Armáda České republiky

AHC – Ad Hoc Committee on Cybercrime

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)

ČNB – Česká národní banka

ČOI – Česká obchodní inspekce

ČR – Česká republika

BBKME – Black Box Key Management Equipment

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

EU – Evropská Unie

EUSPA – Agentura pro evropský globální navigační satelitní systém

GIBS – Generální inspekce bezpečnostních sborů

ICT –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

MŠMT – Ministerstvo školství, mládeže a tělovýchovy

MV – Ministerstvo vnitra

MZ – Ministerstvo zemědělství

MZV – Ministerstvo zahraničních věcí

NAKIT – Národní agentura pro komunikační a informační technologie

NASTAPO – Oddělení národních strategií a politik

NATO – North Atlantic Treaty Organization (Severoatlantická aliance)

NBÚ – Národní bezpečnostní úřad

NCKB – Národní centrum kybernetické bezpečnosti

NCKO – Národní centrum kybernetických operací

NCOZ – Národní centrála proti organizovanému zločinu

NNV – Nespotřebované náklady

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)

NKC – Národní koordinační centrum kybernetického výzkumu a vývoje

OSN – Organizace spojených národů

PČR – Policie České republiky

PESCO – Permanent Structured Cooperation (Stálá strukturovaná spolupráce)

PO – Požární ochrana

PRS – Public Regulated Service (Veřejně regulovaná služba)

PZS – Provozovatel základní služby

QKD – Kvantové distribuce klíčů

REACT– Recovery Assistance for Cohesion and the Territories of Europe

ŘO – Řídící orgán

SC – Specifický cíl

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

SecOps CERT – Oddělení Security operations Odboru Vládního CERTu (Computer Emergency Response Team)

SF EU – Strukturální fondy Evropské unie

SMVS – Správa Majetku ve Vlastnictví Státu

SSHR – Státní správa hmotných rezerv

SÚKL – Státní úřad pro kontrolu léčiv

UN GGE – UN Group of Governmental Experts

ÚS – Ústavní soud

ÚVČR – Úřad vlády České republiky

VeKySIO – Velitelství kybernetických sil a informačních operací

VIS – Významný informační systém

VKB – Výbor pro kybernetickou bezpečnost

VUT – Vysoké učení technické

VZ – Vojenské zpravodajství