

NÚKIB



ZPRÁVA O ČINNOSTI 2022

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST

Praha 2023

Obsah:

1.	Úvodní slovo ředitele	3
2.	Činnost NÚKIB v číslech	5
3.	Oblasti činnosti	6
3.1	Strategie a politiky	6
3.2	Vyhodnocení a řešení kybernetických bezpečnostních událostí a incidentů	7
3.3	Monitoring, analytická činnost a informační podpora	9
3.4	Kontrola, dohled a metodická pomoc	9
3.4.1	Kybernetická bezpečnost	9
3.4.2	Bezpečnost informačních a komunikačních systémů	9
3.4.2.1	Certifikace informačních a komunikačních systémů	9
3.4.2.2	Certifikace kryptografických prostředků a pracovišť	10
3.4.2.3	Ochrana proti kompromitujícímu vyzařování a certifikace stínících komor	10
3.4.2.4	Národní distribuční středisko	10
3.4.3	Správní řízení	10
3.5	Veřejně regulovaná služba Evropského programu družicové navigace Galileo	11
3.6	Vzdělávání a osvěta	11
3.7	Cvičení	13
3.8	Vědecká činnost, výzkum a inovace	15
3.9	Legislativa a vládní agenda	16
3.10	Komunikace	17
3.11	Spolupráce, mezinárodní spolupráce	17
3.12	Ekonomické zabezpečení	21
3.13	Investice a rozvoj	23
3.14	Personální zabezpečení	24
3.15	Interní audit a vnitřní kontrola	28
4.	Seznam použitých zkratk	29

1. Úvodní slovo ředitele

Vážené dámy, vážení pánové,

Zpráva o činnosti Národního úřadu pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) shrnuje, jak sám název napovídá, činnost naší instituce za rok 2022. Uplynulý rok byl pro nás všechny rokem dynamickým, plný výzev a příležitostí. NÚKIB prošel řadou změn, mezi které patřila také neplánovaná změna v jeho čele v podobě odchodu generálporučíka Ing. Karla Řehky, který vedl NÚKIB od 20. 3. 2020 do 30. 6. 2022. Generálporučík Řehka tak přímo ovlivnil činnost v první polovině roku 2022 a nepřímo se zcela pochopitelně jeho rukopis propsal do činnosti nejen v druhé polovině roku, ale volně se propisuje až do současnosti. Děkuji mu za jeho práci pro NÚKIB, kyberbezpečnost České republiky a nás všechny a na nové pozici náčelníka Generálního štábu Armády České republiky mu přeji jen to nejlepší.

Významnou událostí minulého roku bylo pro NÚKIB, stejně jako pro ostatní instituce, české předsednictví v Radě EU (dále jen „CZ PRES“). Podařilo se nám dosáhnout stanovených cílů, což vedlo, a především do budoucna ještě povede k bezpečnějšímu kyberprostoru České republiky a Evropské unie. K nejvýznamnějším námi organizovaným akcím spojeným s CZ PRES patřily Prague Cyber Security Conference, které se zúčastnily stovky lidí z celého světa, nebo velmi pozitivně hodnocený EU TEMPEST Seminar.

Rok 2022 se však nenesl jen ve znamení českého předsednictví. NÚKIB i nadále pokračoval v tradicích a dobré praxi, jež jsou pevně spjaty s jeho jménem. Uspořádali jsme již zavedené a úspěšné akce, jako jsou CyberCon, sektorové cvičení Health Czech nebo Festival bezpečného internetu.

NÚKIB se také podařilo maximálně transparentně komunikovat téma připravovaného nového zákona o kybernetické bezpečnosti a s ním spojenou transpozici evropské směrnice NIS2 a mechanismus prověřování bezpečnosti dodavatelských řetězců. Nespočet aktivit, které jsme v souvislosti s novou legislativou směrem k odborné i široké veřejnosti podnikli, vedl také k zisku podpory, která je nezbytná při prosazování potřebných řešení a upevňuje vzájemnou důvěru mezi státní, soukromou a akademickou sférou.

Aktivní byl NÚKIB i v oblasti informační bezpečnosti. V úzké spolupráci s Národním bezpečnostním úřadem se podílel na přípravě novely zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti.

V průběhu celého roku jsem zaznamenával pozitivní ohlasy z řad odborné i široké veřejnosti na naše vzdělávací kurzy a osvětové kampaně, stejně jako na účast našich kolegů a kolegyň na seminářích, workshopech, konferencích, v diskusích, podcastech a obdobných aktivitách. To vše také patří ke každodenní činnosti NÚKIB, díky níž je naše země bezpečnější.

V neposlední řadě byla v roce 2022 pro NÚKIB významným tématem i finalizace delimitace jeho struktur od Národního bezpečnostního úřadu. Za klíčový úspěch v tomto ohledu považuji především kompletní oddělení utajované informační infrastruktury přinášející zásadní posílení suverenity a vnitřní bezpečnosti NÚKIB.

Vše výše zmíněné proběhlo plně v souladu s vládou schválenou Konceptí rozvoje NÚKIB, která se nám tak daří průběžně naplňovat. Vzhledem k novým výzvám, které se v posledních letech objevily kvůli nestabilnímu bezpečnostnímu prostředí, však před námi stojí úkol revidovat tento dokument.

Dovolím si tedy konstatovat, že rok 2022 byl z pohledu NÚKIB rokem úspěšným. Zvládli jsme

všechny výzvy a úkoly, které před nás byly postaveny. Získali jsme množství nových zkušeností a znalostí a upevnili jsme svou pozici nejen v rámci České republiky, ale také na mezinárodním poli. Bylo nám ctí, že jsme za naši činnost mohli převzít ocenění v soutěži Český zavináč a byli jsme tak představeni jako příklad moderní a respektované instituce, která svými aktivitami zlepšuje kybernetickou odolnost České republiky. Vše, co děláme, děláme se záměrem udělat z českého kyberprostoru co nejbezpečnější místo. Naším posláním je posilovat bezpečnost a odolnost České republiky v kyberprostoru a chránit tak naše spoluobčany. Věřím, že se nám to daří, a o tom, co vše pro to děláme, si můžete přečíst právě v této zprávě.

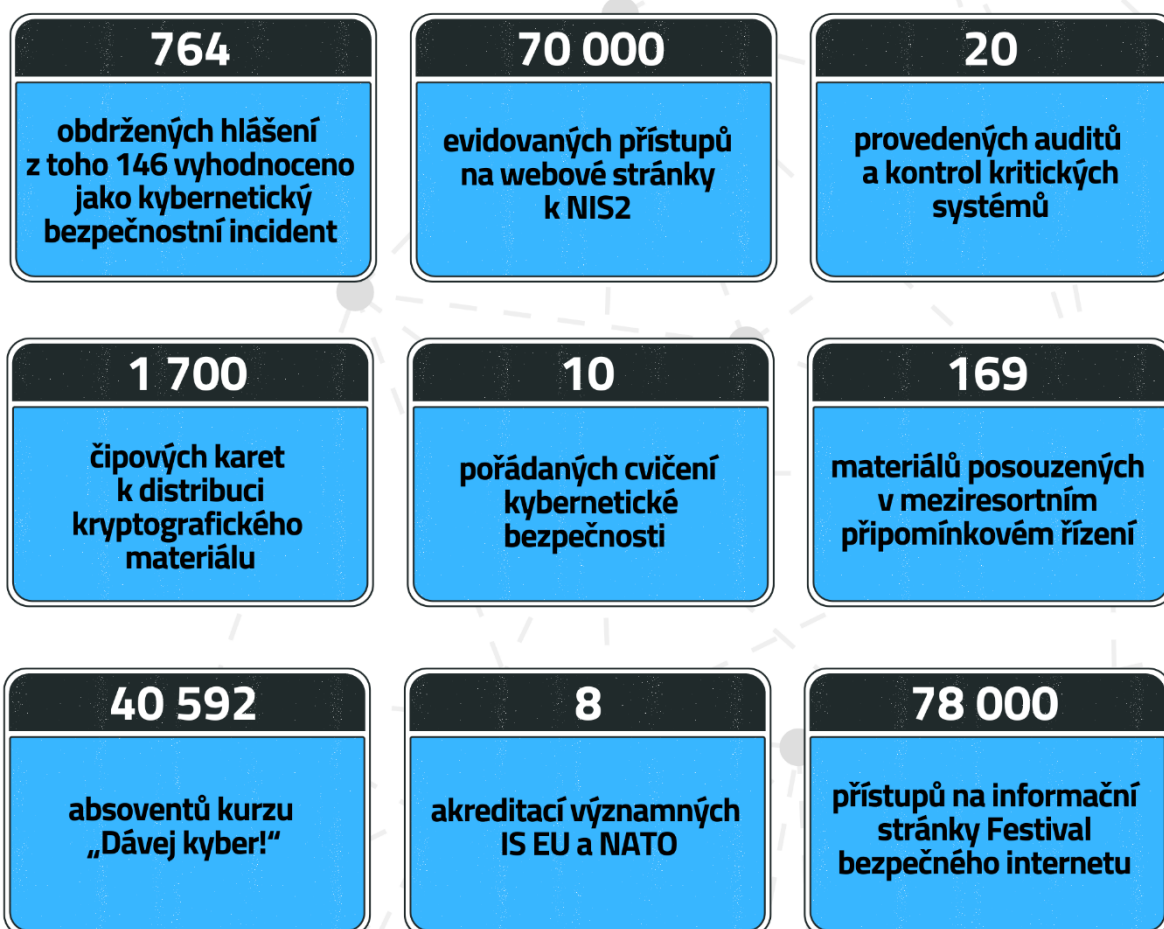
Děkuji za Váš zájem.



Ing. Lukáš Kintr

ředitel Národního úřadu pro kybernetickou a informační bezpečnost

2. Činnost NÚKIB v číslech



Vydané certifikáty



3. Oblasti činnosti

3.1 Strategie a politiky

Při zajišťování kybernetické bezpečnosti je zásadní spolupráce napříč státní, soukromou, akademickou i neziskovou sférou. NÚKIB po celý rok 2022 prohluboval a rozšiřoval kooperaci s mnoha institucemi prostřednictvím četných pracovních jednání, setkání a konferencí. Rovněž připomínkoval řadu koncepčních a strategických dokumentů, aby u nich zajišťoval koherenci s Národní strategií kybernetické bezpečnosti České republiky a přístupem NÚKIB.

V rámci nastavování národních politik v oblasti kybernetické bezpečnosti vyvíjel NÚKIB následující aktivity.

Koordinované zveřejňování zranitelností (dále jen „CVD“) představuje formalizovaný proces dobrovolného objevování zranitelnosti v produktech informačních a komunikačních technologií (dále jen „ICT“) třetími osobami tzv. objeviteli, včetně notifikace objevené zranitelnosti vlastníkoví/správci ICT produktu za účelem provedení bezpečnostní opravy. V současnosti v České republice (dále jen „ČR“) neexistuje formalizovaný a ucelený pohled státu na CVD ani jeho specifická právní úprava. NÚKIB během roku 2022 pracoval na návrhu národního přístupu, který umožní zodpovědné a koordinované objevování zranitelností využitelné pro orgány veřejné moci i soukromý sektor. Zpracovaný návrh národní politiky CVD by měl být základem pro navazující práci na metodických materiálech určených pro snadné praktické využití u konkrétních osob a organizací.

Projekt BIVOJ (bezpečný, inovativní, pro veřejnou správu, odolný, jednotný). Účelem Projektu BIVOJ je zajistit centrální správu a řízení bezpečnosti sdílených informačních a komunikačních systémů a služeb organizací veřejného sektoru ČR. Cílem je vytvoření jednotné, funkční a bezpečné sdílené platformy poskytující bezpečnostní a komunikační služby, do které budou postupně připojeny instituce veřejného sektoru, prvky kritické informační infrastruktury nebo jiné základní služby v rukou státu. Jedná se o celkový program, který v sobě obsahuje více jednotlivých pilířů (například jednotná doména, bezpečnostní dohled, jednotná internetová brána) s horizontem realizace okolo 5 až 7 let. Bezpečnostní rada státu (dále jen „BRS“) ve svých usneseních vzala na vědomí NÚKIB zpracovaný ideový záměr, představující shodu všech zainteresovaných subjektů, a pověřila NÚKIB záměr rozpracovat. Současně byl NÚKIB ustanoven do role koordinátora projektu.

Nastavování bezpečnostního rámce rozvoje 5G sítí. NÚKIB spolu s Ministerstvem průmyslu a obchodu (dále jen „MPO“), Ministerstvem zahraničních věcí (dále jen „MZV“), Bezpečnostní informační službou, Úřadem pro zahraniční styky a informace a Vojenským zpravodajstvím v únoru 2022 vydal Doporučení pro hodnocení důvěryhodnosti dodavatelů technologií do 5G sítí v ČR. Doporučení poskytuje vodítko zejména pro dodávky do informačních a komunikačních systémů kritické infrastruktury ČR a představuje pohled státu, který se neodvíjí pouze od konečné technické podoby dodávaného řešení, ale zohledňuje i netechnické aspekty, podnikatelské, právní a politické prostředí, ve kterém se dodavatel pohybuje.

Bezpečnost dodavatelských řetězců. NÚKIB na základě pověření BRS intenzivně pracoval na návrhu zákona, který umožní státu prověřovat dodavatele do své strategicky významné infrastruktury. Cílem tohoto prověřování je zvýšení odolnosti a bezpečnosti ČR a omezení negativních zahraničních vlivů. Hrozby v oblasti kybernetické bezpečnosti plynoucí z dodavatelských řetězců technologií jsou již dlouhodobě známy, dosud však v právním

řádu ČR neexistuje komplexní právní řešení umožňující rizika plynoucí z těchto hrozeb pro strategicky významnou infrastrukturu cíleně a účinně vyhodnocovat a snižovat. Připravovaný návrh zákona si klade za cíl tento nevyhovující stav změnit. V druhé polovině roku se NÚKIB účastnil řady akcí nebo takové přímo organizoval, kde o problematice bezpečnosti dodavatelského řetězce diskutoval se zástupci veřejného i soukromého sektoru. Lze zmínit diskusi na půdě Poslanecké sněmovny Parlamentu ČR, panel k bezpečnosti dodavatelského řetězce v rámci konference CyberCon, Prague Cyber Security Conference, akce NÚKIB v rámci CZ PRES a seminář k připravovanému návrhu zákona. Harmonogram projektu je spojen s dalším významným projektem NÚKIB, jímž je transpozice směrnice Evropského parlamentu a Rady EU 2022/2555 ze dne 14. 12. 2022, o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (dále jen „směrnice NIS2“), kde dochází k přípravě návrhu zákona, který v budoucnu nahradí zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), a kterým bude směrnice NIS2 transponována do právního řádu ČR.

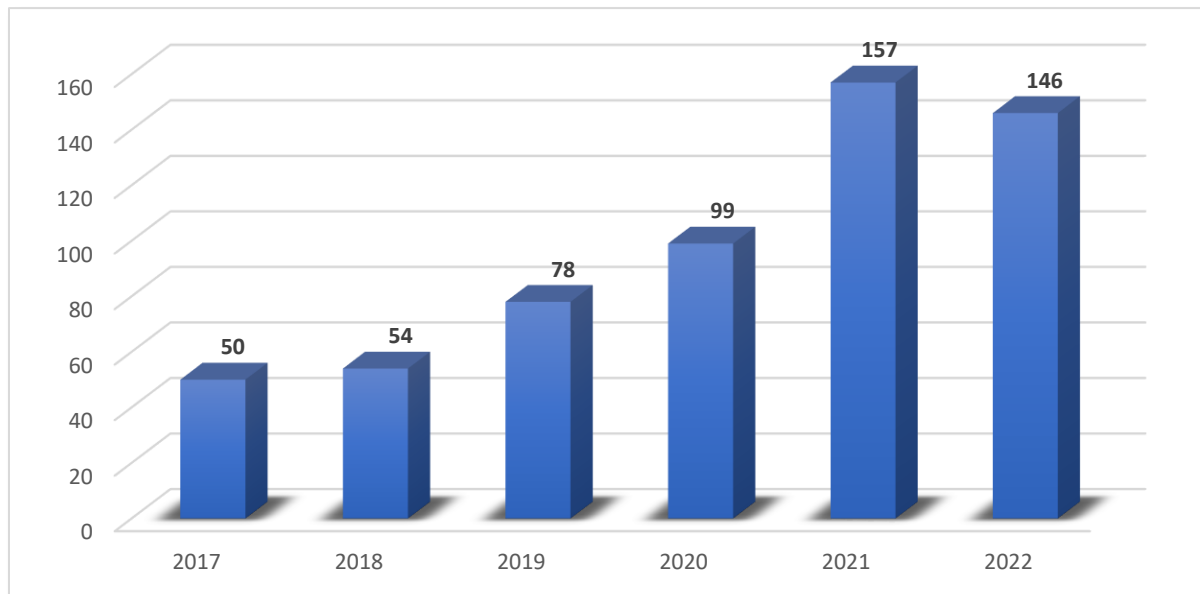
NÚKIB participoval na „Zavedení minimálních standardů projektového řízení pro instituce státní správy“ a „Sjednocení kompetencí projektových manažerů v institucích státní správy a katalogizace projektových prací“. Úkoly pomáhají naplnit cíle strategického materiálu ČR „Koncepce Klienty orientovaná veřejná správa 2030“ v gesci Ministerstva vnitra (dále jen „MV“) s významným podílem Ministerstva pro místní rozvoj. V kontextu připravovaného kompetenčního modelu projektových a portfolio manažerů veřejné správy byla prosazena kompetence zahrnout do projektů odpovídající úroveň kybernetické bezpečnosti a vytvořit podmínky pro bezpečný průběh celého cyklu projektu.

V rámci Integrovaného regionálního operačního programu se NÚKIB podílel na zacílení a tvorbě pravidel pro finanční podporu kybernetické bezpečnosti z fondů EU pro období let 2021–2027. V roce 2022 bylo vypsáno 5 výzev, které umožňují čerpání prostředků na technická opatření související s kybernetickou bezpečností. Celková alokace podpory pro samotnou kyberbezpečnost je přibližně 4 mld. Kč.

3.2 Vyhodnocení a řešení kybernetických bezpečnostních událostí a incidentů

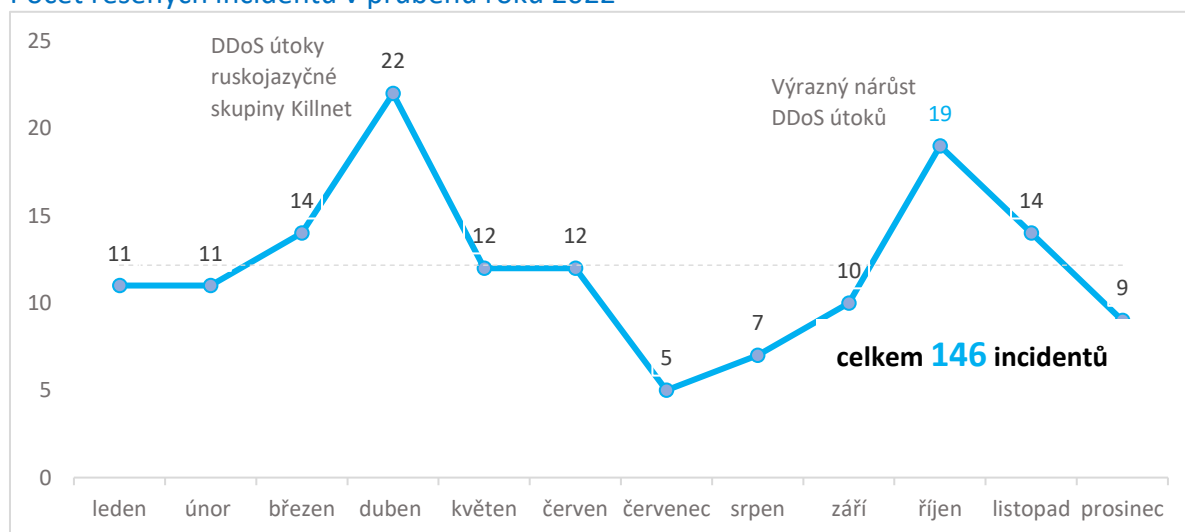
NÚKIB v roce 2022 obdržel celkem 764 hlášení, z nichž 146 vyhodnotil jako kybernetické bezpečnostní incidenty (dále jen „incidenty“), které následně řešil. Po několika letech kontinuálního nárůstu se tak jedná o první zaznamenaný meziroční pokles. Za poklesem oproti roku 2021 stojí především kampaně zneužívající zranitelnosti ProxyLogon a ProxyShell, jejichž cílem byla široce využívaná služba Microsoft Exchange Server, a ke konci roku 2021 byla objevena zranitelnost Log4Shell. V roce 2022 nebyla odhalena žádná taková zranitelnost s tak velkým dopadem.

Vývoj počtu incidentů registrovaných NÚKIB



Nejvíce incidentů v roce 2022 bylo evidováno v měsících dubnu a říjnu, což bylo v obou případech dáno zásadním nárůstem počtu DDoS útoků. Za tímto nárůstem stály především útoky ruskojazyčných hacktivistických skupin. Za dubnovou DDoS kampaní stála skupina Killnet, zatímco k části říjnových útoků se přihlásila skupina Anonymous Russia. Útoky obou skupin velmi pravděpodobně souvisely s českou podporou Ukrajiny.

Počet řešených incidentů v průběhu roku 2022



Do klasifikace incidentů se z velké části promítly rozsáhlé vlny DDoS útoků, a za uplynulý rok tak nejvíce převažovaly incidenty cílící na dostupnost. Nezahrnovaly nicméně pouze výše zmiňované DDoS útoky, ale v některých případech také prosté technické chyby vedoucí k výpadku systémů. V rámci kategorií dostupnosti a škodlivého kódu zůstává nadále trvalým trendem ransomware, který byl v roce 2022 vyjma října evidován každý měsíc. Jeho počet se však meziročně snížil, což se projevilo celkovým poklesem v kategorii škodlivý kód. K poklesu došlo také v incidentech, které NÚKIB klasifikoval jako průnik do systémů. To bylo dáno zejména absencí kampaní zneužívání závažných zranitelností, k jakým docházelo v roce 2021.

Během předchozího roku pokračoval trend rostoucího počtu incidentů u neregulovaných subjektů. Za rok 2022 jich NÚKIB evidoval 74 oproti 64 za rok 2021. U regulovaných subjektů naopak došlo meziročně ke snížení počtu kybernetických incidentů.

Regulované subjekty 72
incidentů

Neregulované subjekty 74
incidentů

3.3 Monitoring, analytická činnost a informační podpora

V návaznosti na monitorování a analýzu trendů, hrozeb a rizik v kybernetickém prostoru poskytoval NÚKIB analytickou podporu také rozhodujícím činitelům v české státní správě a zahraničním partnerům. V této oblasti byla rozvíjena pokročilá analytická kapacita v podobě Cyber Threat Intelligence (dále jen „CTI“). Na základě zpravodajství z otevřených zdrojů poskytoval NÚKIB analytickou podporu i externím partnerům v rámci úzce vymezených agend. Kromě těchto aktivit byla prováděna vlastní interní podpora v oblastech datové analýzy, vývoje, správy a poskytování datových a analytických nástrojů.

3.4 Kontrola, dohled a metodická pomoc

3.4.1 Kybernetická bezpečnost

V roce 2022 bylo provedeno 20 auditů a kontrol podle zákona o kybernetické bezpečnosti, kdy je v rámci běžné kontroly nebo auditu rámcově ověřováno cca 150 kontrolních bodů. S ohledem na eskalaci geopolitické situace ve světě se NÚKIB během kontrolní činnosti zaměřil na nejkritičtější systémy státní správy, u kterých byla provedena kontrola prioritně na oblast řízení kontinuity činností (přípravenost reagovat na krizové situace a schopnost minimalizovat případné následky takové situace). Kontrolovaným organizacím bylo navíc nabídnuto a provedeno zjednodušené table-top cvičení vhodně pokrývající uvedenou oblast. Dále byla prohlubována aktivní spolupráce s ostatními regulátory, kdy se NÚKIB zapojil do kontrolních činností spolu s Úřadem pro ochranu osobních údajů, Úřadem pro civilní letectví a Státním úřadem pro jadernou bezpečnost.

3.4.2 Bezpečnost informačních a komunikačních systémů

NÚKIB je odpovědný za realizaci opatření v oblasti zajištění ochrany utajovaných informací zpracovávaných v informačních a komunikačních systémech a kryptografickou ochranu. Zajišťuje vytváření koncepce rozvoje ochrany utajovaných informací v oblasti bezpečnosti informačních a komunikačních systémů, v oblasti kryptografické ochrany a ochrany před únikem utajovaných informací kompromitujícím vyzařováním, a to s vazbami na jiné obory služby s celostátní a mezinárodní působností. V uvedeném kontextu je zásadní spolupráce s resorty státní správy, podnikateli a akademickou půdou v rámci ČR, orgány EU a Severoatlantické aliance (dále jen „NATO“).

3.4.2.1 Certifikace informačních a komunikačních systémů

NÚKIB plní úkoly Národního střediska pro bezpečnost informačních a komunikačních systémů. Je národní certifikační autoritou ve věci certifikace informačních systémů (dále jen „IS“) nakládajících s utajovanou informací orgánů státní správy a podnikatelů. NÚKIB také vykonává certifikační a metodickou činnost, včetně kontrol ve spolupráci s Národním bezpečnostním úřadem (dále jen „NBÚ“).

V roce 2022 certifikoval NÚKIB 117 významných národních IS, přičemž kromě kontrol prováděných v rámci certifikačního a akreditačního procesu provedl 30 kontrol v rámci kontrolní činnosti NBÚ.

NÚKIB je národní akreditační autoritou ve věci akreditace IS nakládajících s utajovanou informací EU a NATO na území ČR. V roce 2022 NÚKIB akreditoval 8 významných IS EU a NATO.

3.4.2.2 Certifikace kryptografických prostředků a pracovišť

NÚKIB plní úkoly Národního bezpečnostního komunikačního střediska a je národní certifikační autoritou ve věci certifikace kryptografických prostředků a pracovišť orgánů státní správy a podnikatelů. NÚKIB také vykonává certifikační a metodickou činnost u těchto subjektů.

V roce 2022 vydal NÚKIB 12 certifikátů kryptografického prostředku, 16 certifikátů kryptografického pracoviště a schválil 20 zástaveb kryptografického prostředku.

3.4.2.3 Ochrana proti kompromitujícímu vyzařování a certifikace stínících komor

NÚKIB plní úkoly Národního střediska pro měření kompromitujícího vyzařování TEMPEST a TSCM. Vykonává měření elektrických a elektronických zařízení, v souvislosti s ochranou utajovaných informací před jejich únikem kompromitujícím vyzařováním ze zabezpečené oblasti, objektu a certifikace stínících komor. Provádí zónové hodnocení prostorů určených pro zpracování utajovaných informací před jejich únikem prostřednictvím kompromitujícího vyzařování.

V roce 2022 bylo vydáno 39 certifikátů stínících komor, provedeno 43 měření, vyhotoveno 12 instalačních záznamů, provedeno 6 zónových měření a 3 akustická měření.

3.4.2.4 Národní distribuční středisko

NÚKIB plní roli Národního distribučního střediska (dále jen „NDS“), což zahrnuje výrobu a evidenci kryptografického materiálu (dále jen „KM“) a materiálu k zajištění funkce kryptografického prostředku, prováděl distribuci a evidenci KM ČR a EU a KM na základě mezinárodní smlouvy prostřednictvím Crypto Distribution Authority.

V roce 2022 NDS vyrobilo a předalo cca 1 700 ks čipových karet, cca 2 900 ks obálek s heslovým materiálem v tištěné (papírové) podobě a cca 50 ks CD s heslovým materiálem v elektronické podobě. NDS zaevidovalo a označilo hologramy a distribuovalo cca 110 ks kryptografických prostředků a materiálu k zajištění funkce kryptografického prostředku.

3.4.3 Správní řízení

V roce 2022 NÚKIB pravomocně rozhodl o jednom přestupku na úseku zákona o kybernetické bezpečnosti. Proti rozhodnutí nebyl podán opravný prostředek a pokuta byla uhrazena. NÚKIB dále zahájil 3 přestupková řízení pro porušení povinností stanovených zákonem o kybernetické bezpečnosti, ve kterých bylo rozhodnuto pouze nepravomocně, byly podány opravné prostředky, a případy tak v roce 2022 nebyly pravomocně skončeny.

V návaznosti na nedostatky zjištěné při kontrolách v oblasti kybernetické bezpečnosti NÚKIB pravomocně uložil povinným osobám nebo orgánům ve 13 případech jedno nebo více nápravných opatření k odstranění nedostatků.

V roce 2022 zahájil NÚKIB 2 přestupková řízení pro podezření ze spáchání přestupku podle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů (dále jen „zákon o ochraně utajovaných informací“), z nichž v jednom případě bylo v roce 2022 ve věci i pravomocně rozhodnuto. NÚKIB dále pravomocně

rozhodl 2 další případy z minulého období a vybral uložené pokuty. Jednalo se o přestupky fyzických osob spočívající v nakládání s utajovanou informací v necertifikovaném IS.

3.5 Veřejně regulovaná služba Evropského programu družicové navigace Galileo (dále jen „PRS“)

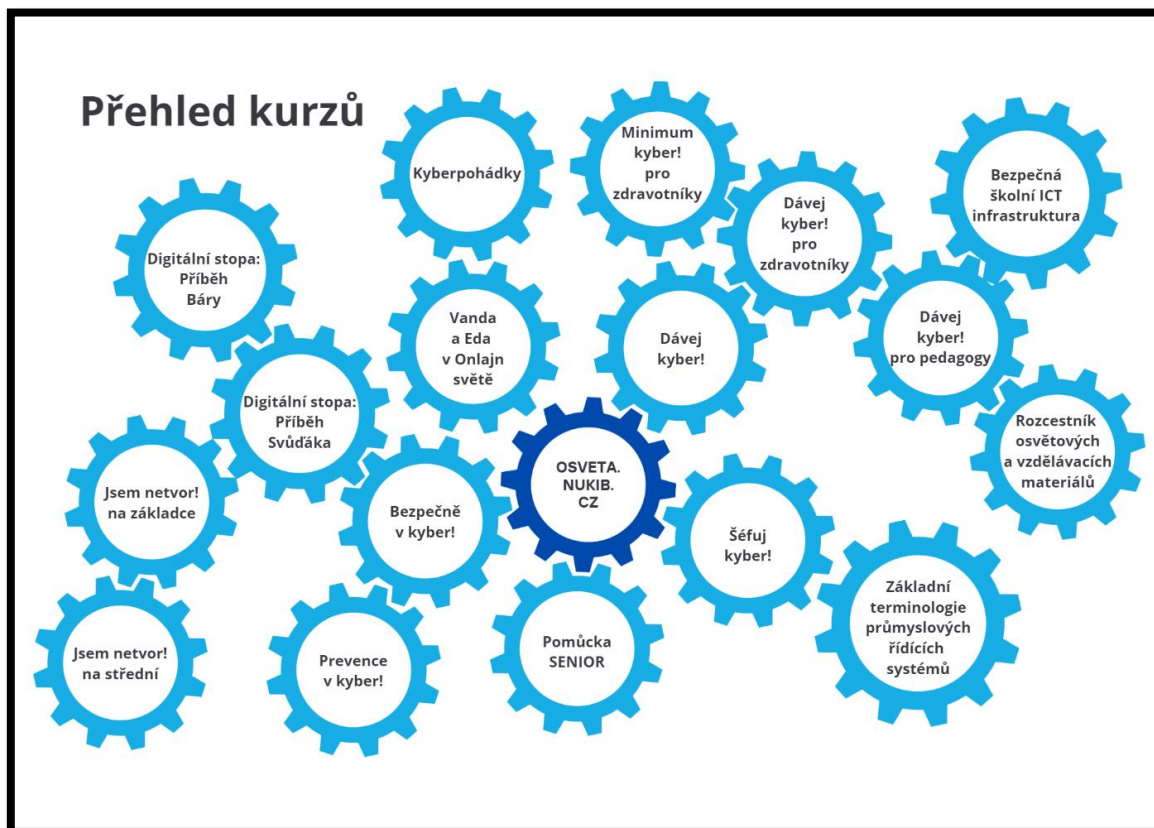
V uplynulém roce byly dobudovány zabezpečené prostory pro instalaci technologií určených pro komunikaci s bezpečnostním a monitorovacím centrem programu Galileo (dále jen „GSMC“) a proběhla příprava podkladů k instalaci první fáze zástavby technologie GRON (Galileo Robust Operation Network) určené pro zabezpečenou komunikaci s GSMC, jejíž zprovoznění se předpokládá v první polovině roku 2023.

V rámci výboru a pracovních skupin Evropské komise proběhl posun v přípravě a přijetí zásadních programových dokumentů nezbytných pro dosažení počátečních operačních schopností PRS.

3.6 Vzdělávání a osvěta

NÚKIB se stejně jako v minulých letech zaměřil na vzdělávání zaměstnanců veřejné správy, zdravotníků a dalších osob podle zákona o kybernetické bezpečnosti. Kromě těchto cílových skupin se věnoval také žákům základních a středních škol, seniorům, pedagogům a knihovníkům. Cílovým skupinám byly nabízeny především e-learningové kurzy na vzdělávacím portálu osveta.nukib.cz, který byl v roce 2022 rozšířen o další kurzy.

Přehled kurzů



Pro bezpečnostní pracovníky informačních technologií vznikl kurz „Základní terminologie průmyslových řídicích systémů“, jehož cílem je seznámit pracovníky se základní terminologií

průmyslových řídicích systémů a se specifiky kybernetické bezpečnosti těchto systémů. Kurz absolvovalo 38 osob.

Další z nově vzniklých kurzů, pomůcka „SENIOR“, si klade za cíl zvýšit osobní bezpečnost seniorů při využívání internetu a přispívá k osvětě rozpoznávání škodlivé elektronické komunikace. Kurz měl přes 78 000 zobrazení.

Vybrané kurzy NÚKIB v číslech



Základní kurzy NÚKIB, mezi které patří „Dávej kyber!“ a „Šéfuj kyber!“, prošly obsahovou a designovou aktualizací. Kurz „Dávej kyber!“, určený zejména zaměstnancům veřejné správy k seznámení se základy kybernetické bezpečnosti pro běžné uživatele, absolvovalo 40 592 uživatelů. Kurz je současně nabízen široké veřejnosti a měl přes 459 478 zobrazení od neregistrovaných uživatelů. Pro účely vzdělávání zdravotnických pracovníků je nabízena speciálně upravená verze kurzu „Dávej kyber!“ a kurz minima kybernetické bezpečnosti „Startuj kyber!“. Tyto kurzy absolvovalo 9 641 zaměstnanců z 27 nemocnic a zdravotnických zařízení. Odborný kurz „Šéfuj kyber!“, který je určen především manažerům kybernetické bezpečnosti a dalším bezpečnostním rolím podle vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů úspěšně absolvovalo 603 uživatelů.

V rámci šíření osvěty mezi dětmi a mladými lidmi byla rozšířena vzdělávací nabídka o knihu Kyberpohádek (v tištěné a elektronické podobě i formě audio), která vznikla ve spolupráci Centra kybernetické bezpečnosti, z. ú, NÚKIB a dalších partnerů.

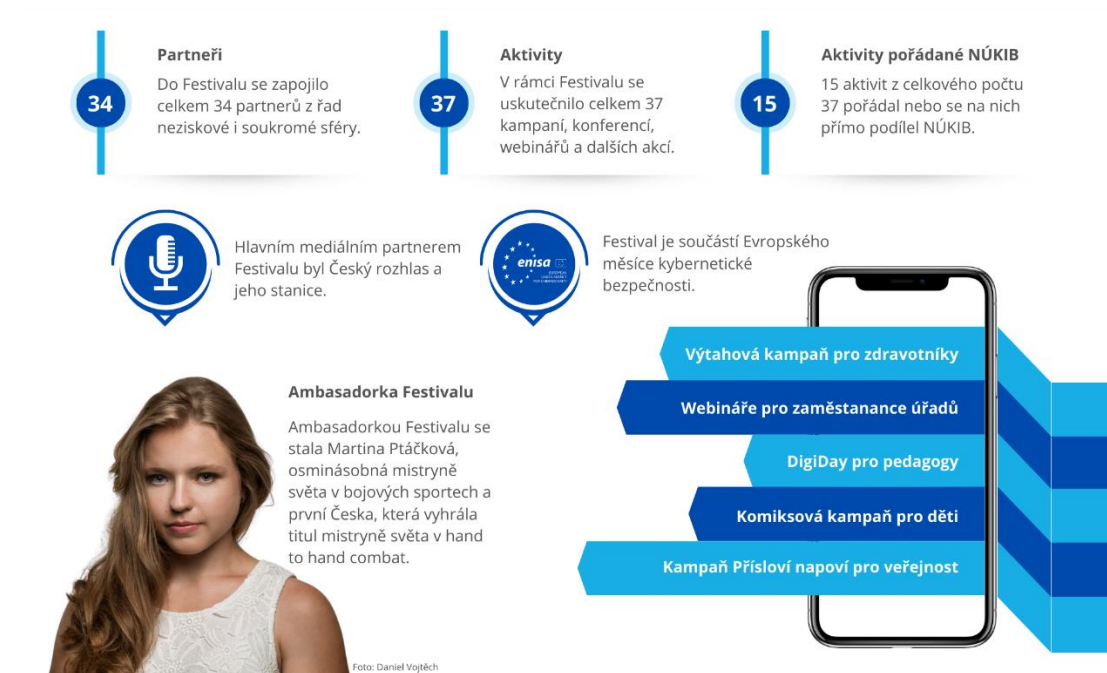
NÚKIB také pokračoval v tvorbě vzdělávacích příspěvků na instagramovém účtu @petr.vytrzny, který byl využit k šíření osvěty v rámci Evropského měsíce kybernetické bezpečnosti, do něhož se NÚKIB každoročně aktivně zapojuje.

Mladé talenty v oblasti kybernetické bezpečnosti podpořil NÚKIB zapojením se do Národního finále soutěže v kybernetické bezpečnosti, které pořádalo Centrum kybernetické bezpečnosti, z. ú.

V souvislosti s transpozicí směrnice NIS2 zveřejnil NÚKIB osvětové stránky k tomuto tématu: [Nová směrnice EU o bezpečnosti sítí a informací \(nukib.cz\)](https://www.nukib.cz). Tento počín se setkal s velkým mediálním zájmem a od zveřejnění stránek bylo evidováno přes 70 000 přístupů.

V říjnu 2022 NÚKIB uspořádal Festival bezpečného internetu zahrnující sérii vzdělávacích akcí, kampaní, konferencí a webinářů pro rozmanité cílové skupiny. Například „Výtahová kampaň“ pro zdravotníky, kampaň v knihovnách „Přísloví napoví“ pro širokou veřejnost, DigiDay pro pedagogy, vzdělávací webináře na témata uživatelských dovedností, evropských certifikací nebo odborné webináře pro manažery kybernetické bezpečnosti. Od zveřejnění bylo evidováno 78 000 přístupů na informační stránku festivalu.

Festival bezpečného internetu 2022



Zaměstnanci NÚKIB se zúčastnili 187 prezenčních nebo on-line konferencí, webinářů, seminářů, kulatých stolů, jednání pracovních skupin, cvičení a přednášek.

Významnou a již tradiční akcí pořádanou NÚKIB, která přispívá ke vzdělávání a osvětě v oblasti kybernetické bezpečnosti, byl 8. ročník konference CyberCon Brno, jehož součástí byl veletrh studijních příležitostí „Studuj kyber!“ určený pro studenty základních a středních škol. Hlavním cílem konference bylo poskytnout prostor pro propojení veřejného, akademického a soukromého sektoru v oblasti kybernetické bezpečnosti. Druhý den konference byl věnován aktuálním novinkám z oblasti regulace, kde odborníci přiblížili aspekty transpozice směrnice NIS2, analýzu rizik či sdíleli hlavní poznatky z auditů kybernetické bezpečnosti. V rámci závěrečného dne byly představeny strategické pohledy na různorodé výzvy v oblasti kybernetické bezpečnosti. Novinkou 8. ročníku byl Workshopový den, během něhož si účastníci mohli prakticky vyzkoušet řešení problémů a výzev souvisejících s kybernetickou bezpečností. Záznam z konference lze nalézt na webu www.cybercon.cz.

3.7 Cvičení

V roce 2022 proběhlo celkem 10 cvičení kybernetické bezpečnosti s celkovým počtem 504 cvičících, které NÚKIB přímo organizoval, případně se podílel na jejich organizaci.

Locked Shields 2022

Ve dnech 18.–22. 4. 2022 se ČR zúčastnila dalšího ročníku největšího mezinárodního cvičení kybernetické bezpečnosti – Locked Shields. Toto hybridní cvičení je pořádáno NATO Centrem excellence pro kybernetickou obranu (dále jen „CCD COE“) sídlícím v Tallinu a na jeho přípravě se podílí řada státních institucí, akademický sektor a přední společnosti z technologického průmyslu. Cílem je zejména prohlubování spolupráce mezi všemi zúčastněnými subjekty. ČR pro tento ročník poprvé utvořila společný tým s kolegy ze Slovenské republiky, přičemž obě země vyslaly do Tallinu své odborníky také pro přípravu cvičení. V rámci ČR se cvičení zúčastnili jak zaměstnanci NÚKIB, tak experti z partnerských institucí ze soukromého i státního sektoru. Společným úsilím bylo dosaženo skvělého výsledku a tým České a Slovenské republiky obsadil 5. příčku.

Cyber Coalition

Dalším mezinárodním cvičením, na kterém zaměstnanci NÚKIB participovali jak při přípravě, tak v roli cvičících, bylo Cyber Coalition. Jedná se o mezinárodní cvičení kybernetické bezpečnosti, které je pravidelně pořádáno NATO a do něhož se zapojila více než tisícovka účastníků. Na úrovni ČR je koordinováno NÚKIB za civilní část a Velitelstvím informačních kybernetických sil za část vojenskou. Samotný název cvičení podtrhuje jeho cíl – podporu silného společenství a vzájemné spolupráce. Toho je dosaženo pomocí scénářů, které sice obsahují technické výzvy, ale podněcují jednotlivé státy ke spolupráci a k vytvoření společného situačního povědomí.

Cvičení v rámci CZ PRES

NÚKIB uspořádal 2 netechnická cvičení kybernetické bezpečnosti, která měla za cíl připravit vybrané pracovníky Úřadu vlády České republiky (dále jen „Úřad vlády“) a dalších relevantních úřadů zapojených do příprav na CZ PRES na realistickou krizovou situaci v oblasti kybernetické bezpečnosti. Cvičení kladla důraz na ověření nastavených krizových komunikačních procesů a kanálů určených pro CZ PRES, a to také s ohledem na informování partnerů v EU. Cvičení dále pomohla zmapovat stav příprav na CZ PRES a odhalit některá potenciálně slabá místa.

Health Czech 2022

Již druhé sektorové cvičení pro sektor zdravotnictví se uskutečnilo ve dnech 13. a 14. 12. 2022 a bylo určeno pro 15 nově regulovaných nemocnic.

Hlavními cíli cvičení bylo umožnit účastníkům procvičení reakce na krizovou situaci v oblasti kybernetické bezpečnosti a zdůraznit komplexnost krizového managementu, rozhodovacího procesu a postupů a současně upozornit na význam role nejvyššího vedení organizace při zvládnání incidentů a navyšování kybernetické bezpečnosti jako takové. Do příprav a exekuce cvičení se zapojili odborníci z Úřadu pro ochranu osobních údajů, Policie České republiky a sdružení CZ.NIC. Realnost cvičení posílila účast štábů České televize a České tiskové kanceláře pro realizaci scénáře tiskové konference.

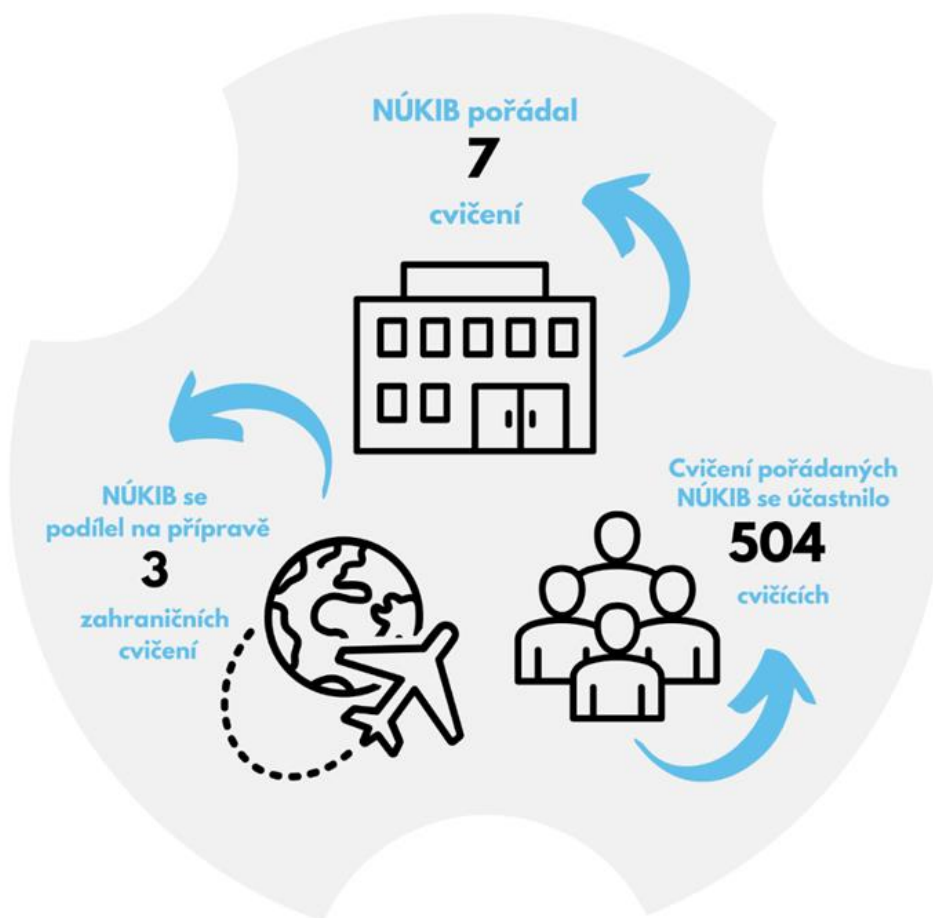
Ostatní cvičení

V průběhu roku proběhlo také několik menších cvičení. Prvním z nich bylo cvičení pro ELSA Summer School, jehož cílem bylo seznámit studenty letní právnické školy s problematikou kybernetické bezpečnosti na příkladech ve formě jednotlivých vstupů do připraveného scénáře.

V podobném duchu se neslo již tradiční cvičení pro studenty předmětu kybernetická bezpečnost, který je vyučován jako součást magisterského navazujícího programu bezpečnostní a strategická studia na Fakultě sociálních studií Masarykovy univerzity.

V rámci workshopového dne již tradiční konference CyberCon pořádané NÚKIB byla realizována ukázka table-top cvičení kybernetické bezpečnosti.

Pořádání a účast na cvičení



3.8 Vědecká činnost, výzkum, vývoj a inovace

Ve spolupráci s partnery z akademického, státního i soukromého sektoru připravil NÚKIB Národní plán výzkumu a vývoje v kybernetické a informační bezpečnosti do roku 2025, který v květnu 2022 schválila vláda. Národní plán stanovuje prioritní výzkumné oblasti v kybernetické a informační bezpečnosti a definuje konkrétní opatření, která mají za cíl stimulovat výzkumné prostředí v ČR, posilovat spolupráci mezi akademickou, soukromou a veřejnou sférou ve výzkumu a vývoji, implementovat technologie v praxi a rozvíjet zahraniční spolupráci.

V rámci výzkumu a vývoje v působnosti NÚKIB byla řešena řada projektů zaměřujících se na oblast kryptografie, matematické kryptologie a kvantových technologií a dále na vývoj speciálních měřících metod a technologií pro zajišťování ochrany před kompromitujícím vyzraňováním. Výstupy těchto projektů nacházejí uplatnění v rámci expertní činnosti NÚKIB a dalších ústředních orgánů státní správy.

NÚKIB prováděl základní a aplikovaný výzkum a vývoj v oblasti kryptografie, kryptoanalýzy a kryptografických prostředků, vyvíjel a schvaloval národní šifrové algoritmy a vytvářel národní politiku kryptografické ochrany. Zabezpečoval vývoj kryptografických schémat pro použití v kryptografických prostředcích ochrany utajovaných informací, prováděl analýzy a hodnocení

šifrových systémů a kryptografických algoritmů určených k ochraně UI a zajišťoval veřejné zakázky NÚKIB v oblasti výzkumu, vývoje a výroby kryptografických prostředků.

NÚKIB podpořil několik projektů financovaných z programu MV „Otevřené výzvy v bezpečnostním výzkumu 2023–2029“ z pozice aplikačního garanta. Jeho rolí je přispět k implementaci výsledků v bezpečnostní praxi. Podpořené projekty se například zaměřují na technologický rozvoj provádění a vyhodnocování kybernetických cvičení, pokročilou analýzu bezpečnostní telemetrie či výzkum v oblasti bezpečnosti optických vláken.

NÚKIB také uspořádal 3 setkání Platformy pro výzkum a vývoj v kybernetické bezpečnosti, jejímiž členy jsou orgány státní správy, akademické a výzkumné instituce a zástupci soukromého sektoru. Tematicky byla setkání zaměřena na aktuální trendy v oblasti kryptografie a na vývoj kvantových technologií.

3.9 Legislativa a vládní agenda

V návaznosti na předložený návrh novely zákona o kybernetické bezpečnosti, vypracovaný NÚKIB, došlo v roce 2022 k jeho projednání Poslaneckou sněmovnou Parlamentu ČR a následně k jeho zveřejnění ve Sbírce zákonů ČR jako zákona č. 226/2022 Sb., kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů s účinností dne 6. 8. 2022. Cílem bylo precizovat kompetenci NÚKIB a národního CERT (Computer Emergency Response Team) k vyhledávání zranitelností a provést adaptaci nařízení Evropského parlamentu a Rady EU 2019/881 ze dne 17. 4. 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) (dále jen „akt o kybernetické bezpečnosti“). V adaptačních ustanoveních bylo stanoveno, že tzv. vnitrostátním orgánem certifikace předvídaným aktem o kybernetické bezpečnosti je NÚKIB, a také byly stanoveny přestupky za nedodržení povinností stanovených aktem o kybernetické bezpečnosti.

Dále v roce 2022 započaly přípravné práce na návrhu zákona, kterým bude transponována směrnice NIS2. Konečné oficiální znění směrnice NIS2 bylo zveřejněno v Úředním věstníku Evropské unie dne 27. 12. 2022. Vzhledem k rozsáhlosti změn, které směrnice NIS2 přináší, připravil NÚKIB návrh zcela nového znění zákona o kybernetické bezpečnosti.

V roce 2022 také pokračovaly intenzivní legislativní práce na přípravě návrhu vyhlášky upravující využívání služeb cloud computingu orgány veřejné moci, konkrétně návrhu vyhlášky o bezpečnostních pravidlech pro využívání služeb cloud computingu orgány veřejné moci. Účinnost vyhlášky upravující tuto problematiku se očekává v průběhu roku 2023.

Vedle legislativních prací na výše uvedených právních předpisech NÚKIB v roce 2022 posoudil v meziresortním připomínkovém řízení 169 materiálů legislativní i nelegislativní povahy, přičemž k řadě z nich uplatnil z hlediska své působnosti připomínky. NÚKIB se například prostřednictvím uplatněných připomínek podílel na přípravě návrhu novely zákona o ochraně utajovaných informací.

NÚKIB zajišťoval také činnosti v oblasti vládní agendy, a to předkládáním vlastních materiálů vládě, BRS či Výboru pro kybernetickou bezpečnost, aktualizací výkaznictví souladu právních předpisů v gesci NÚKIB s právními předpisy EU a řízením gescí NÚKIB k dokumentům EU legislativní i nelegislativní povahy.

3.10 Komunikace

NÚKIB pokračoval v nastavené komunikační strategii a budování vztahů s veřejností prostřednictvím sociálních sítí a webových stránek NÚKIB, jejichž prostřednictvím realizoval komunikační aktivity a kampaně. Mezi nejvíce rezonující témata patřily: dopady ruské agrese na Ukrajině, CZ PRES, transpozice evropské směrnice NIS2 do českého právního řádu a mechanismus posuzování bezpečnosti dodavatelů do strategicky významné infrastruktury ČR. Dále NÚKIB pravidelně a průběžně informoval o organizování akcí pro odbornou i širokou veřejnost, o činnosti zaměstnanců NÚKIB, kybernetických hrozbách a zranitelnostech, o rozšíření nabídky e-learningových kurzů na webu osveta.nukib.cz, měsíčních reportech o kybernetických incidentech a novinkách z oblasti výzkumu a vývoje.

3.11 Spolupráce, mezinárodní spolupráce

Vývoj v oblasti kybernetické bezpečnosti v ČR je do značné míry svázaný s vývojem v zahraničí a rozhodnutími přijímanými nejen na úrovni EU, ale i prostřednictvím dalších mezinárodních subjektů. NÚKIB zastupuje zájmy ČR v oblasti kybernetické bezpečnosti a diplomacie v řadě mezinárodních organizací a integračních uskupení. Významný podíl na rozvoji mezinárodní spolupráce má činnost cyber attaché, pracovníků NÚKIB, kteří působí při EU, NATO, v USA a v Izraeli. Činnost cyber attaché se dlouhodobě ukazuje jako velmi prospěšná a nenahraditelná, neboť tito pracovníci přispívají k udržování kontaktů a výměně informací s partnery v zahraničí, které nelze v dostatečné míře naplňovat z ČR.

Evropská unie

Rok 2022 byl v oblasti mezinárodní spolupráce ovlivněn zejména CZ PRES. První polovina roku proto byla věnována především intenzivním přípravám jak po obsahové, tak organizační stránce a zahrnovala množství jednání s partnery jak na národní, tak unijní úrovni. V Radě EU se NÚKIB podílí zejména na činnosti Horizontální pracovní skupiny pro kybernetické otázky (dále jen „HWPCI“), která se zabývá spoluprací na poli kybernetické bezpečnosti a diplomacie v rámci EU a které NÚKIB v tuto dobu předsedal.

Počínaje okamžikem převzetí předsednictví se NÚKIB na půdě Rady EU věnoval řadě legislativních i nelegislativních dokumentů v oblasti kybernetické bezpečnosti. Podařilo se dosáhnout obecného přístupu Rady EU k návrhu nařízení, kterým se stanoví opatření k zajištění vysoké společné úrovně kybernetické bezpečnosti v orgánech, institucích a jiných subjektech EU, tedy společné pozice všech členských států k tomuto návrhu. Započato bylo rovněž vyjednávání návrhu Aktu o kybernetické odolnosti, který stanovuje požadavky pro širokou škálu produktů s digitálními prvky s cílem zajistit jejich kybernetickou bezpečnost, a to v rámci jejich celého životního cyklu. Vzhledem k tomu, že uvedené nařízení bude mít významný dopad na trh s produkty obsahující digitální prvky, bylo téma během podzimu konzultováno nejen s národními partnery v rámci státní správy, ale také se zástupci soukromého sektoru, na něž regulace dolehne nejvíce.

Mimo uvedené legislativní návrhy se NÚKIB prioritně věnoval tématu posilování bezpečnosti dodavatelského řetězce. Hlavním úspěchem bylo přijetí závěrů Rady k bezpečnosti dodavatelského řetězce ICT, které byly iniciovány a na půdě EU vyjednány právě zástupci NÚKIB. Přijetím těchto závěrů všech 27 členských států EU potvrdilo důležitost tohoto tématu. NÚKIB během CZ PRES inicioval i pravidelné diskuze o unijním kybernetickém krizovém řízení, během kterých se členské státy zaměřily zejména na otázky výměny informací a posilování společného situačního povědomí.

Pozornost v Radě EU byla věnována i otázkám kybernetické diplomacie, na kterých NÚKIB úzce spolupracuje s MZV jakožto národním gestorem uvedené problematiky. Hlavní prioritou v této oblasti bylo téma strategického budování kybernetických kapacit ve třetích zemích. Diskuze na HWPCI se v rámci tohoto tématu zaměřily na pět regionů dle priorit EU – Východní sousedství a Ukrajina, západní Balkán, Latinská Amerika a Karibik, Indo-Pacifik a Afrika. Výstupem těchto diskuzí byl dokument předsednictví, který je shrnuje a nastiňuje další možný postup v této oblasti.

CZ PRES se kromě vlastní činnosti Rady EU též promítlo do chodu řady expertních skupin v oblasti kybernetické bezpečnosti, na jejichž fungování se NÚKIB rovněž aktivně podílel. Konkrétně se jedná o Skupinu pro spolupráci k NIS2, Síť styčných organizací pro řešení kybernetických krizí (EU-CyCLONE) či Síť CSIRT (Computer Security Incident Response Team).

NÚKIB i v roce 2022 nadále spolupracoval s ENISA, jejímž úkolem je přispívat k tvorbě a provádění politik a práva EU v oblasti kybernetické bezpečnosti. NÚKIB se zapojil do vybraných aktivit ENISA zejména prostřednictvím pracovních skupin a zapojil se do pilotního projektu na podporu připravenosti států EU a reakce na incidenty.

Nejvýznamnější událostí CZ PRES byla z pohledu NÚKIB dvoudenní předsednická konference EU Secure and Innovative Digital Future, na jejíž organizaci NÚKIB pracoval společně s MPO a Úřadem vlády, v koordinaci s MZV. První den konference s názvem Prague Cyber Security Conference 2022 byl v režii NÚKIB a navázal na tradici Prague 5G Security Conference konané v předchozích letech. Konference se fyzicky či virtuálně účastnilo přes 500 expertů na kybernetickou bezpečnost z více než 80 zemí světa. Hlavním tématem byla bezpečnost dodavatelského řetězce ICT, její vývoj, výzvy, které přináší, i možné způsoby realizace. Druhý den konference s názvem Towards a Secure and Innovative Ecosystem pak probíhal pod záštitou MPO a Úřadu vlády a věnoval se zejména bezpečnosti nových technologií, například umělé inteligenci či otázce bezpečných toků dat v rámci EU i mimo ni.

V rámci CZ PRES došlo k vůbec prvnímu neformálnímu setkání delegátů zemí EU a NATO, kdy se zástupci členských zemí z HWPCI Rady EU a Výboru pro kybernetickou obranu NATO sešli s cílem posílit spolupráci mezi oběma organizacemi.

NATO

NÚKIB se podílel na plnění aliančních závazků v oblasti kybernetické bezpečnosti a obrany prostřednictvím svého cyber attaché. Významným milníkem bylo historicky první jednání Severoatlantické rady ve formátu národních kybernetických koordinátorů, kterého se za ČR účastnil ředitel NÚKIB. Zástupci NÚKIB byli přítomni také na Cyber Defence Pledge Conference, kde byly hlavními tématy navyšování odolnosti a připravenosti NATO proti kybernetickým hrozbám a budoucí směřování aliančních závazků na poli kybernetické bezpečnosti a obrany.

NÚKIB také pokračoval v úzké spolupráci se CCD COE, jehož je aktivním členem.

Organizace spojených národů (dále jen „OSN“)

Společně s MZV se NÚKIB aktivně podílí na činnosti aktuálně nejvýznamnější platformy vztahující se ke kybernetické bezpečnosti, tzv. Open-Ended Working Group. 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.

Organizace pro hospodářskou spolupráci a rozvoj (dále jen „OECD“)

V OECD 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 držaných soukromým sektorem.

ČR je také členem 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.

Organizace pro bezpečnost a spolupráci v Evropě (dále jen „OBSE“)

V rámci OBSE v roce 2022 pokračovaly aktivity 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. NÚKIB se účastnil ve spolupráci s MZV zasedání IWG a podílel se na implementaci opatření.

Mezinárodní telekomunikační unie (dále jen „ITU“)

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 2022 sledoval a analyzoval dění zejména v oblasti standardizace telekomunikačních technologií, kybernetické bezpečnosti a AI, konkrétně pak v pracovních skupinách a účastí na konferencích.

Mezinárodní spolupráce v oblasti TEMPEST a TSCM

Zástupci NÚKIB se účastnili jednání pracovních skupin organizovaných generálním sekretariátem rady (dále jen „GSC“) ITTF a TSCM a pracovního setkání s NBÚ Slovenské republiky.

Významnou aktivitou NÚKIB bylo zorganizování EU TEMPEST Seminar Prague 2022, který se konal v rámci CZ PRES a byl zastřešený GSC. Akce se účastnilo na 80 příslušníků špičky TEMPEST komunity z 24 členských států EU, zástupci GSC, NATO a komerčních subjektů, kteří měli příležitost vyměnit si informace, znalosti a zkušenosti z oblasti své působnosti.

Rozvojová spolupráce

V roce 2022 se NÚKIB účastnil výroční Global Forum on Cyber Expertise (dále jen „GFCE“) v Haagu, kde se projednávaly aktivity GFCE, mimo jiné i v oblasti rozvojové spolupráce včetně regionu západního Balkánu. NÚKIB se aktivně účastnil i setkání členů EU CyberNet v Bruselu, kde vystupoval s příspěvkem ke kybernetické diplomacii a rozvojové spolupráci.

Bilaterální spolupráce

USA a Kanada

Hlavními tématy spolupráce s USA byla zejména bezpečnost dodavatelského řetězce, přípravy regulace v oblasti nahlašování incidentů, bezpečnost 5G sítí či Counter Ransomware Initiative, která je právě iniciativou USA a ke které se ČR připojila v roce 2021. Na úrovni zahraničních partnerů NÚKIB, například US Cybersecurity and Infrastructure Security Agency, probíhalo sdílení zkušeností s povinností hlášení incidentů či zájem ze strany USA o varování NÚKIB ve věci smartmeterů. Proběhla i setkání s partnery ze soukromého sektoru. Za účasti NÚKIB proběhl ve Washingtonu druhý ročník International Counter Ransomware Initiative Summit, který si klade za cíl prohloubit spolupráci mezi stejně smýšlejícími státy v oblasti prevence, detekce a reakce na narůstající hrozbu ransomware a zhodnotit dosavadní pokrok.

V roce 2022 byla navázána bližší spolupráce s Kanadským centrem pro kybernetickou bezpečnost a Týmem kybernetické diplomacie z Global Affairs Canada.

Izrael

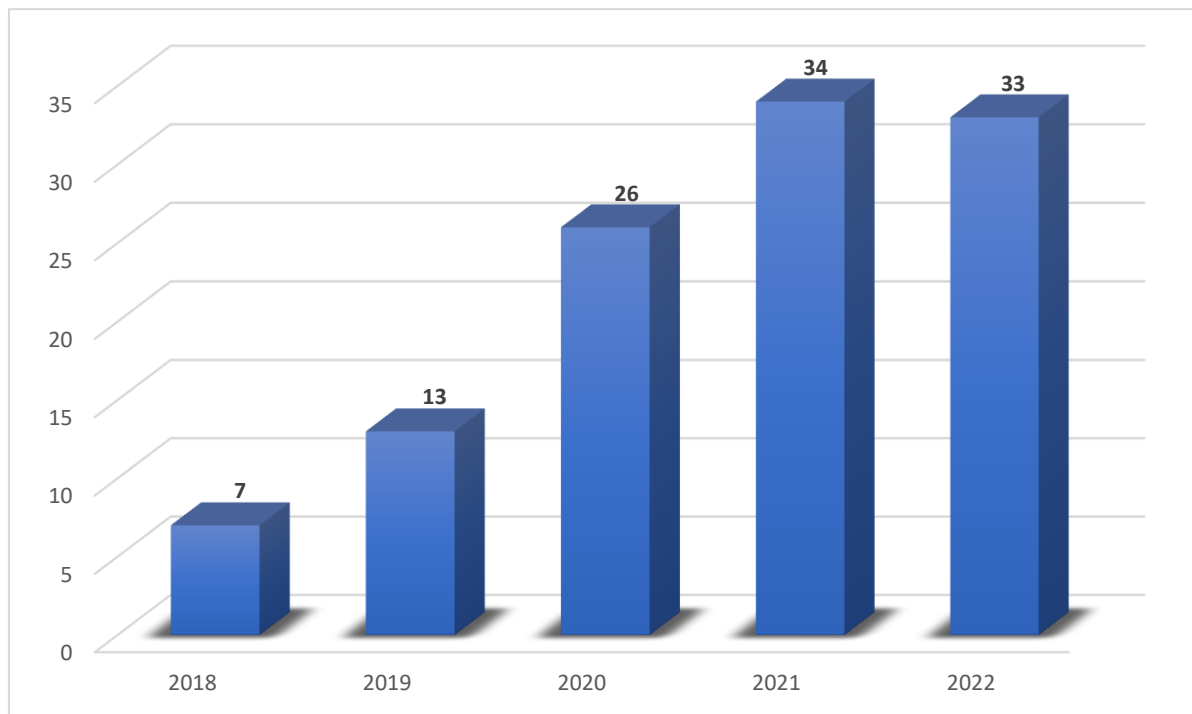
Také v roce 2022 pokračovala spolupráce mezi NÚKIB a partnerským úřadem Israel National Cyber Directorate. Zejména se jednalo o výměnu informací a strukturovaný dialog v oblastech kybernetické bezpečnosti (regulace a právní rámec kybernetické bezpečnosti, vzdělávání a zvyšování bezpečnostního povědomí, koordinace společných postojů v OECD, regulace cloud computingu či operační a analytická spolupráce). Posílena byla i spolupráce mezi oběma CERT týmy a CTI spolupráce. V červnu 2022 NÚKIB zorganizoval návštěvu delegace místopředsedy vlády pro digitalizaci na prestižní konferenci Cyber Week 2022.

Spolupráce s vysokými školami a odborné praxe studentů škol

Vedle pracovních příležitostí poskytuje NÚKIB za účelem přípravy na budoucí povolání praktické stáže pro vysokoškolské studenty a také umožňuje absolvování odborné praxe studentům některých středních škol. Ze středních škol je nejužší spolupráce navázána se Střední školou informatiky, poštovníctví a finančnictví Brno, z níž odbornou praxi vykonávalo 5 studentů oboru kybernetická bezpečnost. V roce 2022 pak byly nově navázány smlouvy o spolupráci se Smíchovskou střední a průmyslovou školou a gymnáziem Praha a se Střední školou technickou Brno. Z vysokých škol byli v roce 2022 nově na odbornou stáž přijati studenti King's College London.

V roce 2022 absolvovalo celkem 33 studentů stáže technického, či politickobezpečnostního zaměření a také stáže v rámci CZ PRES. Součástí spolupráce se studenty byly také pravidelné odborné konzultace diplomových a seminárních prací.

Počet stážistů na odborné praxi



3.12 Ekonomické zabezpečení

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

Rozpočet NÚKIB je tvořen příjmy a výdaji.

Příjmy

Schválený rozpočet celkových příjmů NÚKIB byl v roce 2022 ve výši 400 000 Kč. Celkové příjmy kapitoly za rok 2022 byly ve výši 318 468,95 Kč. Tyto příjmy tvořily ostatní nedaňové příjmy. Část příjmů ve výši 29 000 Kč byla za příjem pokut ze správního řízení podle zákona o ochraně utajovaných informací. Významnou položkou byly neplánované přijaté nekapitálové příspěvky a náhrady v objemu 266 499,97 Kč.

Přehled plnění rozpočtu příjmů v roce 2022 (vyjádření v tis. Kč)

	2021	2022			Plnění k rozpočtu po změnách (%)	Rozdíl skutečností
	Skutečnost	Schválený rozpočet	Rozpočet po změnách	Skutečnost		
Příjmy celkem	1 042,99	400,00	400,00	318,47	79,62	-724,52
Podskupení						
211 – Příjem z vlastní činnosti	0,00	200,00	200,00	0,00	0,00	0,00
221 – Přijaté sankční platby	843,00	200,00	200,00	29,00	14,50	-814,00
232 – Ostatní nedaňové příjmy	173,63	0,00	0,00	266,50	0,00	92,90
413 – Neinvestiční převody z vlastních fondů a ve vztahu k útvarům bez právní osobnosti	26,36	0,00	0,00	22,97	0,00	-3,40

Výdaje

Schválený rozpočet celkových výdajů NÚKIB byl ve výši 529 141 429 Kč.

Během roku byl schválený rozpočet upravován rozpočtovými opatřeními Ministerstva financí (dále jen „MF“) na objem 582 331 262 Kč. Dále byl rozpočet snížen vázáním prostředků na platy a příslušenství za neobsazená pracovní místa v objemu 4 318 277 Kč, a to na částku 578 012 985 Kč. K 31. 12. 2022 bylo z upraveného rozpočtu celkových výdajů vyčerpáno 527 282 456,42 Kč, což je 90,6 %. V průběhu roku 2022 bylo provedeno 11 rozpočtových opatření MF (včetně 4 rozpočtových opatření v rámci vázání prostředků státního rozpočtu za neobsazená pracovní místa).

Konečný rozpočet celkových výdajů kapitoly za rok 2022, tedy rozpočet včetně zapojených nároků z nespotřebovaných výdajů (dále jen „NNV“) ve výši 67 090 161,65 Kč, byl v objemu 645 103 146,65 Kč. Čerpání konečného rozpočtu ve výši 592 817 895,80 Kč, tedy na 91,9 %.

Základní přehled plnění rozpočtu výdajů v roce 2022 (vyjádření v tis. Kč)

	2021	2022				Plnění k rozpočtu po změnách (%)	Plnění ke konečnému u rozpočtu (%)	Rozdíl skutečností
	Skutečnost	Schválený rozpočet	Rozpočet po změnách	Konečný rozpočet	Skutečnost			
Výdaje celkem	567 589,37	529 141,43	582 331,26	645 103,15	592 817,90	101,80	91,90	25 228,52
Běžné výdaje	404 708,88	399 738,54	452 928,38	470 392,20	441 481,74	97,50	93,90	36 772,86
z toho platy včetně příslušenství	228 716,56	261 133,81	271 355,78	268 824,82	267 024,24	98,40	99,30	38 307,68
z toho běžné výdaje bez platů a příslušenství	175 992,32	138 604,74	181 572,60	201 567,38	174 457,49	96,10	86,60	- 1 534,83
Kapitálové výdaje	162 880,50	129 402,89	129 402,89	174 710,95	151 336,16	116,90	86,60	- 11 544,64

Výdaje na platy a příslušenství

Výdaje na platy, ostatní platby za provedenou práci a příslušenství byly rozpočtovány ve výši 261 133 809 Kč pro 311 pracovních míst. V průběhu roku 2022 došlo k navýšení celkem o 20 pracovních míst.

Vázáním prostředků na platy a příslušenství za neobsazená pracovní místa v objemu 4 318 277 Kč byl rozpočet snížen na částku 256 815 532 Kč. Konečný rozpočet výdajů na platy, ostatní platby za provedenou práci a příslušenství ve výši 268 824 815,32 Kč byl čerpán v objemu 267 024 244,78 Kč, tedy v relativním vyjádření na 99,3 %.

V období od 1. 1. 2022 do 31. 12. 2022 nastoupilo na NÚKIB 96 nových zaměstnanců a 36 zaměstnanců skončilo pracovní poměr. Průměrný plat, k průměrnému ročnímu přepočtenému počtu 293,26 zaměstnanců, činil 55 640 Kč měsíčně.

Běžné výdaje

Běžné výdaje (bez výdajů na platy, ostatní platby za provedenou práci a příslušenství) byly rozpočtovány ve výši 138 604 735 Kč.

Rozpočtovými opatřeními byly upraveny na 181 572 597 Kč. Zapojením NNV byly upraveny na konečný rozpočet ve výši 201 567 381,03 Kč. Konečný rozpočet běžných výdajů byl čerpán v objemu 174 457 493,28 Kč, v relativním vyjádření na 86,6 %.

Výdaje na opatření související s řešením epidemie covid-19 činily objem 100 000 Kč. Jednalo se o nákup antigenních testů pro samotestování zaměstnanců a proplácení vybraných externích PCR testů zaměstnancům.

Kapitálové výdaje

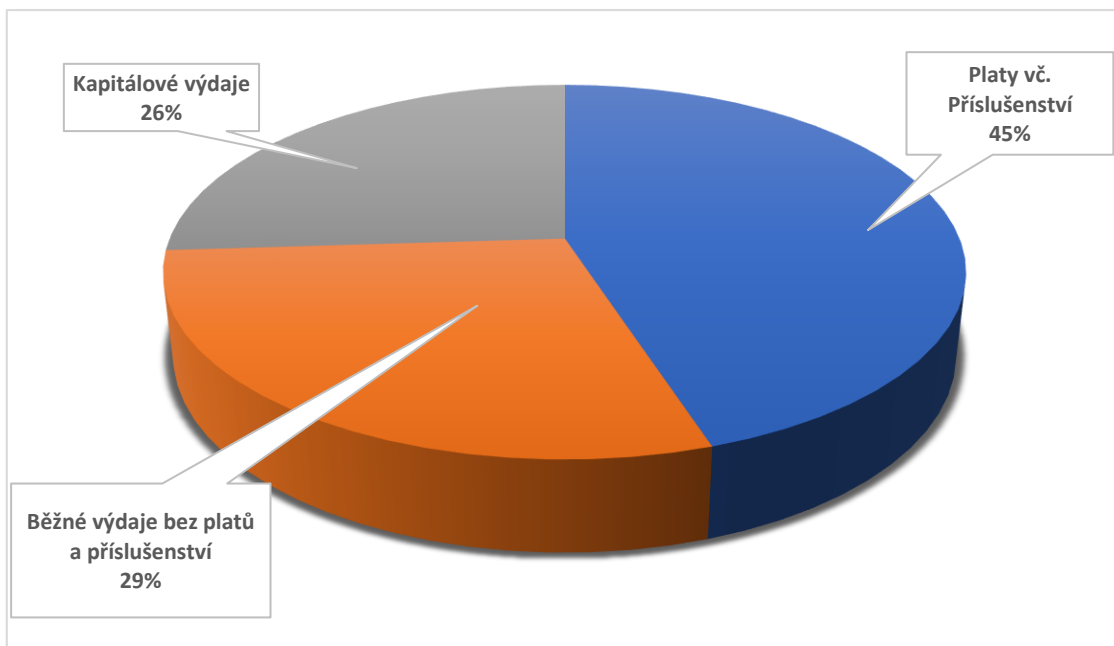
Kapitálové výdaje vedené ve Správě majetku ve vlastnictví státu (dále jen „SMVS“) byly rozpočtovány ve výši 129 402 885 Kč.

Zapojením NNV pak byly kapitálové výdaje upraveny na konečný rozpočet výdajů v SMVS v objemu 174 710 950,03 Kč.

Konečný rozpočet kapitálových výdajů byl čerpán v objemu 151 336 157,74 Kč, v relativním vyjádření 86,6 %.

Nejvýznamnější objem finančních prostředků byl vynaložen na nemovitou infrastrukturu ve výši 93 393 090 Kč. Dále bylo vynaloženo 35 480 730 Kč na dobudování, posílení a obnovu ICT infrastruktury NÚKIB a 16 456 370 Kč na projekty v rámci Výzkumu a vývoje, tj. kryptografické techniky, měřicí techniky nebo nehmotných výsledků a 6 005 970 Kč na zabezpečovací techniku.

Podíl jednotlivých složek čerpání na celkových výdajích 2022

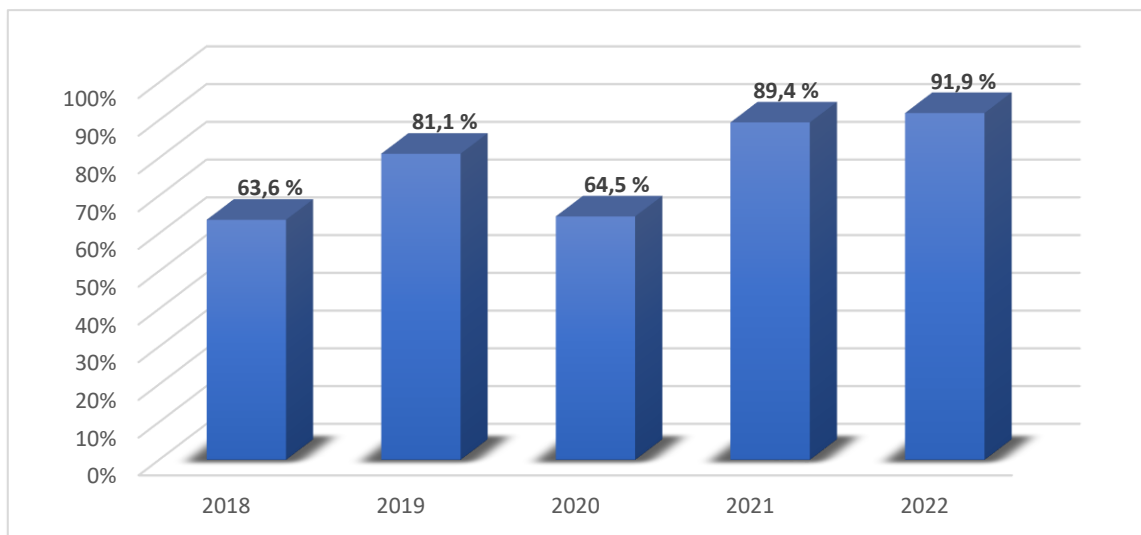


Evidence nároků z nespotřebovaných výdajů

Počáteční stav nároků z nespotřebovaných výdajů k 1. 1. 2022 byl ve výši 67 090 161,65 Kč. Celkem za rok 2022 byly vyčerpány z NNV finanční prostředky v objemu 65 535 439,38 Kč. K 31. 12. 2022 činí zůstatek nároků z nespotřebovaných výdajů částku 1 554 722,27 Kč. K 1. 1. 2023 činí stav NNV 52 285 250,85 Kč.

Všechny nečerpané NNV plánuje NÚKIB využít v roce 2023, a to včetně účelově určených finančních prostředků nevyčerpaných z roku 2022 na zapojení občanů ČR do civilních misí EU a dalších mezinárodních vládních organizací a také účelově určených finančních prostředků nevyčerpaných z roku 2022 na navýšení běžných výdajů rozpočtu kapitoly NÚKIB.

Vývoj čerpání rozpočtu výdajů v letech 2018 až 2022



3.13 Investice a rozvoj

V roce 2022 pokračoval NÚKIB v přípravě a realizaci celé řady významných investičních akcí, které zabezpečovaly nemovitou strukturu nezbytnou pro činnost rozvíjejícího se NÚKIB.

Objekt Cejl, Brno:

V rámci rozšiřování kancelářských kapacit objektu Cejl pro nově nastupující zaměstnance byla dokončena rekonstrukce přízemních prostor. Celkem bylo vybudováno 38 kancelářských míst.

Objekt Gorkého, Brno:

V průběhu roku 2022 pokračovala kompletní rekonstrukce, dle projektové dokumentace, zohledňující bezpečnostní a technické požadavky zaměstnanců NÚKIB. Do konce roku byly realizovány dokončovací stavební práce a vybudováno 86 kancelářských míst.

Administrativní budova NÚKIB, Brno - Černá Pole:

Objekt budovaný v souladu s vládou schválenou Konceptí rozvoje NÚKIB. Proběhlo zpracování studie stavby, která byla v lednu schválena vedením NÚKIB. Následně byla zpracovateli projektové dokumentace předána výzva na započítání prací na dokumentaci pro stavební povolení. V prosinci byla vedením NÚKIB schválena dokumentace pro stavební povolení. Poté byla zpracovateli dokumentace zaslána výzva na započítání prací na dokumentaci pro provedení stavby.

Objekt Olšanská, Praha:

V objektu Olšanská proběhla celková rekonstrukce jednoho patra, kdy dodavatel stavby předal dokončené dílo v měsíci září. Celkem byly vybudovány prostory pro 45 zaměstnanců. Následně proběhlo nastavování a testování bezpečnostních systémů a vybavení kancelářských prostor. Koncem roku byly prostory připravené pro nastěhování zaměstnanců dislokovaných v objektu NBÚ.

Objekt „Paťanka-Juliska“, Praha:

V lednu 2022 bylo vydáno stavební povolení na částečnou rekonstrukci tohoto objektu a následně realizováno výběrové řízení na dodavatele stavebních prací. V květnu bylo předáno staveniště dodavateli a ke konci měsíce srpna proběhla kolaudace objektu. Dodavatel stavby předal dílo během září. Následně proběhlo v objektu nastavení bezpečnostních systémů a vybavení kancelářských prostor. Harmonogram prací směřoval k tomu, aby byly prostory pro zaměstnance, dislokované v objektu NBÚ, připraveny na počátku roku 2023.

3.14 Personální zabezpečení

NÚKIB měl k 31. 12. 2022 319 zaměstnanců na systemizovaných pracovních místech. V souladu s Konceptí rozvoje NÚKIB došlo od 1. 1. 2022 k navýšení počtu pracovních míst NÚKIB o 41. Na podzim roku 2022 pak NÚKIB obdržel dalších 20 nových pracovních míst. Všechna uvedená pracovní místa byla postupně obsazována novými zaměstnanci. Do pracovního poměru v období od 1. 1. 2022 do 31. 12. 2022 bylo přijato 96 nových zaměstnanců. Dalších 8 zaměstnanců vykonávalo činnost na základě uzavřených dohod o pracovní činnosti a s 18 osobami byla uzavřena dohoda o provedení práce.

Základní přehled

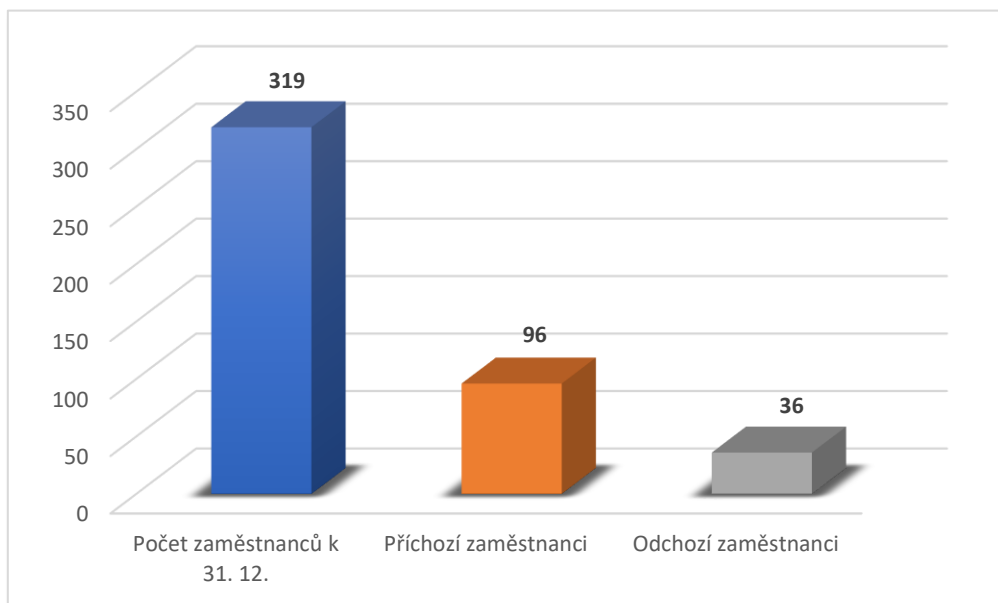
Personální zabezpečení	počet
Evidenční stav zaměstnanců na systemizovaných pracovních místech k 31. 12. 2022 ve fyzických počtech	319
Počet zaměstnanců dočasně mimo systemizovaná pracovní místa (mateřská a rodičovská dovolená, uvolnění k výkonu veřejné funkce)	15
Ukončení pracovních poměrů v průběhu roku 2022	36
Nástupy do pracovního poměru v průběhu roku 2022	96
Návraty z mateřské dovolené, z rodičovské dovolené a neplaceného volna v průběhu roku 2022	2
Odchody na mateřskou či rodičovskou dovolenou v průběhu roku 2022	6

Do konce roku 2022 ukončilo pracovní poměr 36 zaměstnanců, tj. 11,96 % z počtu zaměstnanců evidovaných na systemizovaných pracovních místech.

Přehled způsobů ukončení pracovních poměrů v roce 2022

Způsob ukončení pracovního poměru	počet
zrušení ve zkušební době zaměstnancem § 66 ZP	3
zrušení ve zkušební době organizací § 66 ZP	1
výpověď zaměstnance § 50 ZP, odst. 3	12
uplynutím doby určité § 65 ZP	13
dohodou § 49 ZP	6
výpověď organizace § 52, písm. f ZP	1
Celkem	36

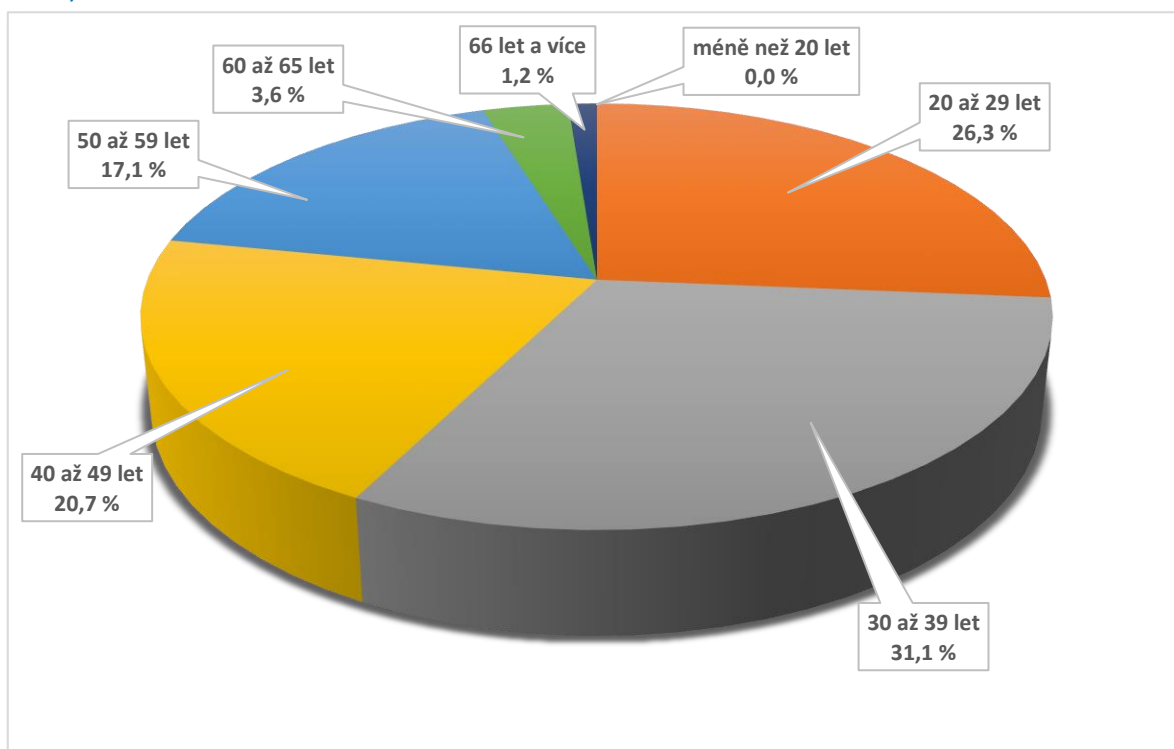
Nástupy a odchody zaměstnanců v roce 2022



Věková struktura zaměstnanců k 31. 12. 2022 (včetně zaměstnanců dočasně mimo systemizovaná pracovní místa)

Věková kategorie	Počet zaměstnanců k 31. 12.2022	Podíl zaměstnanců v %	Z toho	
			muži	ženy
méně než 20 let	0	0,00 %	0	0
20 až 29 let	88	26,35 %	52	36
30 až 39 let	104	31,14 %	66	38
40 až 49 let	69	20,66 %	39	30
50 až 59 let	57	17,07 %	38	19
60 až 65 let	12	3,59 %	10	2
66 a více let	4	1,20 %	3	1
Celkem	334	100,00 %	208	126

Struktura zaměstnanců podle věku k 31. 12. 2022 (včetně zaměstnanců mimo systemizovaná místa)



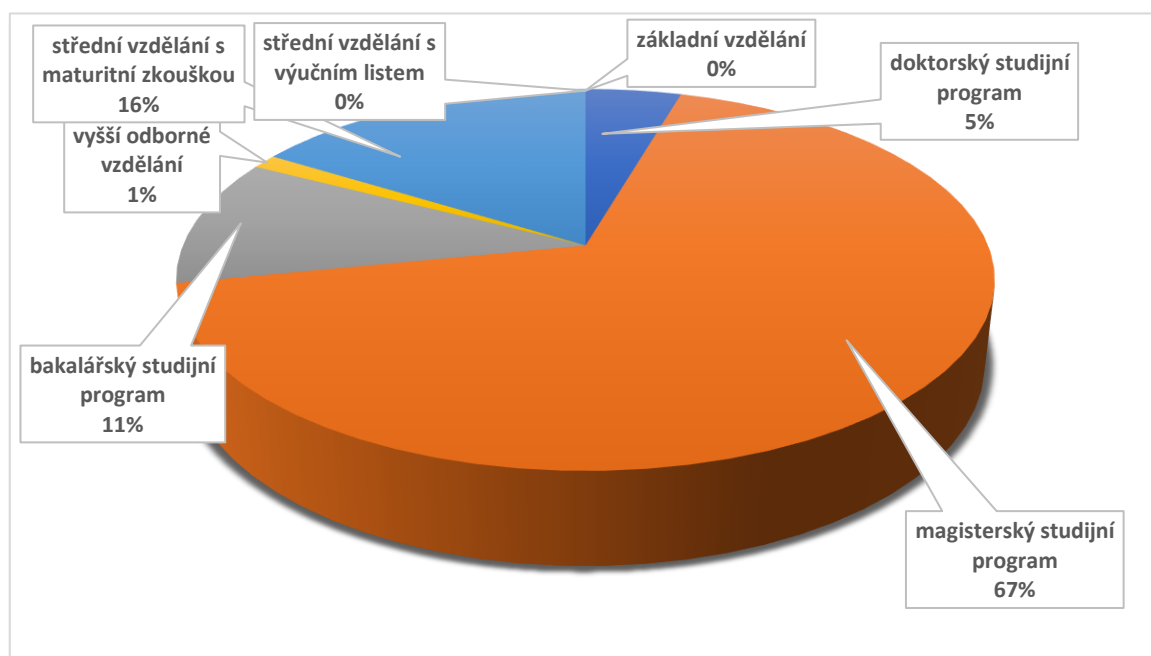
Kvalifikační struktura zaměstnanců

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

Kvalifikační struktura zaměstnanců

Dosažené vzdělání k 31. 12. 2022 (zahrnuti jsou též zaměstnanci dočasně na MD, RD a uvolnění k výkonu veřejné funkce)	Počet zaměstnanců k 31. 12. 2022	Procentní struktura
v doktorském studijním programu	15	4,49 %
v magisterském studijním programu	225	67,37 %
v bakalářském studijním programu	36	10,78 %
vyšší odborné vzdělání	4	1,20 %
střední vzdělání s maturitní zkouškou	54	16,17 %
střední vzdělání s výučním listem	0	0,00 %
základní vzdělání	0	0,00 %
Celkem	334	100 %

Dosažené vzdělání zaměstnanců NÚKIB k 31. 12. 2022



Vzdělávání a rozvoj zaměstnanců

Také v uplynulém roce NÚKIB pokračoval v naplňování cíle mít vzdělané, kvalifikované a odborné zaměstnance, schopné aplikovat nabyté poznatky a zkušenosti při výkonu jejich pracovních činností. Vzdělávání bylo zabezpečováno formou individuálních i hromadných vzdělávacích akcí, realizací 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, MS PowerPoint. Další oblast školení byla zaměřena na změny v legislativě, veřejných zakázkách, novinkách v oblasti ekonomiky, personalistiky, práva a manažerských dovedností. Zaměstnanci NÚKIB se také účastnili zahraničních školení kybernetické bezpečnosti SANS, školení od NATO CCD COE a také školení Searching the Chinese Internet od i-intelligence a reprezentovali NÚKIB na mnoha tuzemských i zahraničních konferencích, například RSA Conference 2022 či International Conference on Cyber Conflict (CyCon), Eurocrypt 2022, CYB3R Days 2022.

Zaměstnávání osob se zdravotním postižením

V roce 2022 měl NÚKIB naplnit povinný podíl v zaměstnávání osob se zdravotním postižením ve výši 11,71 osoby. Plnění povinného podílu bylo splněno zaměstnáváním osob se zdravotním postižením ve výši 1,91 osoby a odběrem výrobků a služeb, který odpovídá v přepočtu zaměstnání 11,15 osob.

3.15 Interní audit a vnitřní kontrola

V průběhu roku byl dokončen následný audit zaměřený na prověření realizace opatření k odstranění nedostatků zjištěných v průběhu auditů vykonaných v roce 2020 a mimořádný audit organizace příprav a realizace Prague 5G Security Conference 2021. Dále byl realizován následný audit zaměřený na prověření realizace opatření k odstranění nedostatků zjištěných v průběhu auditů vykonaných v roce 2021 a mimořádný audit kontrolních zjištění z kontroly Nejvyššího kontrolního úřadu č. 19/26 – Budování kybernetické bezpečnosti ČR.

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 únoru roku 2022 byla odeslána MF zpráva o výsledcích finančních kontrol na NÚKIB za předchozí kalendářní rok.

Finanční kontrolu vykonávanou podle zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů tvoří u NÚKIB tyto složky:

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

V průběhu roku 2022 byl zajišťován výkon řídicí kontroly jednotlivými příkazci operací, hlavní účetní a správcem rozpočtu. V rámci své působnosti prováděly jmenované osoby finanční řídicí kontroly při hospodaření s finančními prostředky na příslušných rozpočtových položkách NÚKIB v rámci jeho rozpočtové skladby. Mimo výkon řídicí 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 řídicí 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 veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů a vyhlášky č. 416/2004 Sb., kterou se provádí zákon č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění zákona č. 309/2002 Sb., zákona č. 320/2002 Sb. a zákona č. 123/2003 Sb., ve znění pozdějších předpisů. Výsledky finančních kontrol ukazují, že nastavený vnitřní kontrolní systém NÚKIB je funkční a zajišťuje jeho účinné a kvalitní řízení. Napomáhá včas odhalovat případné nedostatky a přijímat nápravná opatření.

Při uskutečněných řídicích 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.

4. Seznam použitých zkratk

AI	Artificial Intelligence (umělá inteligence)
BIVOJ	Bezpečný, inovativní, pro veřejnou správu, odolný, jednotný
BRS	Bezpečnostní rada státu
CCD COE	Cooperative Cyber Defence Centre of Excellence (NATO Centrum excelence pro kybernetickou obranu)
CD	Compact disk
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
CTI	Cyber Threat Intelligence
CVD	Coordinated Vulnerability Disclosure (Koordinované zveřejňování zranitelností)
ČR	Česká republika
CZ PRES	Předsednictví České republiky v Radě Evropské unie
DDoS	Distributed Denial of Service
ENISA	European Union Agency for Cybersecurity (Agentura Evropské unie pro kybernetickou bezpečnost)
EU	Evropská unie
EU-CyCLONe	European Cyber Crisis Liaison Organisation Network (Síť styčných organizací pro řešení kybernetických krizí)
GFCE	Global Forum on Cyber Expertise
GRON	Galileo Robust Operation Network
GSMC	Bezpečnostní a monitorovací centrum programu Galileo
GSC	General Secretariat of the Council (Generální sekretariát rady ITTF a TSCM)
HWPCI	Horizontal Working Party on Cyber Issues
ICT	Information and Communication Technologies (Informační a komunikační technologie)
IS	Informační systémy
ITTF	Implementation Tempest Task Force
ITU	International Telecommunication Union (Mezinárodní telekomunikační unie)
IWG	Informal Working Group
KM	Kryptografický materiál
MD	Mateřská dovolená
MPO	Ministerstvo průmyslu a obchodu
MV	Ministerstvo vnitra
MZV	Ministerstvo zahraničních věcí
NATO	North Atlantic Treaty Organization (Severoatlantická aliance)
NBÚ	Národní bezpečnostní úřad
NDS	Národní distribuční středisko
NIS2	Network and Information Security 2 (Směrnice Evropského parlamentu a Rady Evropské unie o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii)
NNV	Nároky z nespotřebovaných výdajů
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OBSE	Organizace pro bezpečnost a spolupráci v Evropě
OECD	Organisation for Economic Cooperation and Development (Organizace pro hospodářskou spolupráci a rozvoj)
OSN	Organizace spojených národů

PRS	Public Regulated Service (Veřejně regulovaná služba Evropského programu družicové navigace Galileo)
RD	Rodičovská dovolená
SDE	Security in the Digital Economy
SMVS	Správa majetku ve vlastnictví státu
TEMPEST	Telecommunication Electronics Materials Protected from Emanating Spurious Transmissions
TSCM	Technical Surveillance Counter Measures
USA	United States of America (Spojené státy americké)