NÚKIB

ZPRÁVA O ČINNOSTI 2024

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST

OBSAH

1. Úvodní slovo ředitele

Vážené dámy, vážení pánové,

rok 2024, podobně jako předchozí roky, přinesl Národnímu úřadu pro kybernetickou a informační bezpečnosti řadu nových výzev, které jsme museli zvládat v prostředí stále komplexnějších bezpečnostních hrozeb a rostoucích požadavků na kybernetickou a informační bezpečnost. Kolegyně a kolegové se museli vypořádat nejen s přetlakem množství agend a s požadavky na kapacity ke zvládnutí zadaných úkolů, ale také s nutností pružně reagovat na změny v prioritách a v budování klíčových schopností NÚKIB. Za osobní angažovanost, iniciativu nad rámec pracovních povinností a společné úsilí posunout NÚKIB zase o kus dál chci na úvod všem poděkovat.

Mezi hlavní priority NÚKIB na rok 2024 patřily zejména práce na návrhu nového zákona o kybernetické bezpečnosti (dále jen „nZKB“) a příprava souvisejících interních procesů, dále obnova a rozvoj klíčových složek infrastruktury informačních technologií a stabilizace personální situace u problematicky obsazovaných vysoce odborných pracovních pozic.

Téma nZKB rezonovalo nejen v odborné komunitě a u regulovaných subjektů, ale i u široké veřejnosti. Transparentní komunikace k výkladu znění zákona jako takového a informování o výsledcích projednávání zákona legislativní radou vlády, Poslaneckou sněmovnou České republiky a určenými výbory se uskutečňovala skrze média, na konferencích, workshopech i během nespočtu individuálních konzultací. Klíčovým projektem bylo i vytvoření, pilotní spuštění a testování komunikační platformy „Portál NÚKIB“, vyvíjené vlastními kapacitami.

V legislativní oblasti probíhal také proces přípravy a schválení čtyř prováděcích právních předpisů k zákonu o ochraně utajovaných informací, které byly ke konci roku úspěšně zveřejněny ve Sbírce zákonů.

Díky aktivitám NÚKIB se Česká republika také stala jednou z prvních zemí Evropské unie, která zprovoznila technologii umožňující komunikaci s bezpečnostním a monitorovacím centrem programu Galileo a zároveň získala schopnost řídit přístup k veřejné službě družicové navigace.

Neměnnou prioritou byla personální práce. Tedy vytváření co nejlepších pracovních podmínek, zavádění atraktivních benefitů a hledání cest, jak zaujmout talentované odborníky i v prostředí, kde z hlediska finančního ohodnocení nejsme schopni konkurovat soukromému sektoru. O to více si vážím všech stávajících kolegyň a kolegů, kteří do práce přinášejí svou vysokou odbornost, loajalitu a smysl pro službu a bezpečnost státu.

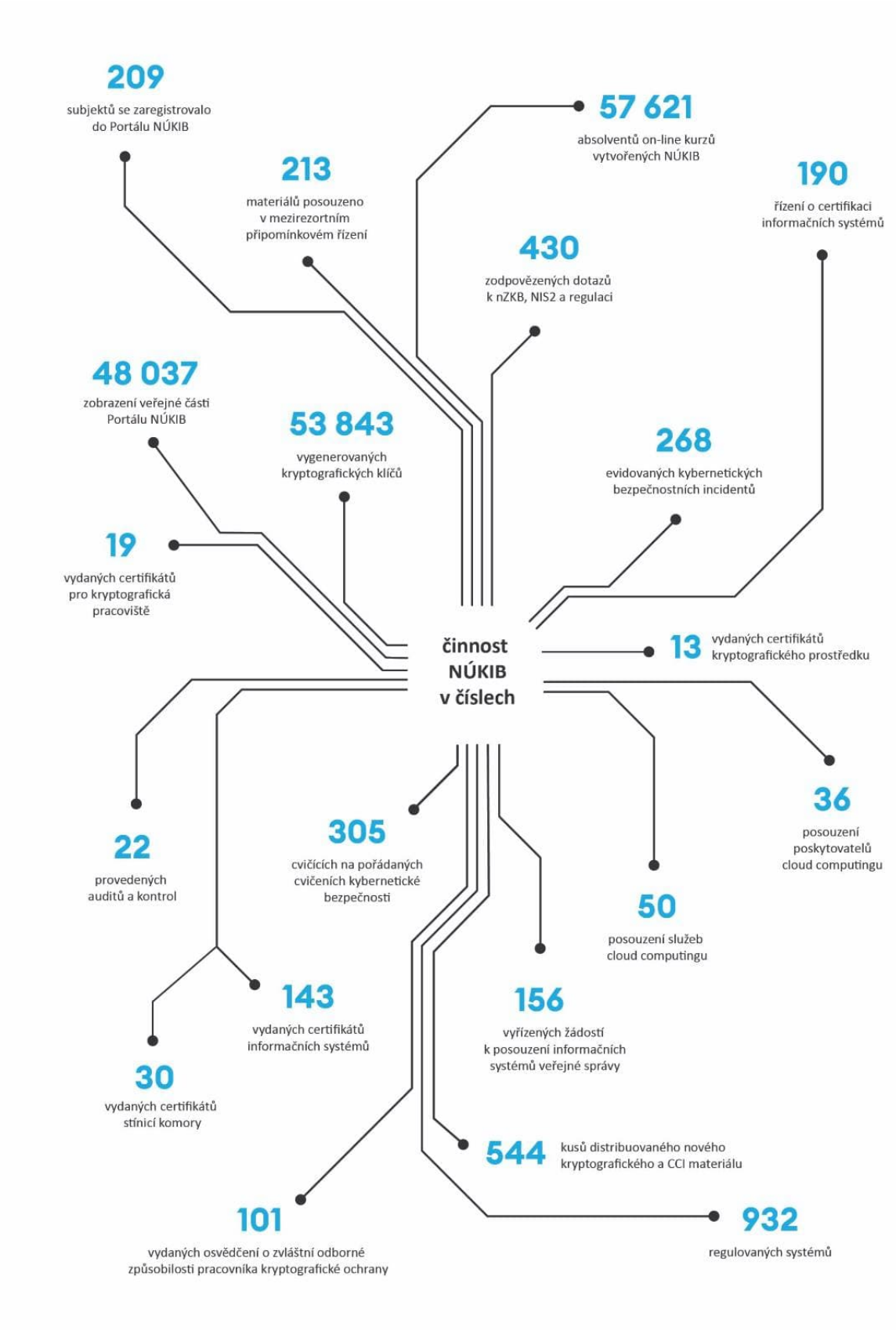
V neposlední řadě v průběhu roku vyvstaly nové výzvy v podobě implementace unijní legislativy Cyber Resilience Act (nařízení Evropské unie definující standardy produktů s digitálními prvky), dále využívání umělé inteligence (přinášející zásadní změny a příležitosti) nebo nástup kvantové technologie (představující jednu z nejrevolučnějších oblastí současného vědeckého a technologického výzkumu).

Uvedené příklady jsou jen výsečí činností, které reflektují společné úsilí v posilování bezpečnosti a odolnosti České republiky v kyberprostoru a ochrany našich občanů.

Děkuji za Váš zájem o naši činnost.

Ing. Lukáš Kintr
ředitel Národního úřadu pro kybernetickou a informační bezpečnost

2. Činnost NÚKIB v číslech



3. Oblasti činnosti

3.1 Strategie a politiky

Stěžejní součástí plnění role národního gestora pro oblast kybernetické bezpečnosti je koordinovat tuto agendu na úrovni státní správy a uvádět aktivity státní správy do souladu s cíli Národní strategie kybernetické bezpečnosti. Za tímto účelem NÚKIB systematicky rozvíjí partnerství napříč veřejnou správou, akademickou sférou, soukromým sektorem a mezinárodními partnery. V uplynulém období se NÚKIB aktivně podílel na přípravě klíčových strategických dokumentů a přispíval k odborné debatě v rámci řady pracovních skupin. Mezi nejvýznamnější aktivity NÚKIB za rok 2024 v této oblasti patří následující:

Nová Národní strategie kybernetické bezpečnosti

NÚKIB se v roce 2024 naplno ponořil do příprav nové Národní strategie kybernetické bezpečnosti, vrcholného národního strategického dokumentu České republiky (dále jen „ČR“) v oblasti kybernetické bezpečnosti. Po prvotních konzultacích požádal NÚKIB o vstupy zástupce soukromého sektoru, akademické sféry, neziskových organizací a zájmových skupin. Byla také vypsána veřejná výzva umožňující vstupy široké veřejnosti. Klíčovým krokem v projektu bylo ustanovení mezirezortní pracovní skupiny, do níž se zapojilo více než 27 institucí zejména ze státní správy a která pomohla dotvořit obsah dokumentu. Předpokládané přijetí nové Národní strategie kybernetické bezpečnosti se očekává ve druhém pololetí roku 2025.

Projekt BIVOJ

V průběhu roku 2024 pokračovala příprava projektu BIVOJ. Projekt představuje komplexní bezpečnostní program, jehož cílem je zajistit centrální správu a řízení bezpečnosti sdílených informačních a komunikačních systémů a služeb organizací veřejného sektoru ČR. Koordinátorem projektu byl i v roce 2024 NÚKIB a úzce na něm spolupracovaly další instituce, jako je Vojenské zpravodajství (dále jen „VZ“), Ministerstvo vnitra (dále jen „MV“), Ministerstvo financí (dále jen „MF“) a Ministerstvo obrany (dále jen „MO“). V průběhu roku 2024 byla zpracována studie proveditelnosti projektu a proběhly přípravy na studie proveditelnosti jeho komponent. Zpracované výstupy byly připraveny pro Bezpečnostní radu státu (dále jen „BRS“) k rozhodnutí o dalším směřování projektu, včetně předání jeho gestorství.

Projekt Koordinované zveřejňování zranitelností (dále jen „CVD“)

V roce 2024 se NÚKIB zaměřil na vyřešení specifických právních aspektů spojených s CVD, zejména v oblasti trestního práva a ochrany osobních údajů. Problematiku konzultoval se zahraničními partnery, mimo jiné s izraelským Israel National Cyber Directorate (dále jen „INCD“). Současně probíhaly práce na implementaci role koordinátora v rámci vládního CERT v souladu s požadavky směrnice Evropského parlamentu a Rady 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“) a návrhu nZKB. Dále byly finalizovány práce na implementaci CVD na systém využívaný NÚKIB. Zavedením CVD ve svých systémech chce

NÚKIB jít příkladem dalším subjektům a zároveň získat data a zkušenosti, ze kterých bude moci vycházet při rozvoji národní politiky CVD a relevantních mezinárodních dokumentů.

Národní politika kryptografické ochrany utajovaných informací

V průběhu roku 2024 NÚKIB finalizoval návrh Národní politiky kryptografické ochrany utajovaných informací, který v listopadu schválila BRS. Stanovení strategického směřování v oblasti kryptografické ochrany utajovaných informací hraje zásadní roli při plnění mezinárodních závazků ČR v rámci Evropské unie (dále jen „EU“) a Severoatlantické aliance (dále jen „NATO“) a je rovněž významné pro společnosti, jež vyvíjejí a vyrábějí kryptografické prostředky. Národní politika kryptografické ochrany utajovaných informací je platná do roku 2030 a stanovuje výhled do roku 2040. V roce 2025 bude připraven její implementační plán, který přenese cíle politiky do konkrétních kroků.

Koncepce ochrany neutajovaných informací citlivé povahy

Návrh koncepce byl v průběhu roku finalizován a v listopadu schválen BRS. Koncepce se skládá z analytické a strategické části a navrhuje konkrétní opatření k posílení bezpečnosti práce s citlivými neutajovanými informacemi. Gestorem implementace koncepce bylo určeno MV. Dalším krokem je ve spolupráci gestora NÚKIB a MO připravit a předložit vládě ČR konkrétní návrhy realizace zvoleného řešení, včetně jednotného systému klasifikace, označování a ochrany neutajovaných informací, a příslušných legislativních změn.

Projekt Kyberliga

Projekt Kyberliga si klade za cíl zapojit dobrovolníky z řad kybernetických expertů a expertek a institucionalizovat jejich využití při zajišťování kybernetické bezpečnosti. V roce 2024 rozpracoval NÚKIB vybranou variantu rozvoje projektu Kyberliga do podoby konkrétního řešení včetně administrativního a právního rámce a technického uchopení projektu. Oficiální spuštění projektu se předpokládá v druhé polovině roku 2025.

3.2 Vyhodnocení a řešení kybernetických bezpečnostních událostí a incidentů

NÚKIB v roce 2024 evidoval dosud největší počet kyberbezpečnostních incidentů, a to 268. Jedná se však o nepatrný nárůst oproti předešlému roku a závažnost dopadů evidovaných incidentů nadále klesá. V roce 2024 NÚKIB evidoval pouze 1 velmi významný incident a 18 významných incidentů.

Významnou část incidentů tvořily DDoS útoky a pokračující vlny těchto útoků vedených zejména ruskojazyčnou hacktivistickou skupinou NoName057(16). Zaznamenané útoky neměly závažnější dopady na zasažené subjekty nad rámec krátkodobých výpadků napadených webů.

Nově zaznamenaným trendem je nárůst počtu hacktivistických skupin, které útočí na slabě zabezpečené systémy operačních technologií a systémy SCADA průmyslových podniků v západních zemích. Jeden incident tohoto typu byl evidován i v ČR.

V roce 2024 nadále přetrvávala hrozba ransomwarových útoků, kterých NÚKIB evidoval nižší jednotky každý měsíc. Ke strmějšímu nárůstu těchto útoků došlo v posledním čtvrtletí, v měsíci říjnu jich NÚKIB evidoval 7, což je dosud nejvyšší evidovaný počet nahlášených incidentů tohoto typu za měsíc. Ransomware útoky činí necelých 11 % z celkového počtu evidovaných incidentů, nicméně jejich dopady ukazují, že se stále jedná o velmi závažnou hrozbu.

Specifickou kyberbezpečnostní událostí byl výpadek EDR softwaru společnosti CrowdStrike, který zapříčinil celosvětový výpadek různých služeb napříč sektory. V ČR NÚKIB evidoval 9 incidentů v této souvislosti, avšak s menším dopadem než v jiných státech.

3.3 Kontrola, dohled a metodická pomoc

3.3.1 Kybernetická bezpečnost

V roce 2024 bylo provedeno celkem 22 auditů a kontrol podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „ZKB“), 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 (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů. V rámci běžné kontroly nebo auditu je rámcově ověřováno cca 150 kontrolních bodů. Kontrola nebo audit od zahájení po ukončení běžně trvá 2 až 3 měsíce.

Nad rámec běžných kontrolních činností se NÚKIB, stejně jako v předchozích letech, věnoval také metodické podpoře především u povinných subjektů formou zodpovídání dotazů, vydávání podpůrných materiálů či provádění auditů u vybraných subjektů. NÚKIB také spolupracoval se zahraničními partnery a vyměňoval si s nimi zkušenosti a poznatky z kontroly a dohledu a z bezpečnostních opatření včetně způsobu jejich plnění.

Na základě usnesení vlády ze dne 20. 12. 2023 č. 991 a v souladu s memorandem o vzájemné spolupráci byl v roce proveden audit kybernetické bezpečnosti u vybraných společností, které se organizačně podílely na zajištění konání Mistrovství světa IIHF v ledním hokeji 2024.

S ohledem na nově chystanou legislativu a potenciální nárůst povinných subjektů dále NÚKIB provedl audit u 3 obcí dle návrhu vyhlášky o bezpečnostních opatřeních pro nižší režim, aby následně mohly být i dalším obcím snáze demonstrovány nároky na tento režim a aktuální plnění vybranými obcemi.

V roce 2024 NÚKIB prohluboval spolupráci s dalšími dozorovými orgány. S Českým telekomunikačním úřadem uzavřel memorandum o spolupráci a odborníci z této instituce byli přizváni k provádění kontroly. Se zástupci České národní banky proběhla jednání o spolupráci při řešení dopadů nové regulace jak na bankovní sektor, tak na kybernetickou bezpečnost.

Regulace cloud computingu

NÚKIB v procesu zápisu poskytovatelů a jejich služeb do katalogu cloud computingu, který vede Digitální a informační agentura, dává vstupy do obou fází tohoto procesu. Při zápisu poskytovatele do katalogu cloud computingu vydává NÚKIB závazné stanovisko, zda je poskytovatel způsobilý zajistit základní úroveň ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy. Zároveň informuje o tom, zda je poskytovatel způsobilý pro poskytnutí cloud computingu orgánu veřejné správy z hlediska veřejného pořádku, bezpečnosti a dodržování práv třetích osob. Ve druhé fázi procesu zápisu, tedy posouzení služeb cloud computingu, vydává NÚKIB závazné stanovisko o tom, zda nabízený cloud computing umožňuje dosažení alespoň základní úrovně ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy, respektive zda splňuje požadavky vyhlášky o některých požadavcích pro zápis do katalogu cloud computingu.

Nejvýznamnější identifikované nedostatky:

- Rozsah systému řízení bezpečnosti informací nepokrývá všechna relevantní aktiva.
- Proces analýzy rizik není prováděn dostatečně.
- Řízení dodavatelů v oblasti kybernetické bezpečnosti není úplné.
- Požadavek na řízení kontinuity činností je opomíjen nebo není prováděn adekvátně, organizace tedy zpravidla nejsou připraveny na dopad kybernetického bezpečnostního incidentu.
- Není využívána vícefaktorová autentizace a současně nejsou využívána dostatečně silná hesla.
- Není dostatečně zajištěna ochrana před škodlivým kódem a nedochází k dostatečné detekci kybernetických bezpečnostních událostí v interní síti.
- Výrobce využívá nepodporovaná, tedy zranitelná technická zařízení.
- Jsou používány kryptografické algoritmy, které již nejsou považovány za odolné.
- Nedochází k dostatečnému testování a ochraně záloh.

Portál NÚKIB

NÚKIB v roce 2024 spustil pilotní verzi veřejné části Portálu NÚKIB, který bude dle připravované právní úpravy sloužit jako hlavní komunikační kanál mezi NÚKIB a povinnými subjekty. Jedná se o platformu, jejímž prostřednictvím plní NÚKIB některé svěřené úkoly v oblasti kybernetické bezpečnosti. Organizace budou prostřednictvím platformy nejenom plnit zákonné požadavky, ale také spolupracovat, sdílet informace a posilovat tak bezpečnost kybernetického prostoru ČR. Součástí portálu je systém Národní MISP, který slouží k automatizovanému sdílení indikátorů kompromitace. Cílem pilotní verze je otestovat funkcionality a uživatelskou přívětivost celé platformy.

3.3.2 Bezpečnost informačních a komunikačních systémů

3.3.2.1 Certifikace informačních a komunikačních systémů

NÚKIB plnil úkoly Národního střediska pro bezpečnost informačních a komunikačních systémů. Z pozice národní certifikační autority v oblasti certifikace informačních systémů nakládajících s utajovanou informací rezortů státní správy a podnikatelů vykonával certifikační a metodickou činnost, včetně kontrol, ve spolupráci s Národním bezpečnostním úřadem.

V roce 2024 probíhalo řízení o certifikaci u 190 informačních systémů. K 53 žádostem o certifikaci informačního systému, jejichž zpracování bylo zahájeno v roce 2023, přibylo v roce 2024 dalších 156 žádostí, a to 33 ze státní správy nebo samosprávy a 123 od podnikatelů. Ve většině případů se jednalo o žádosti o opakovanou certifikaci již provozovaných informačních systémů. Ve 37 případech byla podána žádost o certifikaci nově budovaného informačního systému.

V roce 2024 NÚKIB vydal celkem 143 certifikátů informačních systémů pro žadatele ze státní správy nebo samosprávy, podnikatele, včetně akreditací informačních systémů cizí moci.

3.3.2.2 Certifikace kryptografických prostředků a pracovišť

V roce 2024 bylo certifikováno 13 kryptografických prostředků a 19 kryptografických pracovišť. Bylo vydáno 9 schválení zástavby kryptografického prostředku do mobilního/rozmístitelného systému a 6 schválení materiálu k zajištění funkce kryptografického prostředku.

3.3.2.3 Ochrana proti kompromitujícímu vyzařování a certifikace stínicích komor

TEMPEST měření elektronických zařízení

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 NÚKIB v roce 2024 provedl více než 50 měření různých typů zařízení, mezi nimi TEMPEST měření samostatných zařízení v kombinaci s kryptografickým prostředkem PCS1 a LANPCS Box či novými systémy VTC GearLab pro Armádu ČR. Převážná většina zařízení splňovala stanovené požadavky.

Další TEMPEST měření NÚKIB provedl v rámci certifikace nebo akreditace informačních systémů pro zpracování utajovaných informací stupně utajení Důvěrné nebo Tajné, buď pro orgány státu, např. Úřad vlády ČR, Ministerstvo zahraničních věcí (dále jen „MZV“), MO, MV, Ministerstvo průmyslu a obchodu (dále jen „MPO“), zpravodajské služby aj., nebo pro podnikatele.

Zónové měření, instalační záznamy, obranné prohlídky

V prostorech, ve kterých se nachází zařízení zpracovávající utajované informace, NÚKIB prováděl ohodnocování metodou zónového měření. Tento druh měření byl použit především u objektů NÚKIB, Generální inspekce bezpečnostních sborů a jednotlivých ministerstev. Další zónová měření byla prováděna pro státní správu i pro soukromé subjekty v rámci certifikace informačních systémů. NÚKIB rovněž provedl zónové hodnocení prostorů na základě podkladů dodaných akreditovanými pracovišti MO, Bezpečnostní informační služby (dále jen „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 10 lokalit. Dále byly posouzeny instalační záznamy z akreditovaných pracovišť (MO, BIS, VZ, MV).

V rámci výjezdního zasedání Vojenského výboru NATO a neformálního zasedání Severo-atlantické rady na úrovni ministrů zahraničních věcí provedl NÚKIB hodnocení instalace informačních systémů.

V průběhu roku NÚKIB provedl na základě žádostí orgánů státní správy nebo v rámci certifikace informačních systémů také technické kontroly v několika objektech jak v ČR, tak mimo ČR.

Přehled provedených měření

Typ měření	Počet
Zónové měření	17 lokalit
Kryptografické prostředky	2 typy
Komponenty ICT	50 systémů
Audiotechnika	4 typy zařízení
Obranné prohlídky i v rámci certifikace IS	12 objektů
Mobilní systémy	5 typů systémů
Stínicí komory	30 certifikátů

3.3.2.4 Národní distribuční středisko

Výroba kryptografického materiálu

V roce 2024 NÚKIB vygeneroval celkem 53 843 kryptografických klíčů a hesel uložených na 5 896 nosičích různých typů a dalších 64 ks jiného kryptografického materiálu (provozní dokumentace kryptografického prostředku, instalační a šifrovací SW). Kryptografický materiál je určen pro NÚKIB a orgány státu k zajištění ochrany utajovaných informací v komunikačních a informačních systémech.

NÚKIB v roce 2024 vzal do evidence a zajistil distribuci celkem 544 ks nového kryptografického a Controlled Cryptographic Item materiálu a dále zabezpečil servis a opravy na území ČR u 505 ks kryptografických prostředků a mimo ČR u 39 ks kryptografických prostředků.

NÚKIB vzal do evidence a zajistil distribuci celkem 97 ks kryptografického materiálu EU.

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

Školení pracovníků kryptografické ochrany a zkoušky odborné způsobilosti

NÚKIB v roce 2024 organizačně zajistil a provedl celkem 23 prezentací pro skupiny pracovníků kryptografické ochrany a po následující zkoušce odborné způsobilosti vydal 101 osvědčení o zvláštní odborné způsobilosti pracovníka kryptografické ochrany. Dále NÚKIB provedl zaškolení kurýra kryptografického materiálu a vydal 4 potvrzení o odborném zaškolení kurýra kryptografického materiálu. Školení, která jsou v neutajovaném režimu, proběhla on-line formou.

V roce 2024 byl aktualizován rozsah smlouvy k provádění odborné zkoušky a vydávání osvědčení o zvláštní odborné způsobilosti pracovníků kryptografické ochrany uzavřené mezi NÚKIB a MO. Dále byl aktualizován rozsah (z hlediska typů kryptografických prostředků) smlouvy k provádění odborné zkoušky a vydávání osvědčení o zvláštní odborné způsobilosti pracovníků kryptografické ochrany uzavřené mezi NÚKIB a MV.

3.3.2.5 Vývoj kryptografických prostředků

V roce 2024 probíhaly vývojové projekty aplikované kryptografie k implementaci prioritních úkolů Národní politiky kryptografické ochrany utajovaných informací a Výzkumného záměru výzkumu a vývoje na rok 2024, zejména se jednalo o vývojové projekty: LanPCS, LanPCS – středisko, Digitální GNZ, Autentizace v mobilních zařízeních, OSK II, LanPCS_D, Notebook_V, a dále interní výzkumně-vývojové projekty: vývoj návrhových, překladových, verifikačních a testovacích pracovišť; výzkum v oblasti kryptografických primitiv odolných proti útokům umělé inteligence a vývoj programů a metodik pro generování, verifikaci a testování strukturálních prvků pro kryptografická primitiva.

V roce 2024 probíhaly doplňkové vývojové práce na kryptografickém prostředku ECAr, který je určený pro ochranu utajované informace stupně utajení Vyhrazené.

3.3.3 Správní řízení

V roce 2024 NÚKIB pravomocně rozhodl o 3 přestupcích na úseku ZKB.

Rozkladová komise projednala v rámci řízení o rozkladech proti rozhodnutí o přestupcích 4 případy. V jednom případě byl rozklad jako opožděný zamítnut a obviněný pokutu uhradil. Jedno rozkladové řízení bylo po podání rozkladu přerušeno. V jednom případě nebylo ve věci do konce roku 2024 vydáno rozkladové rozhodnutí.

V návaznosti na nedostatky zjištěné při kontrolách v oblasti kybernetické bezpečnosti NÚKIB pravomocně uložil povinným osobám nebo orgánům v 15 případech jedno nebo více nápravných opatření k odstranění nedostatků.

V roce 2024 zahájil NÚKIB jedno přestupkové 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 „ZoOUI"), proti rozhodnutí byl podán rozklad.

3.4 Bezpečnost satelitních služeb

3.4.1 Veřejně regulovaná služba Evropského programu družicové navigace Galileo (PRS)

V první polovině roku 2024 byla plně zprovozněna první část utajovaného spojení s bezpečnostním a monitorovacím centrem GSMC GRON. Pro tuto technologii byla zprovozněna jak neutajovaná, tak utajovaná část. Následně byla provedena zástavba navazující technologie POCP (zatím pouze neutajovaná část, utajovaná část bude dostupná během dvou let, před plně operační fází služby PRS). NÚKIB se zapojil do konsorcia několika dalších členských států, které disponují technologií GRON/POCP, a bude v rámci projektu testovat připravenost služby a celého systému na PRS počáteční operační schopnosti. V rámci výborů a pracovních skupin Evropské komise proběhl posun v přípravě a přijetí zásadních programových dokumentů nezbytných pro dosažení počátečních operačních schopností PRS.

Zástupci NÚKIB jsou také součástí Komise pro bezpečnostní akreditaci (SAB) a Bezpečnostního akreditačního panelu (SAP), jejichž jednání probíhají v EUSPA a v nichž se řeší bezpečnost a akreditace komponent evropského vesmírného programu. Dále byla řešena příprava na vynášení satelitů na orbitu v roce 2025 a 2026.

NÚKIB se také věnoval bezpečnostní akreditaci prvků pozemní infrastruktury a posílení kybernetické bezpečnosti v rámci kosmického programu.

3.4.2 GOVSATCOM a Program pro bezpečnou konektivitu (USC)

V roce 2024 byla příslušným orgánům Govsatcom (CGA) představena platforma G-HUB (Govsatcom HUB), informační systém a nástroj, který bude používán CGA a uživateli satelitní komunikace poskytované v rámci Govsatcom, ve kterém si budou moci služby vyhledat a vyžádat. V systému bude možné získat také „terminál“ zařízení pro satelitní komunikaci pro danou službu. NÚKIB byl jako CGA přizván k validaci tohoto řešení. Govsatcom přejde v roce 2025 do tzv. iniciační fáze a už v tomto roce bude nabízet služby uživatelům.

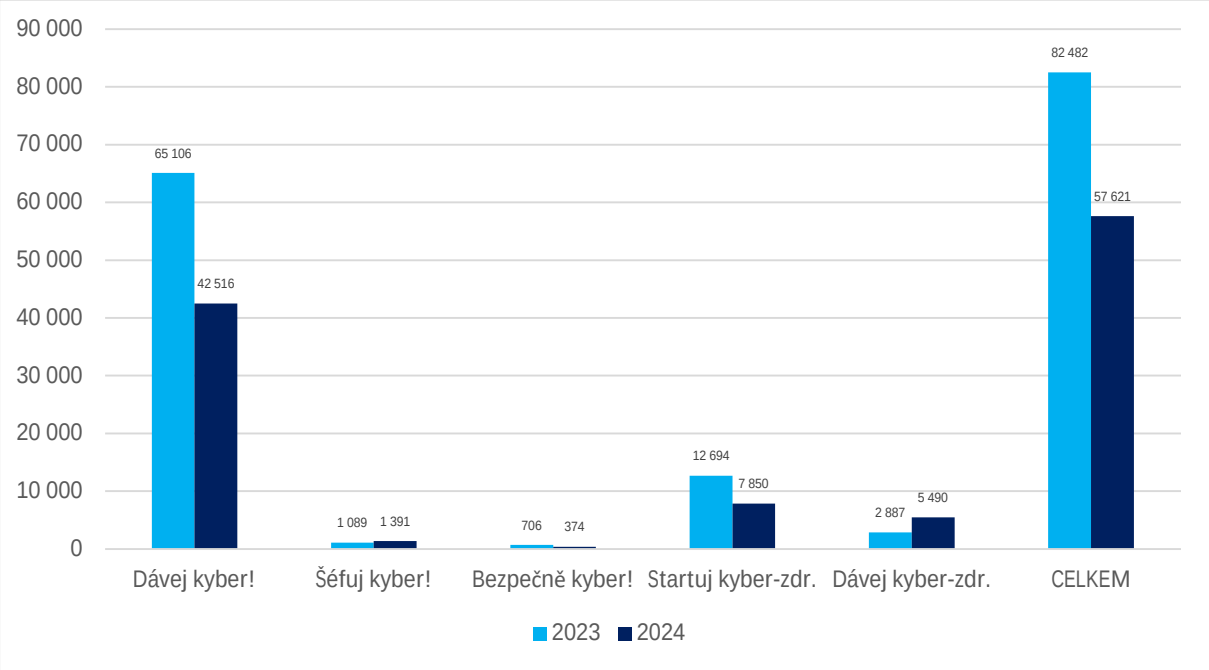
V roce 2024 začala příprava samostatného zákona o PRS/Govsatcom. Proběhly schůzky na politické úrovni s potenciálními uživateli služby PRS a Govsatcom. Byla také zahájena příprava studie využitelnosti PRS a Govsatcom v ČR, která bude realizována v roce 2025 a 2026 a měla by být základním vstupem pro tvorbu legislativy PRS a Govsatcom.

3.5 Vzdělávání a osvěta

Vzdělávání

E-learningové vzdělávací kurzy jsou i nadále hlavním nástrojem vzdělávání veřejnosti v oblasti kybernetické bezpečnosti. V roce 2024 došlo meziročně k poklesu počtu uživatelů e-learningových kurzů vytvořených NÚKIB, které účastníci využívali na portálu osveta.nukib.gov.cz.

Přehled počtu absolvovaných on-line kurzů



Kurzy NÚKIB pravidelně absolvují zaměstnanci veřejných institucí, neziskových organizací, soukromých společností, ale i jednotliví občané, kteří o kurzy projeví zájem. Kurzy jsou dostupné veřejně a zdarma a kdokoliv, kdo má připojení k internetu a ovládá český jazyk, je může prohlížet a absolvovat. To je pozitivní zejména v kontextu veřejné správy, jejíž organizace mohou zvyšovat povědomí svých zaměstnanců bez alokace veřejných výdajů.

V roce 2024 byl obsah jednoho z kurzů rovněž namluven pomocí umělé inteligence a lze jej procházet poslechem. Všechny kurzy a ostatní on-line aktivity NÚKIB se průběžně podle potřeby vylepšovaly a aktualizovaly.

NÚKIB nadále zajišťoval i prezenční vzdělávání u svých cílových skupin. Spolupracoval na výuce kybernetické bezpečnosti v různých oblastech na vybraných vysokých a středních školách zaměřených na výuku kybernetické a informační bezpečnosti. Zaměstnanci NÚKIB se také podíleli na vedení a konzultacích závěrečných prací studentů vysokých škol.

NÚKIB je orgánem příslušným k rozhodování o udělení, prodloužení platnosti nebo odnětí autorizace pro povolání a pracovní činnosti, jejichž výkonu se příslušná profesní kvalifikace týká, v oblasti kybernetické bezpečnosti. V roce 2024 se NÚKIB podílel na tvorbě standardů profesních kvalifikací. V souvislostí s tím revidoval a připravil návrhy šesti profesních profilů (manažer/manažerka, architekt/architektka, analytik/analytička, auditor/auditorka, technik/technička kybernetické bezpečnosti a pracovník/pracovnice dohledového centra).

V roce 2024 byl připraven Národní plán vzdělávání v kybernetické bezpečnosti a předložen ke schválení BRS. Vypracování plánu bylo NÚKIB uloženo v Akčním plánu Národní strategie kybernetické bezpečnosti 2021–2025 a hlavní cíle, které v oblasti vzdělávání (nikoliv osvěty a prevence) identifikuje, jsou: získání přesného situačního přehledu o nedostatku odborníků kybernetické bezpečnosti a o požadavcích trhu; zvýšení počtu odborníků kybernetické bezpečnosti, zejména pro orgány veřejné moci a subjekty regulované ZKB; zajištění centrálního vzdělávání zaměstnanců orgánů veřejné moci a subjektů regulovaných ZKB; zajištění kvalitního vzdělávání poskytovaného veřejnosti a vysoké úrovně povědomí společnosti o systému kybernetické bezpečnosti ČR, o kybernetických hrozbách a o způsobech jejich předcházení.

Osvěta

Zástupci NÚKIB se pravidelně účastnili činnosti v Republikovém výboru pro prevenci kybernetické kriminality, řízeném MV, zorganizovali národní Festival bezpečného internetu a pravidelně se účastnili jednání evropského pracovního týmu pro evropský měsíc kybernetické bezpečnosti (říjen), ve spolupráci s MV a jinými organizacemi se zúčastnili Dne bezpečnějšího internetu.

Na sociálních médiích již tradičně proběhlo několik minikampaní – ženy v ICT, den hesla, výzva pro den dětí.

NÚKIB se zapojil do aktivit partnerů, jako jsou Národní finále soutěže v kybernetické bezpečnosti, Kybercena roku či Týden pro Digitální Česko, a na osvětovém portálu sdílí osvětové materiály vytvořené partnery.

NÚKIB také rozvíjel aktivity pro budoucí studenty kybernetické bezpečnosti a už podruhé se zapojil do veletrhu Gaudeamus 2024 Brno.

Transformací webu NIS2 vzniklo celé informační rozhraní k nZKB s přihlédnutím k personalizaci obsahu pro konkrétní účel, za jakým daná osoba informace hledá. Toto rozhraní mimo jiné obsahuje 10 praktických informačních listů vysvětlujících hlavní témata nZKB nebo nový podpůrný materiál pro obce s rozšířenou působností.

3.6 Cvičení

Cvičení kybernetické bezpečnosti

Locked Shields 2024

Toto hybridní cvičení je pořádáno NATO CCD COE a na jeho přípravě se podílejí přední firmy z technologického průmyslu, zástupci akademického sektoru a řady státních institucí. Cílem je prohloubit spolupráci mezi všemi zúčastněnými subjekty. NÚKIB tvořil společný tým s partnerskými organizacemi a kolegy z Ukrajiny. Do cvičení, jehož součástí je ochrana počítačových systémů před útoky v reálném čase a simulace taktických a strategických rozhodnutí v kritických situacích, se letos zapojilo přibližně 4 000 účastníků ze 40 zemí světa. V konkurenci 18 týmů se česko-ukrajinský tým umístil v první třetině.

NATO Cyber Coalition

Jedná se o cvičení kybernetické bezpečnosti, na kterém zaměstnanci NÚKIB participovali jak při přípravě, tak v roli cvičících. Na úrovni ČR koordinuje cvičení NÚKIB za civilní část a Velitelství informačních a kybernetických sil za vojenskou. Cílem cvičení je budovat silné společenství a vzájemnou spolupráci.

Cvičení pro Albánii – EU Support to Western Balkans Cybersecurity Capacity Building

NÚKIB připravil ve spolupráci s kolegy z albánského Národního úřadu pro elektronickou certifikaci a kybernetickou bezpečnost (AKCESK) scénář pro účastníky z různých vládních institucí a zástupce bank, který se zaměřil na eskalující krizi v kybernetickém prostředí bankovního sektoru a zdůraznil multidimenzionální charakter kybernetických hrozeb. Jedním z cílů simulace byla diskuse nad novou albánskou legislativou v oblasti kybernetické bezpečnosti a zaměření se na vzájemnou spolupráci a krizovou komunikaci mezi zúčastněnými institucemi.

Cyber Europe 2024

NÚKIB se účastnil také jednoho z největších kybernetických cvičení v Evropě, které pořádá Evropská agentura pro kybernetickou bezpečnost (dále jen „ENISA“) každé dva roky a jehož cílem je posílit stávající technické a operační schopnosti cvičících. V roce 2024 se detailně propracovaný scénář zaměřil primárně na energetický sektor a sekundárně na datacentra, kdy simulované kybernetické bezpečnostní incidenty postupně během 2 dnů eskalovaly do kybernetické krize, kterou bylo nezbytné koordinovat na národní i evropské úrovni.

EU Integrated Resolve 2024

Jedná se o cvičení vedené Radou EU, Evropskou komisí a Evropskou službou pro vnější činnost, jehož cílem bylo otestovat připravenost a schopnost EU zvládat složité krize hybridního charakteru. Cvičení proběhlo ve dvou fázích: První fáze se zaměřila na plánování vojenské operace společné bezpečnostní a obranné politiky a koordinaci během konzulární krize. Druhá sestávala z řady simulovaných víceúrovňových scénářů hybridní povahy, včetně evakuace občanů EU z oblasti konfliktu.

Projekt INJECT

Cílem projektu INJECT je vytvoření open source platformy pro přípravu, exekuci a evaluaci netechnických table-top cvičení kybernetické bezpečnosti. Řešitelem je Fakulta informatiky Masarykovy univerzity v Brně (dále jen „MU“). NÚKIB připravil pro zástupce vybraných institucí soukromé a veřejné sféry cvičení k otestování aktuálního vývoje platformy.

Ostatní cvičení

NÚKIB se během roku 2024 zabýval přípravou kurzu Train-the-trainer a připravil rovněž cvičení pro studenty předmětu kybernetická bezpečnost, který je vyučován v rámci magisterského navazujícího programu Bezpečnostní a strategická studia na Fakultě sociálních studií MU.

V rámci workshopového dne každoročně pořádané konference CyberCon byla realizována ukázka table-top cvičení, kde si účastníci mohli vyzkoušet rozhodování v krizové situaci fiktivní společnosti čelící kybernetickému útoku.

V roce 2024 se cvičení, která pořádal NÚKIB, či se na přípravě podílel, účastnilo celkem **305** cvičících.

V roce 2024 NÚKIB pořádal či se podílel na přípravě celkem **9** cvičení.

3.7 Vědecká činnost, výzkum, vývoj a inovace

V rámci vědecké činnosti NÚKIB připravil přihlášky do programů SecPRO a BETA3. Dále rozvíjel spolupráce s akademickou sférou (Vysoká škola báňská – Technická univerzita Ostrava, Univerzita obrany, Vysoké učení technické v Brně, MU, České vysoké učení technické v Praze) i společnostmi bezpečnostního výzkumu a vývoje (S.ICZ, a. s.). V rámci výzkumu a vývoje v oblasti bezpečnosti informačních a komunikačních technologií byly v roce 2024 zahájeny 2 nové projekty vývoje kryptografických prostředků. Úspěšné oponentní jednání ukončilo řešení 2 projektů zahájených v předchozích letech. Současně probíhalo několik interních výzkumně-vývojových projektů na odborném pracovišti. Jednalo se o projekty zabývající se vývojem kryptografických prostředků a ochranou utajovaných informací.

V roce 2024 pokračovala realizace 2 projektů spolufinancovaných z evropského rámcového programu Digitální Evropa. První projekt je zaměřen na podporu vzniku a činnosti Národního koordinačního centra v souvislosti s nařízením Evropského parlamentu a Rady 2021/887, kterým se zřizuje Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center. NÚKIB podpořil v rámci první dotační výzvy 7 projektů pokrývajících rozvoj odborných kapacit, vzdělávání či vývoj v technických oblastech kybernetické bezpečnosti. Druhý projekt je zaměřen na podporu implementace evropského rámce certifikací kybernetické bezpečnosti. Na těchto projektech NÚKIB úzce spolupracuje s konsorciálním partnerem CyberSecurityHubCZ.

NÚKIB byl rovněž aktivní ve Správní radě Evropského průmyslového, technologického a výzkumného centra kompetencí, mezi jehož úkoly patří soustředit investice do výzkumu, technologií a průmyslového vývoje a řídit finanční podporu z programu Digitální Evropa.

NÚKIB také zorganizoval dvě expertní jednání Skupiny kyberbezpečnostního výzkumu a inovací CYRIS. Cílem skupiny je podporovat spolupráci mezi akademickým, veřejným a soukromým sektorem v obasti vývoje a inovací či informovat účastníky o možnostech získání veřejné podpory pro výzkumné projekty.

V rámci výzkumu a vývoje v oblasti bezpečnosti informačních a komunikačních technologií bylo v roce 2024 zahájeno 6 nových, dodavatelsky řešených projektů. Projekty jsou zaměřeny na problematiku TEMPEST, vývoj kryptografických prostředků a kryptologickou analýzu. Současně se zajistilo několik oprav měřicí techniky.

Úspěšné oponentní jednání ukončilo řešení 6 projektů zahájených v předchozích 3 letech. Jednalo se o projekty zabývající se ochranou utajovaných informací.

3.8 Legislativa a vládní agenda

V souladu s Plánem legislativních prací vlády na rok 2024 pracoval NÚKIB na návrhu zákona o kybernetické bezpečnosti, který je transpozičním předpisem směrnice NIS2 do českého právního řádu a který obsahuje právní úpravu mechanismu bezpečnosti dodavatelského řetězce. Za účelem splnění obou těchto požadavků byl ve výsledku připraven jeden návrh zákona řešící obě tyto problematiky – návrh nZKB. Spolu s návrhem zákona byly rovněž připravovány i prováděcí právní předpisy, které byly ve formě pokročile zpracovaných tezí součástí návrhu zákona. Spolu s návrhem nZKB připravil NÚKIB také návrh zákona, kterým se mění některé zákony v souvislosti s přijetím nZKB.

Zástupci NÚKIB obhájili tyto návrhy zákonů před pracovními komisemi LRV a současně také na plénu LRV, kde předseda LRV k návrhům zákonů vydal pozitivní stanovisko. Následně byly návrhy předloženy ke schválení vládě.

Vláda návrhy zákonů schválila a předseda vlády je ve formě vládních návrhů zákonů předložil Poslanecké sněmovně ČR.

Na podzim 2024 proběhlo k návrhům zákonů první čtení v Poslanecké sněmovně ČR a následně byly návrhy zákonů projednávány ve výborech (Výbor pro bezpečnost, Výbor pro obranu, Hospodářský výbor) Poslanecké sněmovny ČR, kde na základě pověření vlády obhajoval tyto návrhy ředitel NÚKIB. Legislativní proces bude dále pokračovat v roce 2025.

Spolu s probíhajícím legislativním procesem návrhu zákona se NÚKIB intenzivně připravoval na účinnost nového zákona nastavováním interních procesů.

Vzhledem ke změnám, které nastanou s účinností návrhu zákona o kybernetické bezpečnosti, je třeba změnit ustanovení účinných právních předpisů v ČR, jež obsahově navazují na tento návrh zákona, a zajistit tím zejména jejich řádnou interpretaci a aplikaci. To bude zajištěno vydáním celkem 9 prováděcích právních předpisů.

Přestože jejich podrobné teze zveřejnil NÚKIB již v roce 2023, v průběhu roku 2024 i nadále vedl další jednání, konzultace a prováděl vlastní analýzy, aby obsah prováděcích právních předpisů zpřesnil a co nejlépe je připravil na jejich vlastní legislativní proces.

Dále v roce 2024 probíhal legislativní proces u prováděcích právních předpisů k ZoOUI. Vzhledem ke změnám, které přinese novela tohoto zákona (účinná od 1. 1. 2025), bude nezbytné již účinné prováděcí právní předpisy podrobit revizi. Koncem roku 2024 byl legislativní proces u 4 prováděcích právních předpisů dokončen a byly zvěřejněny ve Sbírce zákonů ČR s účinností od 1. 1. 2025.

Vedle legislativních prací na výše uvedených právních předpisech NÚKIB v roce 2024 posoudil v mezirezortním připomínkovém řízení 213 materiálů legislativní i nelegislativní povahy, přičemž k řadě z nich uplatnil z hlediska své působnosti připomínky.

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.

NÚKIB se intenzivně zapojoval také do přípravy nového krizového zákona, jehož gestorem je MV, resp. Generální ředitelství Hasičského záchranného sboru. NÚKIB je však jedním z gestorů v této oblasti a již na úrovni směrnic má tento předpis předpokládanou vysokou míru propojenosti se ZKB, i proto byla vyšší míra spolupráce nezbytná.

Mezi další významné legislativní činnosti patří zapojení do otázek spojených s aplikací evropských předpisů – tzv. Aktu o datech a tzv. Network code, které NÚKIB řešil především s MPO.

Významnou unijní legislativou, která ve velkém ovlivní kybernetickou bezpečnost v ČR, je tzv. Akt o kybernetické odolnosti. NÚKIB řešil v roce 2024 velmi intenzivně i otázky spojené s praktickou implementací tohoto unijního nařízení.

3.9 Komunikace

Tradičním kanálem pro zveřejňování informací souvisejících s agendami NÚKIB byly nadále webové stránky úřadu, četná veřejná vystoupení a také média a četné dotazy, které jim byly zodpovězeny. Hlavní zájem v roce 2024 budil legislativní proces návrhu nZKB, jehož částí je mechanismus prověřování bezpečnosti dodavatelského řetězce. Jednotlivé fáze tohoto procesu, stejně jako investigativní práce některých bezpečnostně orientovaných reportérů opakovaně probouzely aktivitu novinářů. Této synergie úřad využil ke kontinuální komunikaci klíčových témat z oblasti kybernetické bezpečnosti. Bezprecedentní – samozřejmě nejen komunikační událostí – byl masivní globální výpadek IT služeb způsobený nezdařenou aktualizací softwaru společnosti CrowdStrike. Důležitou součástí komunikace NÚKIB byla také veřejná vystoupení jak členů vedení, tak i zaměstnanců expertů na konferencích, odborných diskuzích, veletrzích a akcích, které nabízejí příležitost k cílenému sdílení informací.

Společně s Policií ČR a Českou bankovní asociací NÚKIB vytvořil osvětovou kampaň nazvanou Velké odhalení, která veřejnost upozorňuje na vishing, podvodné telefonáty. Pro názorné ukázky různých praktik vishingu byly natočeny videoklipy se známými českými herci, které mají občanům ČR pomoci tyto podvodníky rozpoznat.

Komunikaci NÚKIB doplňovaly účty na sociálních sítích, jejichž modernější vizuální podoba pomáhá v získávání nových sledujících i reagujících uživatelů.

3.10 Spolupráce, mezinárodní spolupráce

V průběhu roku 2024 pokračovalo prohlubování vztahů se soukromými subjekty, které se zabývají kybernetickou a informační bezpečností, a dále též se společnostmi, jež se věnují aktivitám spojeným s vesmírnými technologiemi. Spolupráce probíhala jak s českými, tak i nadnárodními firmami působícími v ČR, případně jednotlivými svazy. Prostřednictvím českých kyberatašé poté docházelo i ke kontaktu se soukromými subjekty působícími v zahraničí (primárně USA a Izrael).

Kromě konzultací a osvěty v rámci NIS2 vycházela spolupráce z potřeby prohloubení či sdílení znalostí v oblasti nových trendů a nastupujících technologií. V průběhu roku NÚKIB zorganizoval několik workshopů se zástupci soukromého sektoru.

V roce 2024 měl NÚKIB sedm zaměstnanců v zahraničí, tzv. kyberatašé a národní experty, a to ve Washingtonu, Tel Avivu, Canberře, Tallinnu (NATO CCDCOE) a Bruselu (při EU, NATO a v ENISA), což umožnilo efektivně budovat nadstandardní spolupráci s klíčovými partnery úřadu.

V roce 2024 NÚKIB uspořádal již tradiční mezinárodní konferenci Prague Cyber Security Conference s globálním dosahem zaměřenou na prosazování klíčových témat kybernetické bezpečnosti. Mezi stěžejní témata patřily dopady umělé inteligence na kybernetickou bezpečnost, ochrana podmořských kabelů před kybernetickými hrozbami a cizím narušením, kybernetické válčení, boj s organizovanými kyberkriminálními skupinami nebo bezpečnost cloudu. Konference byla nejen skvělou příležitostí pro bilaterální jednání se zahraničními delegacemi, ale také pro rozvoj spolupráce se zástupci soukromého sektoru.

Evropská unie

NÚKIB byl činný v řadě skupin pod hlavičkou Evropské unie (HWPCI, NIS CG, CyCLONe, CSIRTs Network). Aktivně se zapojil do přípravy několika unijních legislativních aktů, zejména aktu o kybernetické odolnosti, aktu o kybernetické solidaritě a revize aktu o kybernetické bezpečnosti.

Na konci roku 2024 bylo v úředním věstníku EU zveřejněno nařízení o kybernetické odolnosti Cyber Resilience Act, do jehož vyjednávání se NÚKIB aktivně zapojoval. Cyber Resilience Act představuje průlomovou unijní legislativu na poli kybernetické bezpečnosti, jejímž cílem je zvýšit bezpečnost zavedením požadavků na kybernetickou bezpečnost softwarových a hardwarových produktů, jež bude nutné naplňovat po celou dobu jejich životního cyklu. Cílem nařízení dále je snížit počet zranitelností v produktech a zlepšit informovanost jejich uživatelů.

NÚKIB se významnou měrou podílel na přípravě deklarace Prohlášení k aplikaci mezinárodního práva v kyberprostoru, která potvrzuje, že se mezinárodní právo vztahuje na chování států v kyberprostoru a je nezbytné pro udržení míru a stability v prostředí ICT. Evropská deklarace je v souladu s národní pozicí k aplikaci mezinárodního práva v kyberprostoru a ČR ji publikovala v únoru 2024 pod vedením MZV.

NÚKIB pokračoval v zapojení do aktivit ENISA prostřednictvím účasti ve správní radě, poskytnutím kontaktního místa a vysláním svého zaměstnance na pozici sekondovaného národního experta v srpnu 2024. Dále pokračovaly aktivity v rámci projektu podpůrných služeb (ENISA Support Action), díky čemuž byly vybraným subjektům poskytnuty bezplatné služby penetračního testování, kybernetických cvičení nebo pomoci při analýze rizik.

V rámci Skupiny pro spolupráci zřízené směrnicí NIS2 pokračovala práce na souboru opatření pro bezpečnost dodavatelského řetězce informačních a komunikačních technologií (tzv. Supply Chain Toolbox).

NÚKIB vyjádřil podporu dokumentu Position Paper on Quantum Key Distribution, který vydaly čtyři evropské bezpečnostní autority. Dokument popisuje aktuální možnosti této technologie a posuzuje její aktuální bezpečnostní přínos.

NÚKIB se také připojil k dokumentu Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography, který urguje potřebu realizovat přípravné kroky pro nasazení postkvantové kryptografie, s cílem zajistit dostatečnou míru ochrany proti kvantové hrozbě.

Severoatlantická aliance

I v roce 2024 ČR vyhodnocovala své závazky k NATO směřující k navyšování schopností a kapacit v oblasti kybernetické bezpečnosti a obrany. Stalo se tak prostřednictvím aktualizovaného NATO Cyber Defence Pledge, na němž se spojenci shodli na summitu ve Vilniusu v roce 2023.

Ředitel NÚKIB podepsal jménem ČR v říjnu 2024 memorandum o porozumění s NATO v oblasti kybernetické bezpečnosti a obrany.

NÚKIB je zapojen do činnosti NATO CIS3 partnerství, které se zabývá standardizací hlasové a datové komunikace s cílem zajištění její interoparability v rámci NATO.

Spolupráce v rámci NATO probíhala i prostřednictvím české účasti v NATO Cooperative Cyber Defence Centre of Excellence v Tallinnu.

Organizace spojených národů (OSN)

NÚKIB se podílel na tvorbě pozic a priorit ČR pro jednání v OSN. Probíhaly pravidelné koordinace s MZV při tvorbě projevů v platformě věnované kybernetické bezpečnosti, tzv. Open-Ended Working Group, a NÚKIB také s Ministerstvem spravedlnosti sdílel priority k diskuzím k Úmluvě OSN proti kyberkriminalitě.

V roce 2024 ČR publikovala svou národní pozici k aplikaci veřejného práva v kyberprostoru.

Organizace pro bezpečnost a spolupráci v Evropě (OBSE)

NÚKIB se společně s MZV účastnil pravidelných jednání příslušné pracovní skupiny OBSE, kde nadále pokračoval ve sdílení přístupu ČR k politice CVD a dalších opatření pro budování důvěry v oblasti kyberbezpečnosti (CBMs). Díky aktivnímu sdílení svých zkušeností přispívá NÚKIB ke stabilní spolupráci v této oblasti.

Organizace pro hospodářskou spolupráci a rozvoj

NÚKIB sledoval aktivity expertních podskupin organizace Working Group on Security in the Digital Economy, jejichž analytické výstupy mohou posloužit jako vodítka při zavádění nebo při revizi národních politik, strategií a legislativy v oblasti digitální bezpečnosti, a aktivně se podílel na návrzích a revizích příslušných dokumentů i ve spolupráci s dalšími gestory.

Bilaterální spolupráce

V souladu s národní strategií kybernetické bezpečnosti posiloval NÚKIB stávající partnerství zejména v regionech a zemích s přítomností českých kyberatašé. Současně však pokračoval ve vytváření nových strategických vazeb v různých částech světa a ve spolupráci s partnery sdílel české know-how a zkušenosti v rámci budování kybernetických kapacit.

V říjnu 2024 došlo k podpisu memoranda o porozumění s litevským národním centrem kybernetické bezpečnosti. NÚKIB se tím zapojil do Regional Cyber Defence Centre, které sdružuje Litvu, Polsko, USA, Ukrajinu a Gruzii a zajišťuje spolupráci a výměnu informací v oblasti Cyber Threat Intelligence (CTI).

Austrálie a Indo-Pacifik

Díky zřízení pozice kyberatašé pro Indo-Pacifik se sídlem v australské Canberře došlo k významnému posílení bilaterálních vztahů s Austrálií. Významným prvkem spolupráce byla podpora ze strany Austrálie při atribuci aktivit skupiny APT 28, což posílilo vzájemnou důvěru a schopnost čelit kybernetickým hrozbám na globální úrovni.

Na regionální úrovni se podařilo navázat užší spolupráci s klíčovými partnery v Japonsku, Korejské republice, Singapuru, na Novém Zélandu a Tchaj-wanu. Významnou událostí byla účast technického týmu NÚKIB na mezinárodním kybernetickém cvičení APEX (Allied Power Exercise). Tato návštěva vytvořila prostor nejen pro prohloubení partnerství, ale také pro aktivní prezentaci českého pokroku v oblasti kybernetické bezpečnosti. Diskutována byla mimo jiné legislativní opatření, strategické výhledy, analýza aktuálního prostředí a ochrana kritické informační infrastruktury. Tento komplexní přístup posílil českou pozici v regionu a přispěl k upevnění partnerství založených na sdílených hodnotách a společných cílech.

USA a Kanada

V březnu 2024 proběhl v Praze první ročník tzv. United States – Czech Republic Cyber Dialogue, doposud největší mezivládní konzultace mezi ČR a USA v otázkách kybernetické bezpečnosti, jehož se účastnily klíčové instituce, mezi něž NÚKIB patří. Hlavním tématem jednání bylo prohlubování spolupráce nejen v kybernetické bezpečnosti, ale i v boji proti kybernetickému zločinu, budování kybernetické obrany, koordinaci v kybernetické diplomacii nebo spolupráce v digitálních politikách a přelomových technologiích, včetně umělé inteligence nebo kvantových technologií.

NÚKIB v roce 2024 rovněž pokračoval v zapojení do Counter Ransomware Initiative, v jejímž rámci bylo letos mimo jiné přijato společné prohlášení vyzývající k odpovědnému chování států v kyberprostoru a využívání všech dostupných nástrojů a prostředků v boji proti ransomwaru. ČR na summitu prezentovala dosavadní spolupráci v rámci mezirezortní pracovní skupiny pro boj s ransomwarem, kterou NÚKIB spolu s Národní centrálou proti terorismu, extremismu a kybernetické kriminalitě Policie ČR založil v lednu 2024. Díky varování amerických partnerů a včasnému sdílení informací mezi CERT byl NÚKIB schopen před ransomwarovým útokem ochránit jeden ze subjektů v ČR.

V roce 2024 NÚKIB posílil spolupráci s Kanadou. Vedení NÚKIB zde jednalo s federálními úřady, soukromým sektorem i akademickou sférou o rozvoji spolupráce v oblasti posílení sdílení informací a společných projektech v oblasti vědy a výzkumu.

Izrael

Spolupráce s INCD byla prohloubena po podpisu nového memoranda o porozumění během návštěvy prezidenta ČR v Izraeli. Probíhající konflikt s Hamásem, Hizballáhem a Íránem vedl k zintenzivnění spolupráce v oblasti sdílení operačních a analytických informací. Dále pokračoval strukturovaný dialog ve všech oblastech kybernetické bezpečnosti, zejména pak v oblasti regulace, kde NÚKIB sdílí s INCD svoje zkušenosti z přípravy nZKB.

Pokračovalo také prohlubování spolupráce s dalšími úřady, které mají v gesci kybernetickou bezpečnost, zejména v oblasti sdílení dobré praxe. Zástupce NÚKIB aktivně vystoupil na prestižní konferenci Cyber Week v Izraeli.

Rozvojová spolupráce a budování kybernetických kapacit

NÚKIB zintenzivnil zapojení do budování kybernetických kapacit v regionu západního Balkánu, Latinské Ameriky a Indo-Pacifiku. Na aktivitách spolupracuje s mezinárodními organizacemi (zejména NATO a EU) a klíčovými státy s obdobnými postoji, včetně USA a Estonska. Ve spolupráci s lotyšským CERT vedli zástupci NÚKIB workshopy zaměřené na reakci na kybernetické incidenty v Tiraně a Bělehradu pro zástupce šesti zemí západního Balkánu. V rámci EU projektu Latin America and Caribbean Cyber Competence Centre (LAC4) NÚKIB v roce 2024 participoval na několika aktivitách zaměřených na budování kapacit kybernetické bezpečnosti v regionu Latinské Ameriky.

NÚKIB se také aktivně podílel na rozvojových projektech CyberVac Ministerstva zahraničních věcí. Za účasti zástupců NÚKIB se konaly semináře ke kyberkriminalitě a kybernetické bezpečnosti v Kolumbii, Argentině a Indonésii. NÚKIB také spolupracoval na organizaci

workshopu zaměřeného na právní a strategické aspekty kybernetické bezpečnosti v geopoliticky exponovaném Bhútánu.

3.11 Ekonomické zabezpečení

3.11.1 Příjmy

Celkové příjmy kapitoly za rok 2024 byly ve výši 79 831 396,52 Kč. Příjmy tvořily nedaňové příjmy a přijaté transfery. Část nedaňových příjmů ve výši 305 499,88 Kč byla za příjem pokut ze správního řízení dle ZoOUI. Další položkou byly neplánované přijaté nekapitálové příspěvky a náhrady v objemu 308 723,70 Kč. Jednalo se o refundace cestovních náhrad, o úhrady pohledávek za zaměstnance NÚKIB, o dobropisy za zboží a služby z předchozího rozpočtového roku a také náklady řízení k uděleným pokutám. Přijaté transfery pak tvoří prostředky přijaté od Evropské unie v objemu 79 023 746,68 Kč.

Přehled plnění rozpočtu příjmů v roce 2024 (vyjádření v tis. Kč)

	Schválený rozpočet	Rozpočet po změnách	Skutečnost
Příjmy celkem	475,00	122 050,00	79 831,40
Podseskupení			
136 – Příjem ze správních a soudních poplatků	75,00	75,00	0,00
211 – Příjem z vlastní činnosti	0,00	0,00	53,27
214 – Přijaté výnosy z finančního majetku	0,00	0,00	–0,36
221 – Přijaté sankční platby	400,00	400,00	305,50
232 – Ostatní nedaňové příjmy	0,00	0,00	308,72
311 – Příjem z prodeje dlouhodobého majetku	0,00	0,00	0,00
413 – Neinvestiční převody z vlastních fondů a ve vztahu k útvarům bez právní osobnosti	0,00	0,00	140,52
415 – Neinvestiční přijaté transfery ze zahraničí	0,00	0,00	0,00
421 – Investiční přijaté transfery od rozpočtů ústřední úrovně	0,00	121 575,00	79 023,75

3.11.2 Výdaje

Schválený rozpočet celkových výdajů NÚKIB byl v roce 2024 ve výši 610 947 413,00 Kč.

Během roku 2024 byl schválený rozpočet upravován rozpočtovými opatřeními MF na objem 750 730 129,00 Kč.

Konečný rozpočet celkových výdajů kapitoly za rok 2024, tedy rozpočet včetně zapojených nároků z nespotřebovaných výdajů (dále jen „NNV“) ve výši 72 756 466,32 Kč a zapojených prostředků rezervního fondu ve výši 130 000,00 Kč byl v objemu 820 999 110,32 Kč. Čerpání konečného rozpočtu bylo v relativním vyjádření na 84,6 %, v absolutním vyjádření ve výši 694 565 124,94 Kč.

Konečný rozpočet výdajů kapitoly bez prostředků EU/FM za rok 2024 byl v objemu 677 698 908,60 Kč. Čerpání konečného rozpočtu bylo v relativním vyjádření na 89,97 %, v absolutním vyjádření ve výši 609 730 221,52 Kč.

Základní přehled plnění rozpočtu výdajů v roce 2024 (vyjádření v tis. Kč)

	Schválený rozpočet	Rozpočet po změnách	Konečný rozpočet	Skutečnost
Výdaje celkem	610 947,41	750 730,13	820 999,11	694 565,12
Běžné výdaje	520 207,17	519 914,89	551 402,06	528 402,67
z toho platy včetně příslušenství	322 794,78	323 091,05	325 420,78	321 703,38
z toho běžné výdaje bez platů a příslušenství	197 412,39	196 823,85	225 660,28	206 699,29
Kapitálové výdaje	90 740,24	230 815,24	269 918,05	166 162,46

Výdaje na platy včetně příslušenství

Výdaje na platy, ostatní platby za provedenou práci a příslušenství byly rozpočtovány ve výši 322 794 782,00 Kč pro 373 pracovních míst.

Vázáním prostředků na platy a příslušenství za neobsazená pracovní místa v objemu 2 617 485,00 Kč byl rozpočet snížen na částku 320 177 297,00 Kč. Konečný rozpočet výdajů na platy, ostatní platby za provedenou práci a příslušenství ve výši 325 420 781,62 Kč byl čerpán v objemu 321 703 375,19 Kč, tedy v relativním vyjádření na 98,9 %.

Běžné výdaje

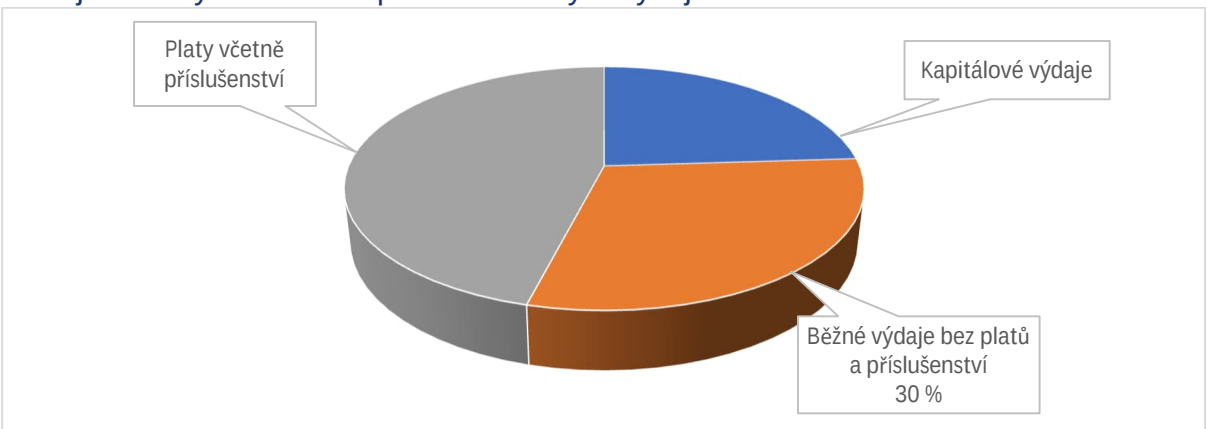
Běžné výdaje (bez výdajů na platy, ostatní platby za provedenou práci a příslušenství) byly rozpočtovány ve výši 197 412 390,00 Kč.

Rozpočtovými opatřeními byly upraveny na 196 823 847,00 Kč. Zapojením NNV byly upraveny na konečný rozpočet ve výši 225 660 275,28 Kč. Konečný rozpočet běžných výdajů byl čerpán v objemu 206 699 291,82 Kč, v relativním vyjádření na 91,6 %.

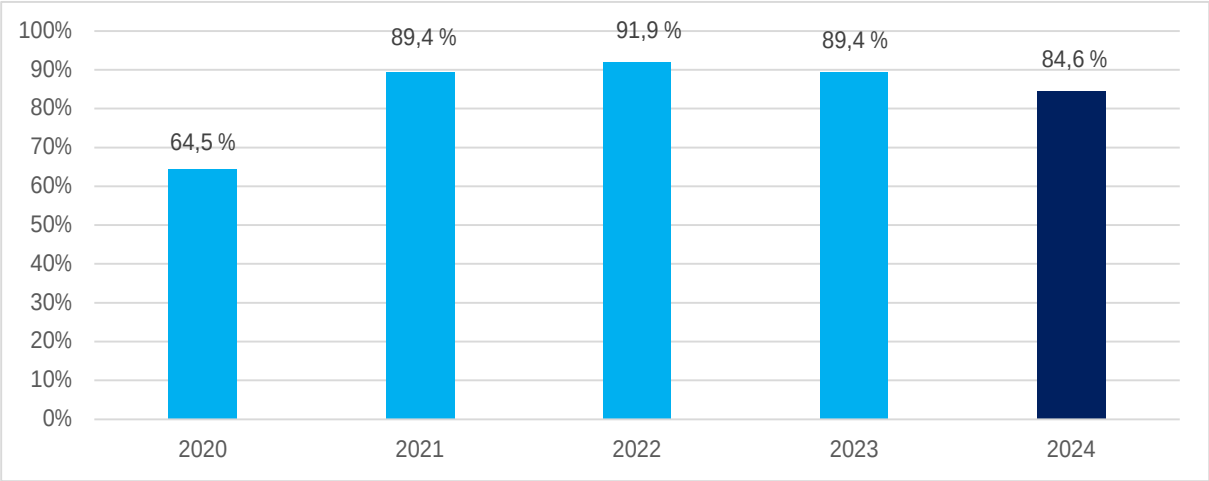
Kapitálové výdaje

Kapitálové výdaje vedené ve Správě majetku ve vlastnictví státu (dále jen „SMVS“) byly rozpočtovány v roce 2024 ve výši 90 740 241,00 Kč. Zapojením NNV pak byly kapitálové výdaje v roce 2024 upraveny na konečný rozpočet výdajů v SMVS v objemu 148 343 058,42 Kč. Konečný rozpočet kapitálových výdajů byl čerpán v objemu 87 138 711,25 Kč, v relativním vyjádření 58,7 %.

Podíl jednotlivých složek čerpání na celkových výdajích v r. 2024



Vývoj čerpání rozpočtu výdajů v letech 2020–2024



3.11.3 Projekty spolufinancované EU

NÚKIB je zapojen do dvou projektů programu Digitální Evropa na základě nařízení (EU) 2021/887 Evropského parlamentu a Rady (EU) ze dne 20. 5. 2023, kterým se zřizuje Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center, a na základě usnesení vlády ze dne 23. 8. 2021 č. 728. Dále je NÚKIB usnesením vlády ze dne 15. 3. 2023 č. 187 pověřen realizováním projektu v rámci Národního plánu obnovy.

Nástroj 14900 – IROP 2021–2027 – Výzva „Kybernetická bezpečnost – NÚKIB – SC 1.1 (ČR)“

Projekt: Černá Pole 3 – Kyberbezpečnost (reg. č. CZ.06.01.01/00/23_089/0005357)

NÚKIB, jakožto příjemce dotace, obdržel rozhodnutí o poskytnutí dotace dne 18. 10. 2024, přičemž financování akce je plánováno v letech 2025–2029. Účelem projektu je realizace technických bezpečnostních opatření podle § 5 odst. 3 ZKB a výkon státní správy v oblasti bezpečnosti informačních a komunikačních systémů. V roce 2024 nedošlo k čerpání z tohoto projektu.

Nástroj 16700 – program Digitální Evropa

Projekt: National Coordination Centre in the Czech Republic (č. 101127941 – NCC-CZ)

Projekt je realizován v období od 1. 11. 2023 do 31. 10. 2025 a jeho cílem je vybudování a podpora činnosti Národního koordinačního centra výzkumu a vývoje v oblasti kybernetické bezpečnosti, které je součástí sítě národních koordinačních center členských států a bude plnit činnosti stanovené evropským nařízením 2021/887.

Celkový rozpočet projektu činí 335 980 EUR, z toho podíl státního rozpočtu 167 990 EUR, podíl EU 167 990 EUR.

Spolupříjemcem dotace je CyberSecurity Hub, z. ú., který obdrží na realizaci projektu částku ve výši 138 030 EUR. Dále je v rámci projektu celkem 150 000 EUR určeno na podporu třetím stranám.

V roce 2024 byly čerpány výdaje v celkové výši 5 871 432,02 Kč (z toho podíl státního rozpočtu 2 935 716,02 Kč, podíl EU 2 935 716,00 Kč, přičemž unijní podíl byl čerpán prostřednictvím nároků z nespotřebovaných výdajů).

Projekt: Building Testing and Certification Capabilities in the Czech Republic (**č**. 101127940 – TEST-CERT-CZ)

Projekt je realizován v období 1. 12. 2023 až 30. 11. 2026 a podporuje budování testovacích a certifikačních schopností v ČR, a to prostřednictvím přerozdělování finanční podpory třetím stranám v této oblasti. Cílem je zlepšit schopnost a spolupráci v oblasti evropských certifikací kybernetické bezpečnosti v souladu s cíli Aktu o kybernetické bezpečnosti (Cyber Security Act).

Celkový rozpočet projektu činí 841 761 EUR, z toho podíl státního rozpočtu 0 EUR, podíl EU 841 761 EUR. Celkem 500 000 EUR je určeno na podporu třetích stran.

Spolupříjemcem dotace je rovněž CyberSecurity Hub, z. ú., který na realizaci projektu obdrží částku ve výši až 119 840 EUR.

V roce 2024 byly čerpány výdaje v celkové výši 2 875 440,74 Kč, a to prostřednictvím nároků z nespotřebovaných výdajů.

Nástroj 17014 – NPO – grant Digitální ekonomika a společnost, inovativní start-upy a nové technologie

Projekt: Czech National Quantum Communication Infrastructure (**č**. 101091684 – CZQCI)

Projekt je realizován v období 1. 3. 2023 až 31. 8. 2026 a hlavním příjemcem dotace je CyberSecurity Hub, z. ú.

Projekt je z 50 % financován z Národního plánu obnovy a z 50 % z programu Digitální Evropa.

NÚKIB byl pověřen realizováním projektu usnesením vlády č. 187/2023 a uzavřením delegační smlouvy o implementaci Národního plánu obnovy pro část komponenty 1.4 – Digitální ekonomika a společnost, inovativní start-upy a nové technologie s MPO k převzetí role subjektu implementace a naplnění administrativních úkonů pro zajištění zprostředkovaní dotace řešiteli projektu CZQCI (CyberSecurity Hub, z. ú.) včetně sledovaní čerpání finančních prostředků po dobu realizace projektu. Financování z programu Digitální Evropa si příjemce zajišťuje sám.

Rozpočtovým opatřením A-hlavička č. 1000000057 byly přesunuty příjmy a výdaje z rozpočtové kapitoly 322 – MPO do rozpočtové kapitoly 378 – NÚKIB v souvislosti se schváleným projektem CZQCI ve výši 130 000 000,00 Kč. Rozhodnutím o poskytnutí dotace č. 1/2024 byla upřesněna výše dotace příjemci podpory na částku 121 574 994,89 Kč.

3.12 Investice a rozvoj

V roce 2024 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 pokračování rozšiřování a úprav kancelářských kapacit objektu Cejl pro nově nastupující zaměstnance proběhla stavební realizace 5. etapy rekonstrukce objektu Cejl, která se týkala úprav skladových prostor a vybudování nových kancelářských prostor.

Objekt Gorkého, Brno

Na objektu Gorkého proběhly v roce 2024 drobné udržovací stavební práce (úprava akustické stěny u klimatizačních jednotek, výměna oken v 5. NP).

Administrativní budova NÚKIB, Brno – Černá Pole

Objekt budovaný v souladu s vládou schválenou Koncepcí rozvoje NÚKIB je predikovaným administrativním centrem NÚKIB v Brně. Po vydání stavebního povolení počaly v roce 2024 práce zpracovatele projektové dokumentace na dokumentaci o provedení stavby a následovala kontrola předmětné dokumentace za strany NÚKIB.

Objekt Olšanská, Praha

Pro objekt Olšanská schválila vládní dislokační komise rozšíření nájemního prostoru o jedno patro k pokrytí požadovaných kapacit. Předpoklad stavební realizace včetně interiérového a technického vybavení je v roce 2025.

Objekt „Paťanka“, Praha

V rámci zvýšení bezpečnosti vnějšího perimetru objektu bylo rozhodnuto o realizaci oplocení, k čemuž byla zpracována projektová dokumentace a zajištěna potřebná stanoviska.

3.13 Personální zabezpečení

Ke dni 31. 12. 2024 disponoval NÚKIB 373 přidělenými místy. Skutečná obsazenost systemizovaných míst k výše uvedenému datu byla 365.

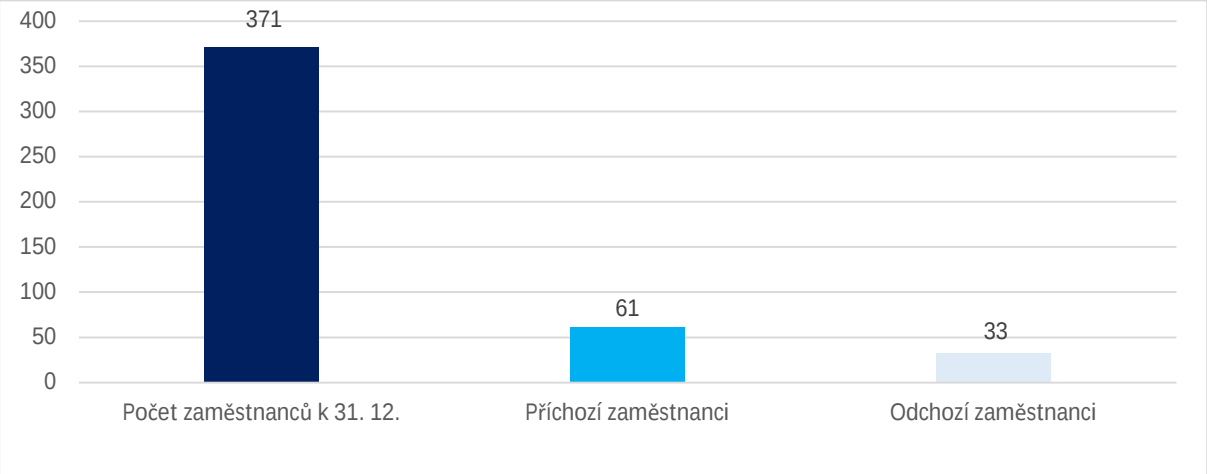
Do pracovního poměru bylo v období od 1. 1. 2024 do 31. 12. 2024 přijato 61 nových zaměstnanců. Dalších 8 zaměstnanců vykonávalo činnost na základě uzavřených dohod o pracovní činnosti a s 27 osobami byla uzavřena dohoda o provedení práce.

Do konce roku 2024 ukončilo pracovní poměr 33 zaměstnanců, tj. 8,92 % 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, 6 zaměstnanců ukončilo pracovní poměr uplynutím doby určité, 17 zaměstnanců výpovědí ze strany zaměstnance a 8 pracovních poměrů bylo ukončeno dohodou na žádost zaměstnance.

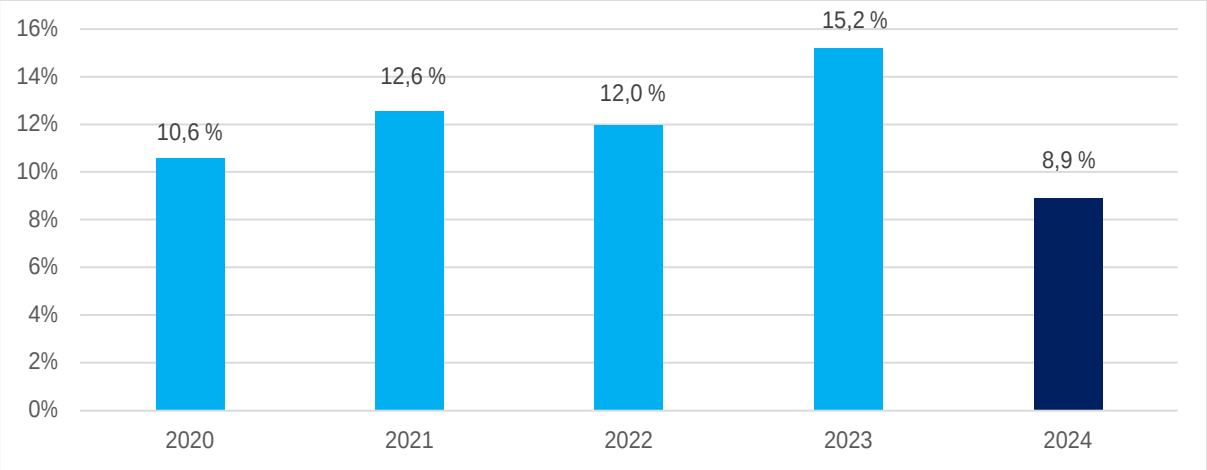
Základní přehled

Evidenční stav zaměstnanců na systemizovaných pracovních místech k 31. 12. ve fyzických počtech	371
Počet zaměstnanců dočasně mimo systemizovaná pracovní místa (mateřská a rodičovská dovolená, uvolnění k výkonu veřejné funkce)	20
Ukončení pracovních poměrů v průběhu roku 2024	33
Nástupy do pracovního poměru v průběhu roku 2024	61
Návraty z mateřské dovolené, z rodičovské dovolené a neplaceného volna v průběhu roku 2024	5
Odchody na mateřskou či rodičovskou dovolenou v průběhu roku 2024	9

Nástupy a odchody zaměstnanců v roce 2024



Fluktuace zaměstnanců NÚKIB v letech 2020–2024



Věková struktura zaměstnanců k 31. 12. 2024 (včetně zaměstnanců dočasně mimo systemizovaná pracovní místa)

Věková kategorie	Počet zaměstnanců k 31. 12. 2024	Podíl zaměstnanců v %	Z toho	
			muži	ženy
méně než 20 let	0	0,00 %	0	0
20 až 29 let	97	24,81 %	56	41
30 až 39 let	133	34,02 %	72	61
40 až 49 let	88	22,51 %	52	36
50 až 59 let	49	12,53 %	32	17
60 až 65 let	16	4,09 %	9	7
66 a více let	8	2,05 %	7	1
Celkem	391	100,00 %	228	163

Průměrný věk zaměstnance činil 39,22 roku.

Kvalifikační struktura zaměstnanců k 31. 12. 2024

Dosažené vzdělání k 31. 12. 2024 (zahrnuti jsou též zaměstnanci dočasně na MD, RD a uvolnění k výkonu veřejné funkce)	Počet zaměstnanců k 31. 12. 2024	Procentní struktura
v doktorském studijním programu	17	4,35 %
v magisterském studijním programu	269	68,80 %
v bakalářském studijním programu	40	10,23 %
vyšší odborné vzdělání	4	1,02 %
střední vzdělání s maturitní zkouškou	60	15,35 %
střední vzdělání s výučním listem	1	0,26 %
základní vzdělání	0	0,00 %
Celkem	391	100 %

Zaměstnávání osob se zdravotním postižením

V roce 2024 měl NÚKIB naplnit povinný podíl v zaměstnávání osob se zdravotním postižením ve výši 14,26 osoby. Plnění povinného podílu bylo splněno zaměstnáváním osob se zdravotním postižením ve výši 2,52 osoby a odběrem výrobků a služeb který odpovídá v přepočtu zaměstnání 11,79 osob.

3.14 Interní audit a vnitřní kontrola

V průběhu roku byl dokončen audit Fondu kulturních a sociálních potřeb, následně byl realizován audit procesu přijímání zaměstnanců, audit činnosti zaměstnanců vysílaných do zahraničí (kyberatašé) a audit whistleblowingového systému.

Veškerá auditní zjištění z provedených interních auditů byla projednána s auditovanými útvary tak, aby byla zajištěna implementace auditních doporučení a následná zpětná vazba.

V únoru roku 2024 byla odeslána MF Zpráva o výsledcích finančních kontrol na NÚKIB za předchozí kalendářní rok.

Ve spolupráci interního auditu a vedoucích zaměstnanců byla identifikována a vyhodnocena rizika NÚKIB.

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 (řídící kontrola) a interní audit,
- veřejnosprávní kontrola vykonávaná státními kontrolními orgány vůči NÚKIB.

V průběhu roku 2024 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 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.

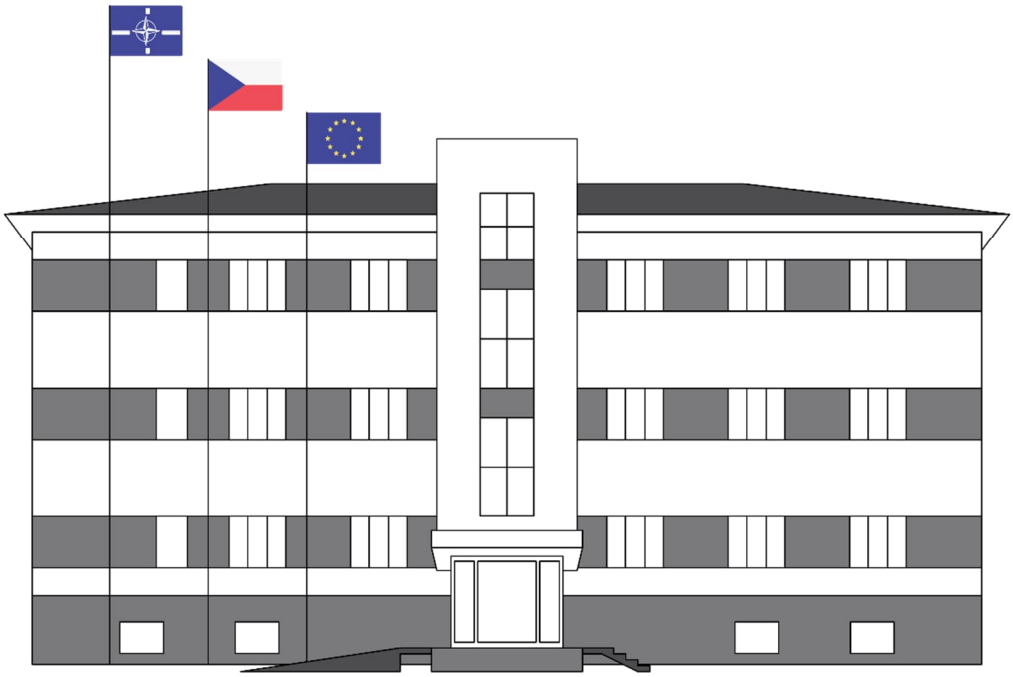
Výsledky finančních kontrol ukazují, že nastavený vnitřní kontrolní systém NÚKIB je plně funkční a zajišťuje jeho účinné a kvalitní řízení. Napomáhá včas odhalovat případné nedostatky a přijímat nápravná opatření.

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.

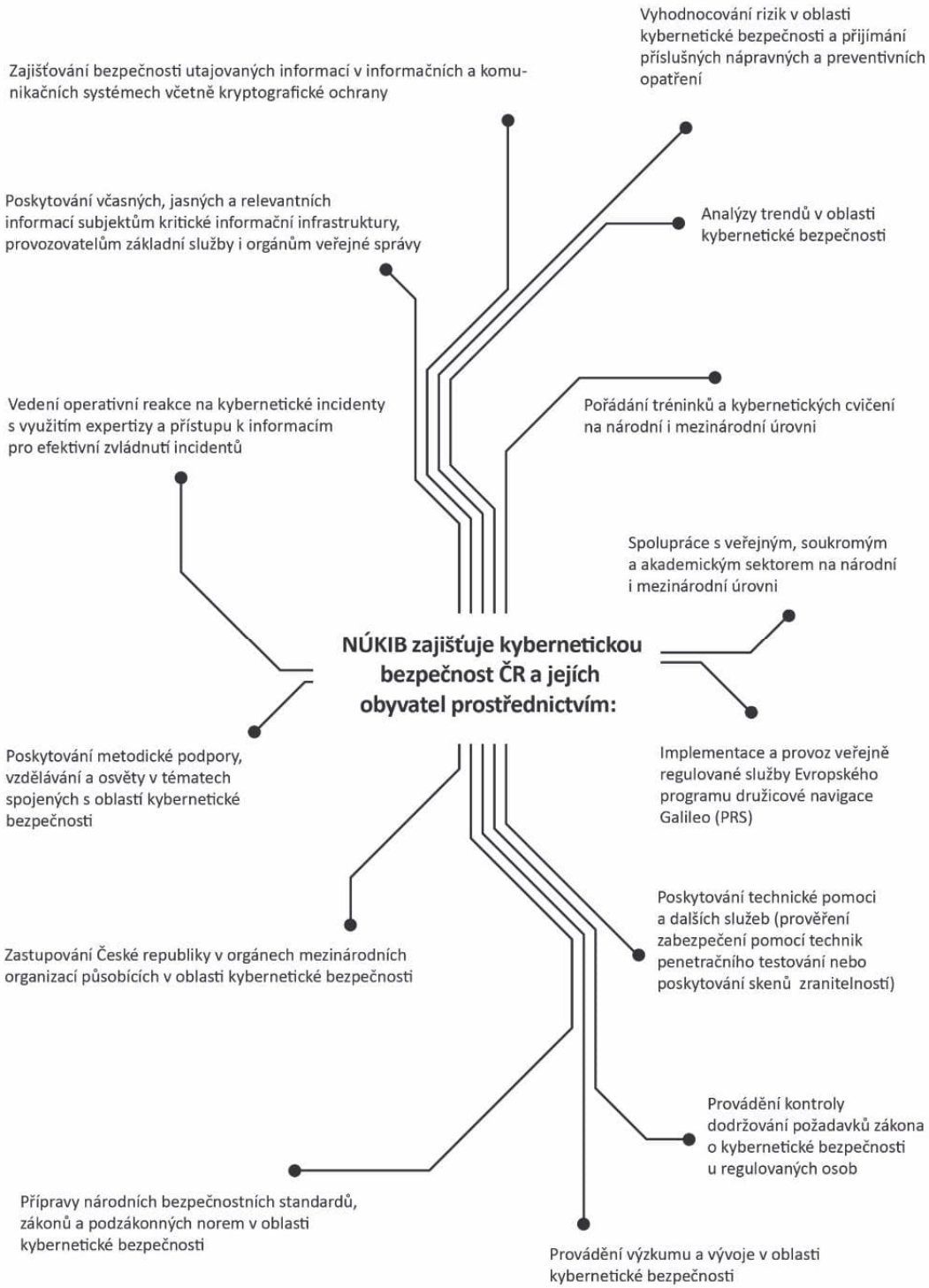
4. Seznam použitých zkratek

APEX	Allied Power Exercise
BIS	Bezpečnostní informační služba
BIVOJ	Bezpečný, inovativní, pro veřejnou správu, odolný, jednotný
BRS	Bezpečnostní rada státu
CGA	Competent Govsatcom Authority
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
CVD	Coordinated Vulnerability Disclosure (koordinované zveřejňování zranitelností)
CyCLONe	Crisis Liaison Organisation Network
ČR	Česká republika
DDoS	Distributed Denial of Service
EDR	Endpoint Detection and Response (detekce a reakce koncových bodů)
EU	Evropská unie
EUSPA	European Agency For Space Program (Agentura Evropské unie pro Kosmický program)
GOVSATCOM	Governmental Satellite Communications
GRON	Galileo Robust Operation Network
GSMC	Galileo Security Monitoring Centre (Bezpečnostní a monitorovací centrum programu Galileo)
HWPCI	Horizontal Working Party on Cyber Issues
ICT	Information and Communication Technologies (informační a komunikační technologie)
LRV	Legislativní rada vlády
MF	Ministerstvo financí
MO	Ministerstvo obrany
MPO	Ministerstvo průmyslu a obchodu
MU	Masarykova univerzita
MV	Ministerstvo vnitra
MZV	Ministerstvo zahraničních věcí
NATO	North Atlantic Treaty Organization (Severoatlantická aliance)
NATO CCD COE	Cooperative Cyber Defence Centre of Excellence (NATO Centrum excelence pro kybernetickou obranu)
NIS CG	The Network and Information Systems Cooperation Group
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
nZKB	nový zákon o kybernetické bezpečnosti
POCP	Galileo Point of Contact Platform (platforma kontaktních míst systému Galileo)
PRS	Public Regulated Service (Veřejně regulovaná služba Evropského programu družicové navigace Galileo)

SCADA	Supervisory Control and Data Acquisition (dispečerské řízení a sběr dat)
SMVS	správa majetku ve vlastnictví státu
SW	software
TEMPEST	Telecommunication Electronics Materials Protected from Emanating Spurious Transmissions
USA	United States of America (Spojené státy americké)
USC	Union Secure Connectivity
VZ	Vojenské zpravodajství
ZKB	zákon o kybernetické bezpečnosti
ZoOUI	zákon o ochraně utajovaných informací a bezpečnostní způsobilosti



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 veřejně regulované služby v rámci družicového systému Galileo. NÚKIB vznikl 1. 8. 2017 na základě zákona č. 205/2017 Sb., kterým se změnil zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).


NÚKIB zajišťuje kybernetickou bezpečnost ČR a jejích obyvatel prostřednictvím:
Vyhodnocování rizik v oblasti kybernetické bezpečnosti a přijímání příslušných nápravných a preventivních opatření
Zajišťování bezpečnosti utajovaných informací v informačních a komunikačních systémech včetně kryptografické ochrany
Analýzy trendů v oblasti kybernetické bezpečnosti
Poskytování včasných, jasných a relevantních informací subjektům kritické informační infrastruktury, provozovatelům základní služby i orgánům veřejné správy
Pořádání tréninků a kybernetických cvičení na národní i mezinárodní úrovni
Vedení operativní reakce na kybernetické incidenty s využitím expertizy a přístupu k informacím pro efektivní zvládnutí incidentů
Spolupráce s veřejným, soukromým a akademickým sektorem na národní i mezinárodní úrovni
Poskytování metodické podpory, vzdělávání a osvěty v tématech spojených s oblastí kybernetické bezpečnosti
Implementace a provoz veřejně regulované služby Evropského programu družicové navigace Galileo (PRS)
Zastupování České republiky v orgánech mezinárodních organizací působících v oblasti kybernetické bezpečnosti
Poskytování technické pomoci a dalších služeb (prověření zabezpečení pomocí technik penetračního testování nebo poskytování skenů zranitelností)
Provádění kontroly dodržování požadavků zákona o kybernetické bezpečnosti u regulovaných osob
Přípravy národních bezpečnostních standardů, zákonů a podzákonných norem v oblasti kybernetické bezpečnosti
Provádění výzkumu a vývoje v oblasti kybernetické bezpečnosti