NÚKIB

# ZPRÁVA O ČINNOSTI 2023

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU
A INFORMAČNÍ BEZPEČNOST

# OBSAH

# 1. Úvodní slovo ředitele

Vážené dámy, vážení pánové,

uplynulý rok byl pro NÚKIB opět rokem dynamickým, plným výzev i příležitostí. Pokračující trend rostoucího počtu kybernetických útoků, kterým jako společnost čelíme, znamenal zvýšené úsilí věnované podpoře a pomoci zasaženým institucím – takových případů bylo za loňský rok 262. Zhoršující se bezpečnostní kontext zvyšuje také poptávku po bezpečné komunikaci a s tím rostou požadavky v oblasti ochrany utajovaných informací v informačních systémech. V loňském roce jsme vydali celkem 164 certifikátů k informačním systémům, kryptografickým prostředkům a pracovištím.

Velké úsilí bylo v souladu s plánem legislativních prací věnováno vypořádání připomínek k návrhu nového zákona o kybernetické bezpečnosti, upravujícího také problematiku prověřování bezpečnosti dodavatelů do strategicky významné infrastruktury České republiky. V souvislosti s legislativním procesem jsme kladli důraz na transparentní komunikaci směrem k odborné i široké veřejnosti a za tímto účelem jsme podnikli stejně jako v předcházejícím roce nespočet aktivit nejen při prosazování potřebných řešení, zejména však k upevnění vzájemné důvěry mezi státní, soukromou a akademickou sférou.

Neméně důležité byly práce na novele zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti včetně prováděcích vyhlášek.

Výrazný nárůst počtu uživatelů našich vzdělávacích aktivit v podobě kurzů a osvětových kampaní poukazuje nejen na jejich aktuálnost a potřebu, ale i užitek, který přinášejí jak odborné, tak široké veřejnosti.

Žádaná je také účast našich kolegyň a kolegů na seminářích, workshopech, konferencích a v podcastech. V roce 2023 jsme uspořádali vlastní již zavedené a úspěšné akce, jako jsou CyberCon Brno nebo Festival bezpečného internetu, a realizovali přípravy na Prague Cyber Security Conference 2024.

Dařilo se nám působit na mezinárodním poli a posilovat postavení v organizacích a uskupeních, ve kterých zastupujeme zájmy České republiky v oblasti kybernetické a informační bezpečnosti.

Stěžejní záležitostí byla v posledních letech, a i nadále zůstává, personální práce a vytvoření co nejlepších podmínek pro stávající a nově příchozí kolegyně a kolegy. Je třeba reagovat a hledat řešení na nepříznivý trend nárůstu fluktuace, kde nemalou roli hrají ztížené podmínky konkurenceschopnosti finančního ohodnocení odborníků ve vztahu k soukromé sféře. Bez osobní angažovanosti a nasazení nad rámec pracovních povinností bychom nemohli dosahovat tak skvělých výsledků a plnit úkoly v takovém rozsahu.

Úspěšným naplněním vytyčených cílů a splněním zadaných úkolů NÚKIB přispěl k bezpečnějšímu prostředí České republiky, k ochraně našich spoluobčanů a v souladu se svým posláním posiloval bezpečnost a odolnost České republiky v kyberprostoru.

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 pokračuje v nastoleném trendu z minulých let v navazování nové a prohlubování stávající spolupráce s institucemi veřejného i soukromého sektoru, a to jak tuzemskými, tak zahraničními. V rámci této spolupráce se podílel na tvorbě mnoha strategických a legislativních materiálů a organizaci pracovních skupin a konferencí či se do nich aktivně zapojoval jako účastník. Mezi nejvýznamnější aktivity NÚKIB za rok 2023 v této oblasti patří následující.

**Projekt BIVOJ**

V průběhu roku 2023 pokračovala příprava projektu BIVOJ (bezpečný, inovativní, pro veřejnou správu, odolný, jednotný). Cílem projektu BIVOJ je zajistit centrální správu a řízení bezpečnosti sdílených informačních a komunikačních systémů a služeb organizací veřejného sektoru České republiky. Projekt představuje komplexní bezpečnostní program, který obsahuje více jednotlivých komponent, které k posílení kybernetické bezpečnosti přispívají jak samostatně (např. jednotná doména gov.cz, bezpečná síť, komunikační nástroj pro neutajovanou, instantní a bezpečnou komunikaci, bezpečné DNS), tak ve vzájemném propojení. Koordinátorem tohoto projektu byl v roce 2023 nadále NÚKIB, úzce na něm spolupracoval i s dalšími institucemi, jako jsou Vojenské zpravodajství (dále jen „VZ“), Ministerstvo vnitra (dále jen „MV“), Ministerstvo financí (dále jen „MF“), Úřad vlády České republiky či kabinet místopředsedy vlády pro digitalizaci. V závěru roku 2023 zpracoval NÚKIB analýzu strategického směřování projektu a doporučil variantu jeho budoucího řízení, která byla předložena k projednání Bezpečnostní radě státu (dále jen „BRS“) a k rozhodnutí o dalším postupu v projektu.

**Projekt koordinované zveřejňování zranitelností (dále jen „CVD“)**

V roce 2023 NÚKIB finalizoval návrh národní politiky CVD, která má za cíl podporovat nalézání zranitelností v produktech informačních a komunikačních technologií (dále jen „ICT“) napříč subjekty v České republice bez hrozby negativních právních dopadů pro objevitele zranitelností. S ohledem na specifické právní aspekty CVD se NÚKIB v roce 2023 zaměřil zejména na detailní analýzu všech relevantních právních oblastí CVD (v trestním právu, v problematice náhrady škody, ochraně osobních údajů či dotčených práv třetích osob). NÚKIB dále zahájil přípravu implementace vlastní CVD politiky na vybranou infrastrukturu, kterou užívá a u které je minimální bezpečnostní riziko způsobení škody či jiné újmy ze strany objevitelů zranitelností. Zavedením CVD ve svých systémech chce jít NÚKIB příkladem a zároveň získat cenná data, ze kterých bude moci vycházet při rozvoji národní politiky CVD a mezinárodních dokumentů v této oblasti.

**Koncepce ochrany neutajovaných informací citlivé povahy**

Zpracování Koncepce ochrany neutajovaných informací citlivé povahy je úkolem z Akčního plánu k Národní strategii kybernetické bezpečnosti České republiky. Po zpracování analýzy stávajícího stavu a prvotních diskusích s interními a externími partnery byl v roce 2023 vypracován interní návrh Koncepce ochrany neutajovaných informací citlivé povahy.

### Národní politika kryptografické ochrany utajovaných informací

V průběhu roku 2023 zpracoval NÚKIB také prvotní návrh Národní politiky kryptografické ochrany utajovaných informací. Vypracování tohoto strategického dokumentu pro oblast zpracování utajovaných informací (dále také jako „UI“) v informačních systémech ukládá zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů (dále jen „ZoOUI“).

### Projekt Kyberliga

NÚKIB interně zpracoval varianty rozvoje projektu Kyberliga, vycházející z aktuálního vývoje prostředí, a to zejména z hlediska personálních nároků přípravy a implementace nového zákona o kybernetické bezpečnosti. Projekt Kyberliga si klade za cíl zapojit dobrovolníky z řad kybernetických expertů a institucionalizovat jejich využití při zajišťování kybernetické bezpečnosti.

## 3.2 Vyhodnocení a řešení kybernetických bezpečnostních událostí a incidentů

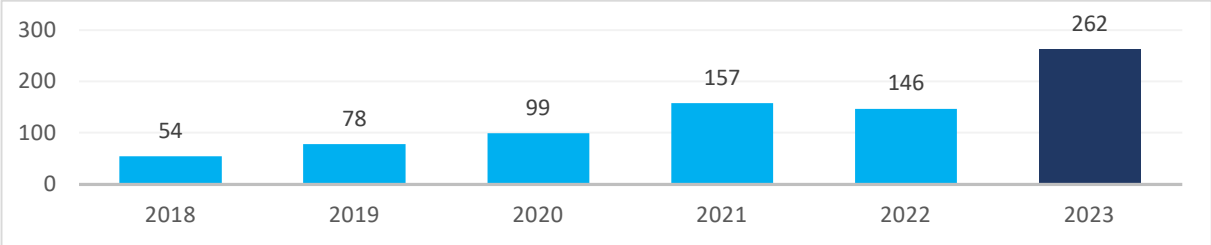
### Změny v rámci klasifikace incidentů

Při revalidaci a reklasifikaci některých údajů o kybernetických bezpečnostních incidentech (dále jen „incidenty“) se tyto údaje již nemohly zpětně propsat do zveřejněných měsíčních přehledů o incidentech. Z tohoto důvodu byly zavedeny nové interní metriky, na jejichž základě jsou incidenty vyhodnocovány. Nejvýraznější změnou je volba jiného klíčového časového údaje. Incidenty jsou nyní řazeny podle data zaevidování na straně NÚKIB namísto data jejich vzniku.

### Shrnutí dění v kyberprostoru za rok 2023 pohledem NÚKIB

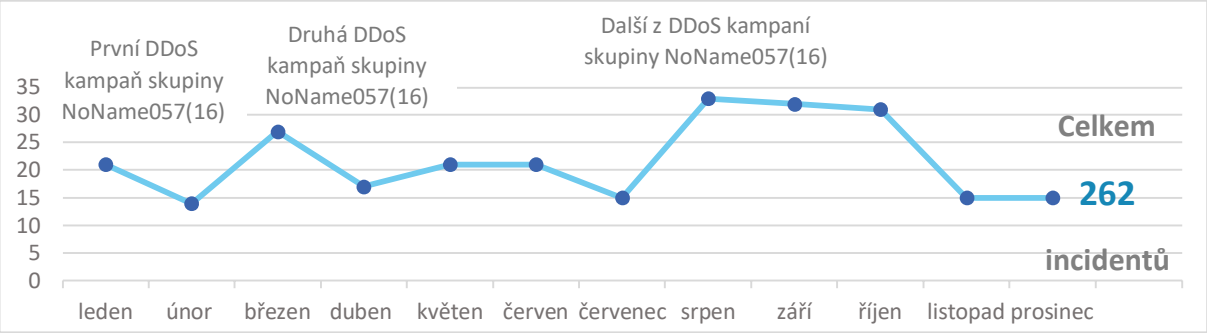
NÚKIB v roce 2023 evidoval celkem 262 incidentů. Oproti roku 2022, kdy bylo evidováno 146 incidentů, tak došlo k téměř 80% nárůstu. Za tímto nárůstem stojí primárně opakované vlny DDoS útoků vedených zejména proruskými hacktivistickými skupinami.

**Vývoj počtu incidentů evidovaných NÚKIB v letech 2018–2023**

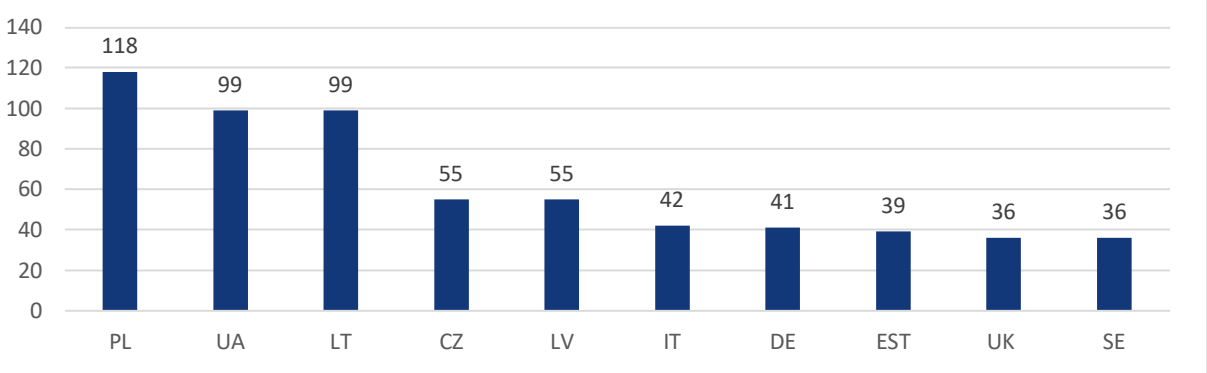



DDoS útoky tvořily významnou část všech evidovaných incidentů v roce 2023. Jednoznačně nejčastějším původcem těchto útoků byla skupina NoName057(16), která na české cíle útočila pravidelně. Kampaně NoName057(16) vůči českým cílům zpravidla probíhaly v návaznosti na dění či výroky spojené s konfliktem na Ukrajině a Česká republika patřila mezi tímto aktérem nejzasaženější státy Evropy. Zaznamenané útoky však neměly závažnější dopady a v naprosté většině vedly pouze k dočasné nedostupnosti webových stránek napadených subjektů. DDoS útoky obecně zahlcují provoz na webových stránkách a službách přístupných z internetu, informační systémy organizací však nekompromitují.

### Vývoj počtu incidentů řešených NÚKIB v roce 2023




### Počet deklarovaných DDoS útoků skupinou NoName057(16) proti evropským státům

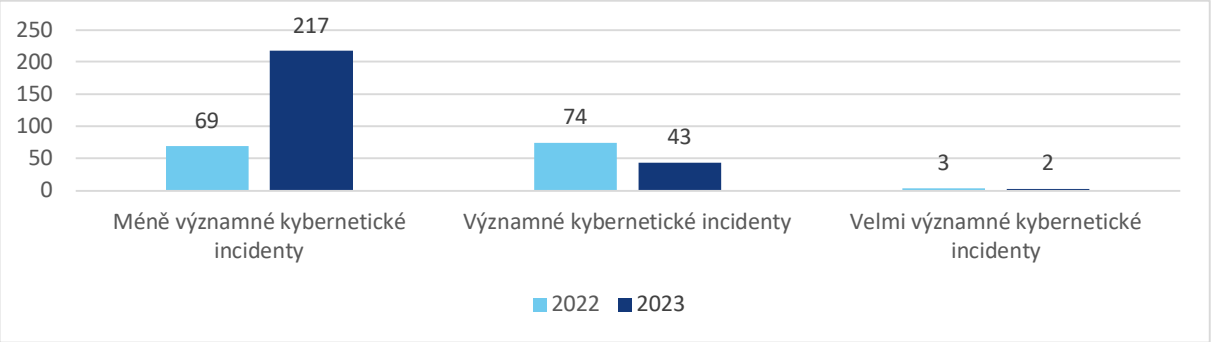



NÚKIB v roce 2023 evidoval také řadu DDoS útoků, u nichž nebyl identifikován původce. Specifickým případem byla kampaň nazvaná DNS NXDOMAIN. Tato kampaň byla specifická zejména tím, že u ní nebyl zřetelný vzorec výběru oběti (tedy že by jednotlivé útoky byly vázány např. na geopolitické dění nebo činnost napadených obětí), který by umožňoval objasnit aktivity útočníka. Jediným vodítkem tak kromě využívaných technik a infrastruktury zůstává specifická viktimologie, v jejímž rámci NÚKIB zaznamenal útoky cílené výhradně na české státní instituce.

V průběhu června NÚKIB zaznamenal zvýšený zájem ransomwarových aktérů o některé české strategické cíle, což vedlo k vydání upozornění na zvýšené riziko ransomwarových útoků. Nejvýrazněji se pak do statistik propsaly aktivity gangů PLAY a LockBit, což zrcadlí i globální trend. Mimo výše uvedené NÚKIB registroval také řadu phishingových kampaní, a to jak ze strany státem podporovaných aktérů, tak kyberkriminálních skupin.

Z pohledu závažnosti evidovaných incidentů bylo možné sledovat pozitivní vývoj. Navzdory výraznému nárůstu počtu incidentů došlo k meziročnímu snížení počtu významných a velmi významných kybernetických incidentů. Zatímco méně významných incidentů přibylo více než trojnásobně, významných incidentů ubylo o třetinu. Nárůst počtu a pokles závažnosti evidovaných incidentů lze vysvětlit opakovanými DDoS útoky proti českým cílům, zpravidla však bez významnějších a dlouhodobějších dopadů.

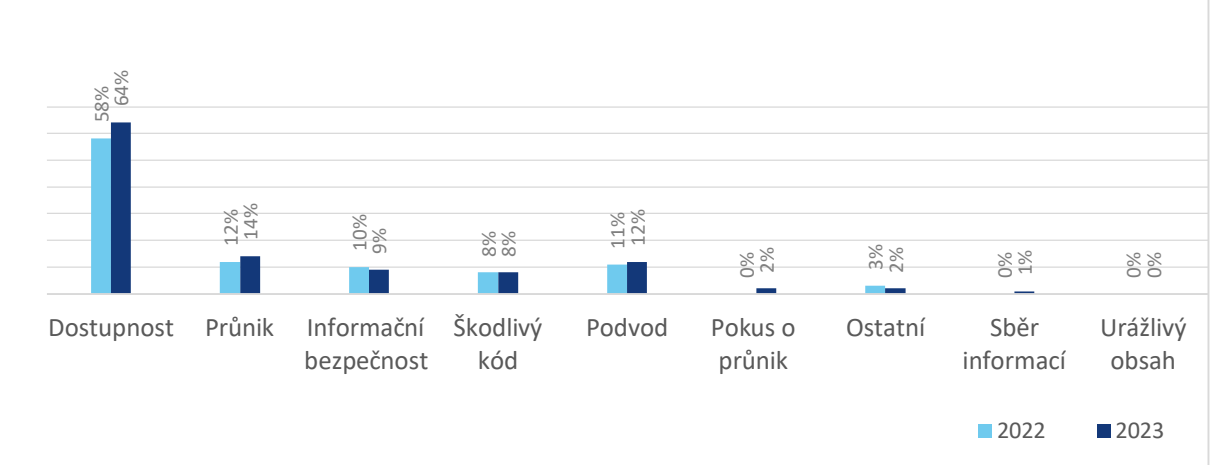
**Meziroční srovnání závažnosti incidentů evidovaných NÚKIB v letech 2022–2023**




V krátkodobém výhledu následujících tří let lze předpokládat, že budou pokračovat některé nastolené trendy. I nadále bude pravděpodobně docházet ke kybernetickým útokům v reakci na geopolitické dění či jiné politicky citlivé události, a to ne zcela nutně pouze v souvislosti s ukrajinským konfliktem. V těchto případech lze očekávat zapojení zejména různých hacktivistických skupin, nelze však vyloučit ani působení jiných typů aktérů. Podobně jako v uplynulých letech pak lze očekávat řadu plošných phishingových kampaní vůči státním i soukromým subjektům, ale také ransomwarové útoky napříč odvětvími.

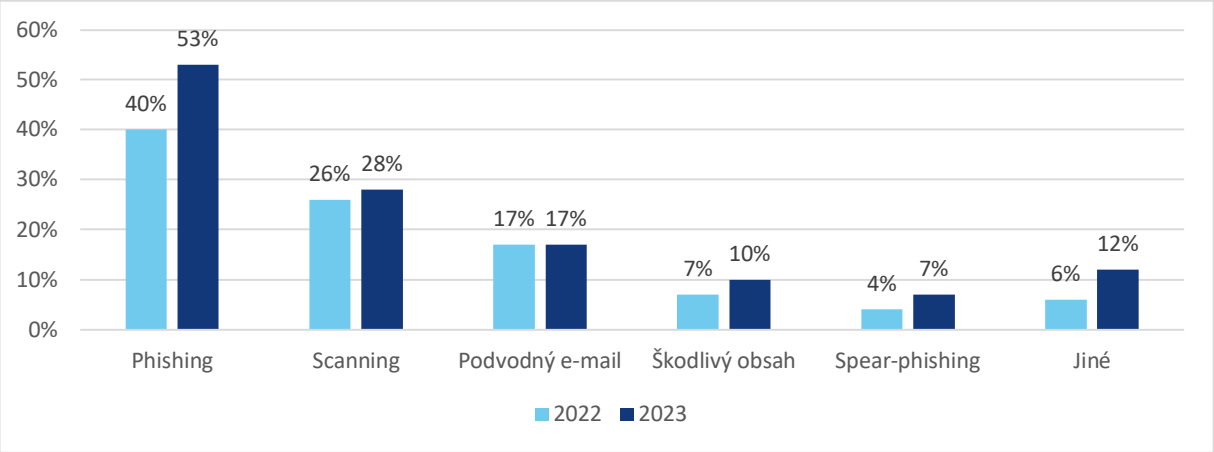
Z hlediska klasifikace nejvíce převažovaly incidenty cílící na dostupnost (např. webových stránek či služeb), což odpovídá vysokému počtu zaznamenaných DDoS útoků. Tato kategorie nicméně obsahuje také řadu incidentů, za kterými nestojí útoky, ale například technické chyby vedoucí k výpadku systémů. Druhou nejpočetnější pak byla kategorie průnik. Sem spadaly zpravidla útoky využívající metod sociálního inženýrství, nejčastěji phishingové útoky vedoucí ke kompromitaci e-mailových či jiných účtů. Třetí nejčastěji evidovanou pak byla kategorie informační bezpečnost, v jejímž rámci převládaly ransomwarové útoky.

**Procentuální zastoupení v incidentech**




Statistikám kybernetických útoků dlouhodobě dominuje phishing, nicméně z letošních dat vyplývá, že se využívání této techniky dále stupňuje. Během roku 2023 lze pozorovat výrazný nárůst této kategorie. Nárůst lze vidět taktéž v kategorii cílených spear-phishingových útoků, což odpovídá obecnému trendu rostoucí četnosti i kvality phishingu, který vyplývá i z dalších poznatků činnosti NÚKIB.

**Kategorie nejčastějších typů kybernetických útoků v letech 2022–2023 (% respondentů)**




## 3.3 Monitoring, analytická činnost a informační podpora

V roce 2023 došlo k transformaci analytického pracoviště, které nově pracuje na modelu centrální analytiky. Strategická analytika spolu s nově se rozvíjejícím týmem věnujícím se informačním šetřením poskytovaly analytickou podporu dovnitř NÚKIB i mimo něj, zejména partnerům z bezpečnostní komunity, rozhodujícím činitelům v české státní správě nebo vybraným partnerům v zahraničí. V oblasti datové analytiky probíhal rozvoj stávajících a implementace nových nástrojů za účelem celkového zefektivnění analytických procesů a zkvalitnění finálních produktů. Pokračovalo budování analytické kapacity v podobě Cyber Threat Intelligence, která napomáhala při řešení významných incidentů. V roce 2023 byly také kultivovány analytické vztahy s prioritními tuzemskými partnery (např. bezpečnostní komunita) a také s partnery zahraničními (především v západní Evropě, Pobaltí či regionu Indo-Pacifiku).

## 3.4 Kontrola, dohled a metodická pomoc

### 3.4.1 Kybernetická bezpečnost

Rok 2023 byl stejně jako rok 2022 z pohledu kontrolní a auditní činnosti ovlivněn eskalací geopolitické situace ve světě. I v tomto roce jsme proto pokračovali v prověřování kybernetické bezpečnosti klíčových subjektů zajišťujících základní fungování státu a především služby občanům.

Celkem bylo v roce 2023 provedeno 20 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. Je-li při kontrole zjištěno porušení povinností vyplývajících ze ZKB, jsou kontrolované osobě uložena nápravná opatření, případně pokuty za přestupek. V návaznosti na provedení auditu nejsou nápravná opatření ani pokuty za přestupek ukládány.

Nad rámec standardních auditů a kontrol byl taktéž vykonán tzv. komplexní audit, který zahrnuje nejenom samotné ověření stavu organizace formou auditu, v jehož rámci jsou prováděny rozhovory a případné ukázky reálného nastavení některých zařízení, ale i penetrační testování, skenování zranitelností a table-top cvičení. Takto provedený

komplexní audit poskytuje organizaci úplnou zpětnou vazbu o stavu kybernetické bezpečnosti a její připravenosti čelit případným kybernetickým bezpečnostním incidentům.

Dále byl ve spolupráci se sdružením CZ.NIC na základě usnesení vlády České republiky ze dne 11. ledna 2023 č. 23, o záměru migrace na jednotnou doménu a vytvoření jednotné vizuální identity ústředních orgánů státní správy, proveden audit domény gov.cz.

V rámci kooperace s ostatními regulátory byly provedeny kontrolní činnosti ve spolupráci s Českou národní bankou, Českým telekomunikačním úřadem (dále jen „ČTÚ“) a Úřadem pro civilní letectví.

V oblasti kybernetické bezpečnosti NÚKIB posuzuje žádosti subjektů veřejné správy o stanovisko k záměru výdaje v oblasti informačních a komunikačních technologií. Stanovisko vydává Digitální a informační agentura (dále jen „DIA“). Požadavek na kybernetickou bezpečnost lze považovat za součást požadavku na architektonickou konzistenci s architekturou eGovernmentu. Cílem je zajistit, aby posuzované informační systémy byly v souladu se ZKB a jeho prováděcími právními předpisy.

**Regulace cloud computingu**

NÚKIB v procesu zápisu poskytovatelů a jejich služeb do katalogu cloud computingu, který vede DIA, dává vstupy do obou fází tohoto procesu. Při procesu zápisu poskytovatele do katalogu cloud computingu vydává NÚKIB závazné stanovisko o způsobilosti poskytovatele poskytovat základní úroveň ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy a dále informuje o tom, jestli je poskytovatel způsobilý pro poskytnutí cloud computingu orgánu veřejné správy z hlediska veřejného pořádku, bezpečnosti a dodržování práv třetích osob. V 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.

### 3.4.2 Bezpečnost informačních a komunikačních systémů

V říjnu 2023 proběhla u NÚKIB a u vybraných subjektů státní správy inspekce EU v oblasti ochrany utajovaných informací EU v informačních systémech České republiky a jejich kryptografické ochraně při distribuci a ukládání materiálu k zajištění jeho funkce.

Ze zápisu inspekce EU, který NÚKIB obdržel prostřednictvím Národního bezpečnostního úřadu (dále jen „NBÚ“) vyplývá, že Česká republika je v oblasti ochrany utajovaných informací EU v informačních systémech a její kryptografické ochraně v souladu s legislativou EU, NÚKIB zajišťuje řádný výkon ochrany utajovaných informací EU v informačních systémech, včetně její kryptografické ochrany, a inspekce nezjistila v kontrolovaném období jakékoliv nedostatky.

#### 3.4.2.1 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 resortů státní správy a podnikatelů vykonával certifikační a metodickou činnost, včetně kontrol ve spolupráci s NBÚ.

V roce 2023 probíhalo řízení o certifikaci u 202 informačních systémů. K 46 žádostem o certifikaci informačního systému, jejichž zpracování bylo zahájeno v roce 2022, přibylo v roce

2023 dalších 146 žádostí, a to 51 ze státní správy nebo samosprávy a 95 od podnikatelů. Ve většině případů se jednalo o žádosti o opakovanou certifikaci již provozovaných informačních systémů. Ve 35 případech byla podána žádost o certifikaci nově budovaného informačního systému.

V roce 2023 bylo vydáno celkem 135 certifikátů informačních systémů pro žadatele ze státní správy nebo samosprávy, podnikatele, včetně akreditací informačních systémů cizí moci.

#### 3.4.2.2 Certifikace kryptografických prostředků a pracovišť

NÚKIB plnil úkoly Národního bezpečnostního komunikačního střediska. Z pozice národní certifikační autority ve věci certifikace kryptografických prostředků a pracovišť resortů státní správy a podnikatelů vykonával certifikační a metodickou činnost.

V roce 2023 NÚKIB vydal 24 certifikátů kryptografického prostředku, 5 certifikátů kryptografického pracoviště a schválil 4 zástavby kryptografického prostředku.

#### 3.4.2.3 Ochrana proti kompromitujícímu vyzařování a certifikace stínicích komor

**TEMPEST měření elektronických zařízení**

NÚKIB prováděl TEMPEST měření podle standardů NATO řady SDIP, EU řady IASG 7 a podle metodiky bezpečnostních standardů NBÚ. Objektem měření byla především zařízení orgánů státu. Jednalo se jak o měření komerčních zařízení, tak speciálních informačních systémů.

Celkem bylo v roce 2023 provedeno více než 50 měření různých typů zařízení. Z toho bylo prováděno TEMPEST měření samostatných zařízení v kombinaci s kryptografickým prostředkem PCS1 či novými systémy VTC GearLab pro Armádu České republiky. Tato měření byla prováděna podle metodiky standardu SDIP-27/2. Další TEMPEST měření byla prováděna v rámci certifikace nebo akreditace informačních systémů pro zpracování utajovaných informací stupně utajení Důvěrné a Tajné pro orgány státu, Úřad vlády České republiky, Ministerstvo zahraničních věcí (dále jen „MZV“), Ministerstvo obrany (dále jen „MO“), MV, Ministerstvo průmyslu a obchodu (dále jen „MPO“), zpravodajské služby nebo soukromý sektor.

**Zónové měření, instalační záznamy, obranné prohlídky**

NÚKIB dále prováděl ohodnocování prostorů metodou zónového měření. Jednalo se o prostory, ve kterých se nacházela zařízení zpracovávající utajované informace. Tento druh měření byl použit především u objektů NÚKIB, Bezpečnostní informační služby (dále jen „BIS“), MO a MV. Na žádost bylo provedeno zónové měření pro státní subjekt Severní Makedonie. Další zónová měření byla prováděna pro státní správu i pro soukromé subjekty v rámci certifikace informačních systémů. Zónové hodnocení prostorů bylo rovněž prováděno na základě podkladů dodaných akreditovanými pracovišti MO, BIS a VZ.

Bylo provedeno hodnocení instalace informačních systémů zpracovávajících utajované informace stupně utajení Důvěrné a Tajné a v rámci certifikace těchto systémů byly zpracovány instalační záznamy z více než 10 lokalit.

V roce 2023 byly provedeny obranné prohlídky v několika objektech jak v České republice, tak mimo Českou republiku na základě žádostí orgánů státní správy nebo v rámci certifikace informačních systémů.

**Přehled provedených měření**

| Typ měření | Počet |
|---|---|
| Zónové měření | 10 lokalit |
| Kryptografické prostředky | 2 typy |
| Komponenty ICT | 50 systémů |
| Audiotechnika | 4 typy zařízení |
| Obranné prohlídky i v rámci certifikace informačních systémů | 15 objektů |
| Mobilní systémy | 3 systémy |
| Instalační záznamy | >10 lokalit |
| Stínicí komory | 49 certifikátů |

### 3.4.2.4 Národní distribuční středisko

NÚKIB plnil roli Národního distribučního střediska (dále jen „NDS“) zahrnujícího výrobu a evidenci kryptografického materiálu (dále jen „KM“) a materiálu k zajištění funkce kryptografického prostředku (dále jen „KP“), prováděl distribuci a evidenci KM České republiky a EU a KM na základě mezinárodní smlouvy prostřednictvím Crypto Distribution Authority.

V roce 2023 bylo NÚKIB vygenerováno celkem 59 122 kryptografických klíčů a hesel uložených na 4 151 nosičích různých typů a dalších 34 kusů jiného KM (procesory, paměti, provozní kryptografická dokumentace, instalační a šifrovací SW).

Do evidence byla vzata a provedena distribuce celkem 696 kusů nového kryptografického a Controlled Cryptographic Item materiálu, zajištěn servis a opravy na území České republiky u 213 kusů KP a mimo Českou republiku u 29 kusů KP.

Byla zajištěna výroba, evidence a distribuce celkem 37 kusů KM EU a zajištěna přeprava na servis 1 kusu KP EU.

NÚKIB v roce 2023 vydal 160 osvědčení o zvláštní odborné způsobilosti pracovníka kryptografické ochrany.

### 3.4.2.5 Vývoj kryptografických prostředků

NÚKIB prováděl základní a aplikovaný výzkum a vývoj v oblasti kryptografie, kryptoanalýzy a KP, vyvíjel a schvaloval národní šifrové algoritmy a vytvářel národní politiku kryptografické ochrany.

Zabezpečoval vývoj kryptografických schémat pro použití KP k ochraně UI, prováděl analýzy a hodnocení šifrových systémů a kryptografických algoritmů určených k ochraně UI a podílel se na zajišťování veřejných zakázek v oblasti výzkumu, vývoje a výroby KP.

Vlastními zdroji byl vyvinut nový KP ECAr, určený pro ochranu UI stupně utajení Vyhrazené. KP je v současnosti ve fázi certifikace.

### 3.4.3 Správní řízení

V roce 2023 NÚKIB pravomocně rozhodl o dvou přestupcích na úseku zákona ZKB. Proti jednomu rozhodnutí byla podána správní žaloba, která byla Krajským soudem v Brně

zamítnuta. Proti druhému rozhodnutí nebyla podána správní žaloba a pokuta byla v obou případech uhrazena.

NÚKIB zahájil tři přestupková řízení pro porušení povinností stanovených ZKB, ve kterých bylo rozhodnuto pouze nepravomocně. V rámci správního řízení byly podány opravné prostředky, a případy tak v roce 2023 nebyly pravomocně skončeny.

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

NÚKIB zahájil jedno přestupkové řízení pro podezření ze spáchání přestupku podle ZoOUI, které nebylo v průběhu roku 2023 pravomocně skončeno.

## 3.5 Bezpečnost satelitních služeb

### 3.5.1 Veřejně regulovaná služba Evropského programu družicové navigace Galileo (PRS)

V uplynulém roce byla provedena první fáze zástavby technologie GRON určené pro zabezpečenou komunikaci s GSMC, jejíž úplné zprovoznění se předpokládá v první polovině roku 2024.

Byl dokončen testovací projekt pro pilotní ověření prototypů přijímačů PRS (P3RS2) s názvem GIMME, který byl součástí JTA EUSPA.

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 Security Accreditation Board a Security Accreditation Panel, jejichž jednání probíhají v EUSPA a v nichž se řeší bezpečnost a akreditace komponent evropského vesmírného programu. V roce 2023 byla projednávána hlavně migrace systému Galilea na nový System Build SB2.0, a tím umožnění přechodu otevřené služby do plně operační fáze a služby PRS do počátečních operačních schopností. Dále bylo řešeno vynášení satelitů na orbitu mimo území EU. V neposlední řadě se NÚKIB věnoval bezpečnostní akreditaci prvků pozemní infrastruktury a posílení kybernetické bezpečnosti v rámci kosmického programu.

### 3.5.2 GOVSATCOM a Union Secure Connectivity

GOVSATCOM je družicová komunikace pro účely státní správy a je to jedna ze složek Kosmického programu Unie, zavedeného nařízením Evropského parlamentu a Rady 2021/696. V rámci evropského programu Union Secure Connectivity zavedeného nařízením Evropského parlamentu a Rady 2023/588 bude vznikat družicová infrastruktura IRIS$^2$, která zajistí komunikační služby a vysokorychlostní širokopásmový internet s celosvětovým pokrytím.

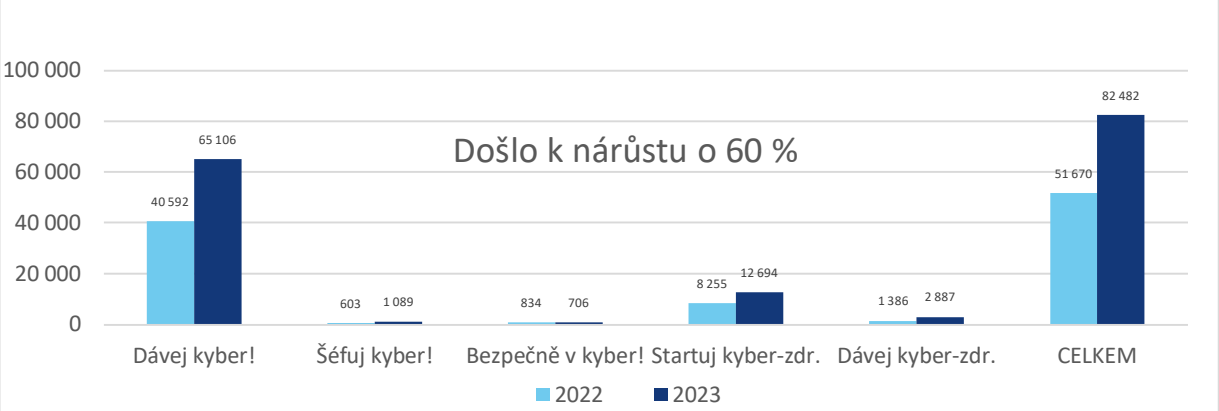
NÚKIB začal v roce 2023 řešit agendu spojenou s příslušnými orgány pro GOVSATCOM a bezpečnou konektivitu (Competent GOVSATCOM Authority a Competent Secure Connectivity Authority). NÚKIB bude podobně jako u služby PRS zajišťovat činnost příslušných orgánů.

## 3.6 Vzdělávání a osvěta

### Vzdělávání

Hlavním nástrojem vzdělávání veřejnosti v oblasti kybernetické bezpečnosti byly stejně jako v předchozích letech online e-learningové vzdělávací kurzy. V roce 2023 došlo k výraznému nárůstu uživatelů kurzů vytvořených NÚKIB na provozovaném portálu osveta.nukib.gov.cz.

**Přehled počtu absolvovaných online kurzů**




Mezi uživatele kurzů NÚKIB patří veřejné instituce, neziskové organizace, soukromé firmy a jednotliví občané České republiky. Pozitivním trendem pro návratnost investice NÚKIB do online e-learningové platformy je trvale rostoucí počet organizací veřejné správy, které prostřednictvím online kurzů NÚKIB zajišťují zvyšování povědomí svých zaměstnanců, a zároveň snižování veřejných výdajů na zajišťování vzdělávání v oblasti kybernetické bezpečnosti.

Všechny kurzy a ostatní online aktivity NÚKIB byly průběžně a podle potřeby vylepšovány a aktualizovány.

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

V rámci rozšíření spolupráce se středními školami zajišťujícími přípravu budoucích odborníků kybernetické bezpečnosti byla založena platforma spolupráce ředitelů škol a NÚKIB.

NÚKIB pokračoval v rozšiřování svých aktivit i do oblasti akreditací vzdělávacích programů a nově má zastoupení v akreditační komisi pro vyšší odborné vzdělávání. NÚKIB se stal k 1. dubnu 2023 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 souladu s novelou zákona č. 179/2006 Sb., o ověřování a uznávání výsledků dalšího vzdělávání a o změně některých zákonů (zákon o uznávání výsledků dalšího vzdělávání), ve znění pozdějších předpisů. NÚKIB se tak nově podílel na tvorbě standardů profesních kvalifikací a zároveň bude udělovat autorizace subjektům, jež budou způsobilé tyto zkoušky provádět. V rámci této činnosti připravil návrhy šesti profesních profilů (manažer/manažerka, architekt/architektka, analytik/analytička, auditor/auditorka, technik/technička kybernetické bezpečnosti a pracovník/pracovnice dohledového centra).

### Osvěta

Osvěta a prevence v oblasti kybernetické bezpečnosti byly tradičně důležitými tématy při zajišťování kybernetické bezpečnosti a zvyšování odolnosti společnosti v souladu s cíli Národní strategie kybernetické bezpečnosti 2021–2025.

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 (tj. říjen) nebo se ve spolupráci s MV a jinými organizacemi zúčastnili Dne bezpečnějšího internetu.

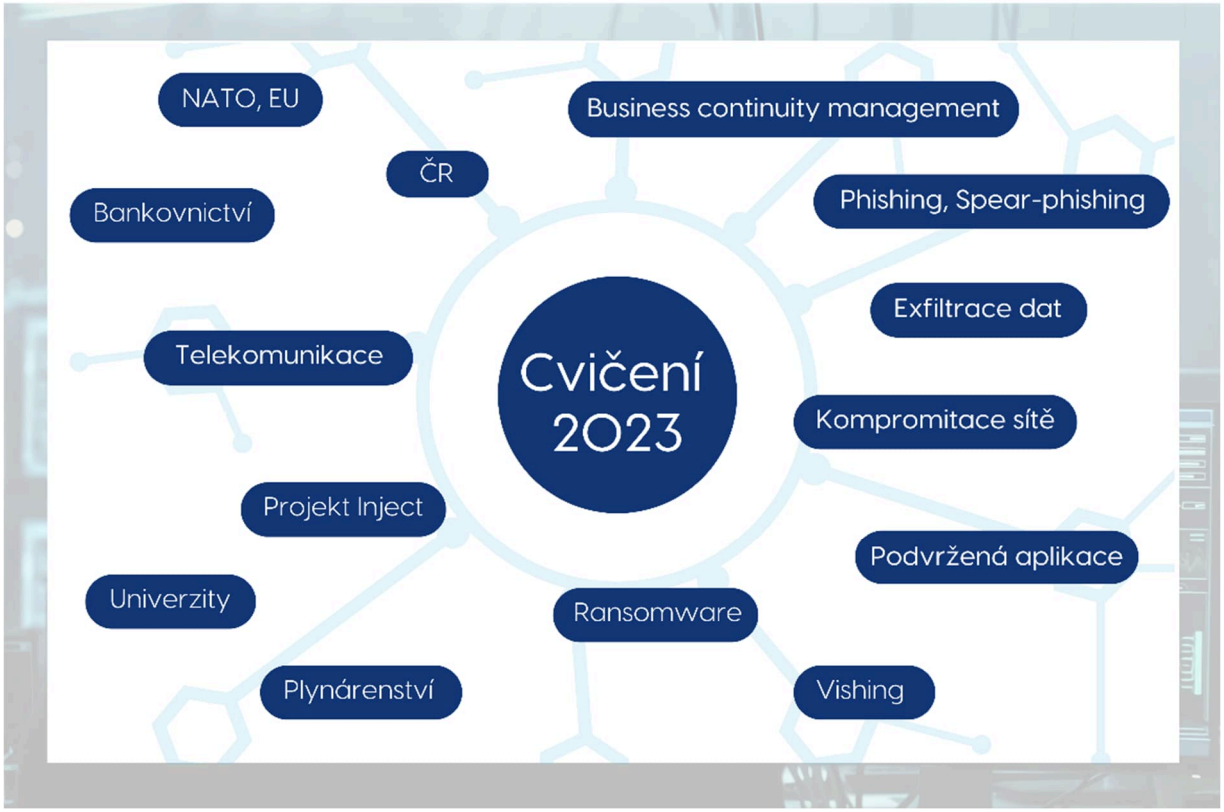
Proběhlo několik vlastních minikampaní na sociálních médiích NÚKIB (Ženy v ICT, Den hesla, Výzva pro Den dětí). NÚKIB se zapojil do aktivit partnerů, jako jsou Národního finále soutěže v kybernetické bezpečnosti a Kybercena roku, které pořádalo Centrum kybernetické bezpečnosti, z. ú., či Týden pro Digitální Česko pořádaný místopředsedou vlády pro digitalizaci, a také se podílel na přípravě a propagaci velmi úspěšného projektu České bankovní asociace Kybertest.

Byly rozvíjeny aktivity směrem k budoucím studentům kybernetické bezpečnosti. V rámci veletrhu Gaudeamus a ve spolupráci s vysokými školami NÚKIB zajišťoval zvyšování počtu potenciálních studentů a studentek oborů s uplatněním v oblasti kybernetické bezpečnosti.

Pro zájemce o působení v oboru kybernetické bezpečnosti NÚKIB připravil osvětový projekt NejsmeJenIT, který má za cíl zvýšit informovanost zejména studentů vysokých škol o možném uplatnění jak v technických, tak i netechnických oblastech kybernetické bezpečnosti.

## 3.7 Cvičení

### Cvičení kybernetické bezpečnosti



**Locked Shields 2023**

Ve dnech 18.–21. dubna 2023 se Česká republika zúčastnila dalšího ročníku největšího mezinárodního cvičení kybernetické bezpečnosti – Locked Shields. Toto hybridní cvičení kombinující prvky technických a netechnických aspektů kybernetické bezpečnosti je pořádáno NATO Cooperative Cyber Defence Centre of Excellence (dále jen „NATO CCD COE“) a na jeho přípravě se podílí přední firmy z technologického průmyslu, zástupci akademického sektoru a řada státních institucí. Cvičící týmy jsou ve většině případů složeny z členských či spolupracujících států NATO, popřípadě je tvoří vybrané mezinárodní instituce. Cílem je zejména prohlubování spolupráce mezi všemi zúčastněnými subjekty.


Česká republika pro rok 2023 zvolila nový princip složení Blue Team. Ten byl tvořen zaměstnanci NÚKIB a partnerských organizací s cílem reflektovat řešení potenciální krizové situace v reálném světě. Přestože byla zhruba polovina týmu tvořena nováčky, obsadil tým 8. místo z 24 účastníků, což lze považovat za velmi dobrý výsledek.

**NATO Cyber Coalition**

Dalším cvičením kybernetické bezpečnosti, na kterém zaměstnanci NÚKIB participovali jak při přípravě, tak v roli cvičících je NATO Cyber Coalition. Na úrovni České republiky NÚKIB koordinuje cvičení za civilní část a Velitelství informačních a 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.

**TELCO23**

NÚKIB dále připravil netechnické table-top sektorové cvičení pro vybrané zástupce telekomunikačního sektoru České republiky (Vodafone, $O_2$, T-Mobile a CETIN), které se uskutečnilo 18. října 2023 v prostorách MZV v Praze. Hlavními cíli bylo připravit účastníky cvičení na možnou krizovou situaci v oblasti kybernetické bezpečnosti, umožnit zúčastněným subjektům, aby si ověřily vhodnost, funkčnost a úplnost svých nastavených procesů v oblasti kybernetické bezpečnosti, pomoci cvičícím identifikovat možné nedostatky a slabá místa, poukázat na komplexnost řešení kybernetických incidentů a získat hlubší porozumění ekonomickému, právnímu, mediálnímu či politickému kontextu krizové situace odehrávající se v kyberprostoru nebo z něj pocházející. Cvičení se zúčastnili také zástupci relevantních státních organizací (NÚKIB, MZV, MPO, ČTÚ, MV, Policie České republiky, BIS a VZ), kteří společně představovali stát a jeho reakce v nastolených krizových situacích.

**Projekt Inject**

Na konci roku 2023 proběhlo první ze série cvičení v rámci projektu Inject, který má za cíl vytvoření open source platformy pro přípravu, exekuci a evaluaci netechnických table-top

cvičení kybernetické bezpečnosti. Řešitelem je Fakulta informatiky Masarykovy univerzity v Brně. Jednalo se o interní cvičení NÚKIB a mělo za cíl ověřit stávající fungování platformy.

**Ostatní cvičení**

V srpnu 2023 proběhlo pravidelné komunikační cvičení Comm Czech 2023, jehož cílem bylo ověřit dosažitelnost určených kontaktních osob subjektů regulovaných podle ZKB.

V září 2023 se uskutečnilo netechnické table-top cvičení kybernetické bezpečnosti pro zástupce středního a vyššího managementu Komerční banky, a. s. Scénář představil kybernetický útok s velmi závažným dopadem na fungování banky, a bylo tak nutné reagovat s využitím krizových a business continuity plánů.

NÚKIB dále připravil cvičení pro studenty předmětu kybernetická bezpečnost, který je vyučován v rámci navazujícího magisterského programu bezpečnostní a strategická studia na Fakultě sociálních studií Masarykovy univerzity.

V rámci workshopového dne každoročně pořádané konference CyberCon byla již tradičně jednou z nabízených aktivit ukázka table-top cvičení kybernetické bezpečnosti.

V roce 2023 se cvičení, která NÚKIB pořádal nebo na jejichž přípravě se podílel, účastnilo celkem **1 645** cvičících

V roce 2023 NÚKIB pořádal, či se podílel na přípravě, celkem **12** cvičení kybernetické bezpečnosti

## 3.8 Vědecká činnost, výzkum, vývoj a inovace

V roce 2023 NÚKIB zahájil realizaci dvou 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 (dále jen „ECCC") pro kybernetickou bezpečnost a síť národních koordinačních center. Na národní úrovni mají tato centra sloužit jako kontaktní bod pro Komunitu kompetencí pro kybernetickou bezpečnost a jejich úkolem je podporovat zapojování relevantních subjektů do projektů v oblasti kybernetické bezpečnosti financovaných ze zdrojů EU a poskytovat finanční podporu třetím stranám. Za tímto účelem NÚKIB zřídil webovou stránku nkc.nukib.gov.cz, kde se zájemci mohou dozvědět bližší informace o činnosti ECCC a Národního koordinačního centra. Druhý projekt je zaměřen na podporu implementace evropského rámce certifikací kybernetické bezpečnosti. Prostřednictvím tohoto projektu bude NÚKIB pomocí grantů podporovat vznik certifikačních laboratoří a instituce, které se rozhodnou certifikovat své produkty či služby dle nařízení Evropského parlamentu a Rady

(EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“).

NÚKIB dále zorganizoval dvě expertní jednání Platformy výzkumu a vývoje v kybernetické a informační bezpečnosti. Platforma sdružuje instituce veřejného, akademického a soukromého sektoru a jejím cílem je informovat účastníky o možnostech získání veřejné podpory na výzkumných projektech a zároveň podpořit snahy o užší spolupráci mezi uvedenými sektory.

Z pozice aplikačního garanta NÚKIB podpořil několik projektů financovaných z programů bezpečnostního výzkumu MV či Technologické agentury České republiky. Smyslem této podpory je přispět k implementaci výsledků výzkumu a vývoje v bezpečnostní praxi. Podpořené projekty se zaměřovaly například na využití umělé inteligence v oblasti penetračního testování či na pokročilé nástroje monitorování síťového provozu.

V součinnosti se zastupitelskými úřady v zahraniční realizoval NÚKIB tři výzkumné mise s cílem podpořit mezinárodní výzkumnou spolupráci. Zástupci akademického a veřejného sektoru se zúčastnili expertní mise pro oblast bezpečnosti optických vláken v Německu, následně pak česko-bavorského networkingového semináře na téma implementace evropské směrnice NIS2. Třetí mise se uskutečnila v Singapuru se zaměřením na detekci malware. Tyto aktivity byly realizovány prostřednictvím projektů ekonomické a vědecké diplomacie (PROPED), které jsou v gesci MZV.

## 3.9 Legislativa a vládní agenda

V roce 2023 NÚKIB v souladu s Plánem legislativních prací vlády na rok 2023 připravil návrh zákona o kybernetické bezpečnosti, jehož cílem bylo zpracovat a předložit vládě jednak návrh zákona, kterým se mění ZKB, a jednak návrh zákona o posuzování bezpečnostní spolehlivosti dodavatelů informačních a komunikačních technologií do strategicky významné infrastruktury České republiky. Výše uvedené návrhy byly do Plánu legislativních prací vlády na rok 2023 zařazeny na základě potřeby transpozice směrnice Evropského parlamentu a Rady 2022/2555 ze dne 14. prosince 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“) do českého právního řádu a za účelem splnění úkolu obsaženém v usnesení BRS ze dne 21. června 2022 č. 41. Za účelem splnění obou těchto požadavků byl ve výsledku připraven jeden návrh zákona řešící obě tyto problematiky – návrh nového zákona o kybernetické bezpečnosti.

Spolu s návrhem zákona byly rovněž připravovány i prováděcí právní předpisy, které byly ve formě pokročile zpracovaných tezí součástí návrhu zákona.

Spolu s návrhem nového zákona o kybernetické bezpečnosti připravil NÚKIB také návrh zákona, kterým se mění některé zákony v souvislosti s přijetím nového zákona o kybernetické bezpečnosti. Vzhledem ke změnám, které nastanou s účinností návrhu nového zákona o kybernetické bezpečnosti, je třeba změnit ustanovení účinných právních předpisů v České republice, které obsahově navazují na ZKB, a zajistit tím zejména jejich řádnou interpretaci

a aplikaci. Návrh obou těchto předpisů prošel v roce 2023 meziresortním připomínkovým řízením a v roce 2024 se bude dále pokračovat v legislativním procesu, a to včetně samostatných meziresortních připomínkových řízení pro prováděcí právní předpisy.

Dále byla v roce 2023 publikována ve Sbírce zákonů České republiky vyhláška č. 190/2023 Sb., o bezpečnostních pravidlech pro orgány veřejné moci využívající služby poskytovatelů cloud computingu, která nabyla účinnosti dne 1. 7. 2023.

V roce 2023 také probíhal legislativní proces novely ZoOUI, na kterém se NÚKIB podílel. Legislativní proces bude pokračovat v roce 2024. V návaznosti na tuto novelu NÚKIB započal přípravy prováděcích právních předpisů k výše uvedenému zákonu, kdy vzhledem ke změnám, které novela přinese, bude nezbytné již účinné prováděcí právní předpisy podrobit revizi.

Vedle legislativních prací na výše uvedených právních předpisech NÚKIB v roce 2023 posoudil v meziresortním připomínkovém řízení 170 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 (dále jen „VKB“), aktualizací výkaznictví souladu právních předpisů v gesci NÚKIB s právními předpisy EU a řízením gescí NÚKIB k dokumentům EU legislativní i nelegislativní povahy.

V rámci výše uvedeného NÚKIB, jenž zajišťuje činnost sekretariátu VKB, připravil ve spolupráci se sekretariátem BRS návrh novely Statutu a Jednacího řádu Výboru. Návrhy obou dokumentů byly BRS a vládou schváleny a zveřejněny na webových stránkách vlády.

## 3.10 Komunikace

Komunikace NÚKIB s veřejností se rozvíjela jak pomocí webových stránek a profilů NÚKIB na sociálních sítích, tak prostřednictvím interakce s médii a účastí na veřejných akcích. Jedním z ukazatelů aktivity je rostoucí počet sledujících na sociálních sítích.

Hlavním komunikovaným tématem v průběhu celého roku 2023 byl návrh nového zákona o kybernetické bezpečnosti. Významným tématem byla také osvěta v oblasti kybernetické bezpečnosti. Vhodně zvolenými komunikačními kanály byly propagovány e-learningové kurzy, což přispělo k výraznému nárůstu počtu návštěvníků webových stránek a absolventů kurzů.

NÚKIB zveřejňoval informace o akcích, které organizoval nebo se jich účastnil, o významných zahraničních cestách zaměstnanců NÚKIB, jejich činnostech, o kybernetických incidentech, zranitelnostech a novinkách z oblasti výzkumu a vývoje.

## 3.11 Spolupráce, mezinárodní spolupráce

Vývoj v oblasti kybernetické bezpečnosti v České republice je do značné míry svázaný s vývojem v zahraničí a rozhodnutími přijímanými nejen na úrovni EU, ale i v dalších mezinárodních organizacích a integračních uskupeních, v jejichž rámci NÚKIB zastupuje zájmy České republiky v oblasti kybernetické bezpečnosti a diplomacie. Významný podíl na rozvoji mezinárodní spolupráce má činnost kyberatašé, pracovníků NÚKIB, kteří působí při EU, NATO a bilaterálně v USA, Izraeli a od roku 2023 nově i v Austrálii.

**Evropská unie**

V roce 2023 NÚKIB navázal na úspěšné české předsednictví v Radě EU (dále jen „CZ PRES“) a soustředil se zejména na činnost Horizontální pracovní skupiny pro kybernetické otázky v Radě EU. V rámci legislativního vývoje bylo v průběhu roku finalizováno a přijato nařízení, kterým se stanoví opatření k zajištění vysoké společné úrovně kybernetické bezpečnosti v orgánech, institucích a jiných subjektech Unie a k jehož vyjednání NÚKIB během CZ PRES velkou měrou přispěl. Na práci během CZ PRES bylo navázáno také v návrhu Aktu o kybernetické odolnosti, jenž zavádí povinné požadavky na kybernetickou bezpečnost hardwarových a softwarových produktů a jehož vyjednávání bylo uzavřeno přijetím politické dohody na sklonku roku 2023. Taktéž u dvou nových legislativních návrhů Aktu o kybernetické solidaritě a Aktu o kybernetické bezpečnosti bylo vyjednávání zahájeno a na konci roku 2023 nalezena shoda mezi členskými státy tak, aby mohla být zahájena meziinstitucionální vyjednávání mezi Radou, Evropským parlamentem a Evropskou komisí. Došlo také k revizi tzv. Kybernetického diplomatického toolboxu, který je sadou diplomatických nástrojů pro prevenci kybernetické škodlivé aktivity či pro reakci na ni. Toolbox byl aktualizován a zejména rozšířen o další diplomatická opatření i okruh subjektů, vůči kterým je možné jej uplatnit. Detailněji je potom rozpracován ve své neveřejné části.

Mimo půdu Rady byl NÚKIB zapojen především do činnosti Evropské sítě styčných organizací pro řešení kybernetických krizí (EU-CyCLONe), jejíž existence byla formalizována účinností směrnice NIS2 začátkem roku 2023, a dále pak také do aktivit Sítě CSIRT[1]. NÚKIB byl aktivní a prohluboval spolupráci i v rámci Skupiny pro spolupráci, zřízené směrnicí NIS, zaměřující se na metodickou podporu při implementaci požadavků směrnice NIS2. Mimo to probíhala práce na dalším rozvinutí tématu bezpečnosti dodavatelského řetězce, a to v souladu se závěry Rady k bezpečnosti dodavatelských řetězců ICT přijatými během CZ PRES, které zdůrazňují potřebu přijetí souboru obecných opatření ke snížení kritických rizik dodavatelských řetězců ICT. Kromě toho se NÚKIB na unijní úrovni v rozsahu své působnosti věnoval také dalším tématům a jejich kyberbezpečnostním aspektům, jako jsou umělá inteligence, kvantové technologie či telekomunikační sítě a podmořské kabely.

NÚKIB také nadále zastával roli kontaktního místa pro unijní agenturu pro kybernetickou bezpečnost ENISA a v roce 2023 z pozice národního koordinátora poskytl agentuře ENISA podporu nezbytnou pro úspěšnou realizaci tzv. projektu podpůrných služeb (ENISA Support Action) ke zvýšení kybernetické bezpečnosti regulovaných subjektů na území České republiky.

**Severoatlantická aliance**

NÚKIB se podílel na plnění aliančních závazků v oblasti kybernetické bezpečnosti a obrany prostřednictvím svého kyberatašé ve Výboru pro kybernetickou obranu NATO. V roce 2023 se NÚKIB spolu s národními partnery zapojil do nové iniciativy NATO, jež poskytuje virtuální podporu Spojenců v reakci na kybernetické incidenty (VCISC), což představuje pro Českou republiku nové možnosti efektivních reakcí na hrozby. Mimo to NÚKIB nadále pokračoval v úzké spolupráci s NATO CCD COE skrze svého vyslaného experta.

[1] Síť CSIRT se skládá z týmů CSIRT jmenovaných členskými státy EU a skupiny CERT-EU. Účelem je vyměňovat si informace a budovat důvěru na úrovni EU, provádět koordinované reakce na incidenty, spolupracovat a vyměňovat si osvědčené postupy v reakci na incidenty.

**Organizace spojených národů**

NÚKIB se společně s MZV aktivně podílel na činnosti nejvýznamnější platformy dedikované kybernetické bezpečnosti, tzv. Open-Ended Working Group. Skupina se věnuje otázkám nových hrozeb, uplatnitelnosti mezinárodního práva, normám, pravidlům, principům, opatřením pro zvyšování důvěry mezi státy v kyberprostoru a budováním kapacit v oblasti kybernetické bezpečnosti.

NÚKIB taktéž spolupracoval s Ministerstvem spravedlnosti na vyjednávání nové úmluvy OSN proti kyberkriminalitě na fóru ad hoc výboru OSN, přičemž toto vyjednávání bude pokračovat i v roce 2024.

**Organizace pro bezpečnost a spolupráci v Evropě**

Ve spolupráci s MZV se NÚKIB účastnil zasedání skupiny Informal Working Group, která se soustředí zejména na implementaci přijatých opatření pro budování důvěry mezi státy v oblasti kybernetické bezpečnosti.

**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.

**Mezinárodní telekomunikační unie**

NÚKIB v rámci činnosti jednotlivých pracovních skupin unie sledoval a analyzoval dění zejména v oblasti standardizace telekomunikačních technologií, kybernetické bezpečnosti a umělé inteligence (dále jen „AI“).

**Bilaterální spolupráce**

**Austrálie a Indo-pacifik**

V roce 2023 byl v Austrálii zřízen post kyberatašé pro region Indo-Pacifiku, jehož cílem je podpora a prohloubení vzájemné spolupráce se zeměmi tohoto regionu.

Tato spolupráce zahrnuje témata z oblastí ochrany kritické informační infrastruktury, výzkumu, inovací, digitalizace či aktivit nedemokratických států v kyberprostoru. Dále identifikaci možností pro technickou spolupráci nebo sdílení a sledování legislativního a strategického vývoje v oblasti kybernetické bezpečnosti.

Během roku 2023 se podařilo zejména v Austrálii navázat kontakt se všemi hlavními vládními insitucemi v oblasti kybernetické bezpečnosti, a došlo k propojení s hlavními velvyslanectvími regionu (Austrálie, Indie, Japonsko, Korejská republika, Nový Zéland, Singapur), se kterými byl konzultován plán aktivit na následující rok. Největší akcí v regionu, které se zúčastnili zástupci NÚKIB, byl pak Singapore International Cyber Week, na němž Česká republika pořádala i regionální seminář na téma ochrany kritické infrastruktury a implementaci norem zodpovědného chování státu v kyberprostoru.

**USA a Kanada**

Ve spolupráci s USA řešil NÚKIB relevantní kybernetické hrozby a v rámci uzavřených bilaterálních briefingů sdílel zkušenosti např. s transpozicí směrnice NIS2 nebo přístupy ke kybernetickým cvičením. Mezi důležitými událostmi lze zmínit strategický dialog mezi Českou republikou a USA, na němž byla vůbec poprvé v historii za účasti zástupců NÚKIB a MZV diskutována spolupráce v oblasti kybernetické bezpečnosti. Zástupci NÚKIB se tradičně účastnili International Cyber Security Forum pro vybrané mezinárodní partnery a již třetího ročníku International Counter Ransomware Summit ve Washingtonu, kde Česká republika prezentovala poslední vývoj a opatření v oblasti ransomware. Zároveň se Česká republika připojila ke společnému prohlášení proti placení výkupného za ransomware, které bylo hlavním výstupem letošního summitu. Zástupci NÚKIB návštívili NIST Cyber Security Centre of Excellence za účelem rozvoje další spolupráce v oblasti kvantových technologií a pod hlavičkou Úřadu vlády České republiky se zapojili do mise v USA ke kvantovým technologiím, v jehož rámci jednali o dalším rozvoji v oblasti přechodu na postkvantovou kryptografii.

V rámci spolupráce v oblasti cvičení navštívili NÚKIB experti z USA a Kanady, zástupci kanadského dopravního sektoru nebo poradci členů amerického Kongresu, pro které NÚKIB připravil briefing k aktuálním kybernetickým hrozbám.

NÚKIB zveřejnil společné analýzy s americkými úřady (FBI nebo NSA) k tzv. Security by Design přístupu a k bezpečnosti AI. NÚKIB se rovněž zapojil do dvou misí na podporu ekonomické diplomacie, které přispěly k navázání kontaktů mezi českými soukromými institucemi a výzkumnými institucemi v USA a Kanadě v oblasti kybernetické bezpečnosti. Pokračovala také dlouhodobá spolupráce mezi Českou republikou a USA v oblasti bezpečnosti dodavatelského řetězce a budování kapacit ve třetích zemích v rámci tzv. Commercial Law Development Programu.

**Izrael**

Pokračovalo prohlubování spolupráce s partnerskými úřady, které mají v gesci kybernetickou bezpečnost, zejména s Israel National Cyber Directorate, se kterým probíhá strukturovaný dialog v oblasti kybernetické bezpečnosti (právní rámec, regulace, cvičení, strategie, vzdělávání, výměna operačních informací).

Dále probíhala spolupráce s Water Authority, Ministry of Finance, National Digital Agency, Ministry of Health, Ministry of Energy, Ministry of Environmental Protection a Ministry of Defence zejména v oblasti sdílení informací a dobré praxe. V červenci 2023 proběhlo v Praze jednání se zástupcem Water Authority na téma zajištění kybernetické bezpečnosti v sektoru vodního hospodářství.

Byla realizována bilaterální jednání se zástupci INCD a také akademické sféry (Tel Aviv University a Haifa University). V rámci programu TAIEX se experti zúčastnili školení izraelských partnerů na téma směrnice NIS a NIS2.

Účast na konferenci Cyber Week v Izraeli byla využita k bilaterálním jednáním jak s izraelskými, tak zahraničními partery (Kanada, Singapur, Německo, USA).

**Prague Cyber Security Meeting**

V polovině roku 2023 proběhla virtuální událost Prague Cyber Security Meeting, která se věnovala důležitosti a hrozbám AI a budování partnerství mezi veřejným a soukromým sektorem.

### Rozvojová spolupráce

NÚKIB uzavřel smlouvu s e-Government Agency, se kterou bude spolupracovat na kyberbezpečnostních projektech pro oblast západního Balkánu do roku 2026. V rámci expertní mise pod záštitou TAIEX byly vládním CERT poskytnuty 4 workshopy zaměstnancům ministerstva obrany Bosny a Hercegoviny za účelem zvýšení jejich kapacity v oblasti reakce na kybernetické bezpečnostní incidenty. Ve spolupráci s NATO se NÚKIB podílel na projektu v Jordánsku, který byl zaměřen na agendu vládního CERT a sdílení informací. V neposlední řadě NÚKIB přijal příchozí mise z Albánie, Kolumbie, Indonésie a Senegalu za účelem sdílení právního rámce kybernetické bezpečnosti v České republice, strategického směřování v kybernetické bezpečnosti a bezpečnosti dodavatelského řetězce.

## 3.12 Ekonomické zabezpečení

### Příjmy

Celkové příjmy kapitoly za rok 2023 byly ve výši 18 479 981,21 Kč. Příjmy tvořily nedaňové příjmy, kapitálové příjmy a přijaté transfery. Část nedaňových příjmů ve výši 300 000 Kč byla za příjem pokut ze správního řízení dle ZoOUI. Další položkou byly neplánované přijaté nekapitálové příspěvky a náhrady v objemu 585 330,23 Kč. V kapitálových příjmech se jednalo o příjem za prodej nepotřebného majetku ve výši 14 100 Kč. Přijaté transfery pak tvoří prostředky přijaté od Evropské unie v objemu 17 575 396,72 Kč. Jedná se jmenovitě o neinvestiční přijaté transfery na projekt TEST-CERT-CZ ve výši 14 311 283,82 Kč a projekt NCC-CZ ve výši 3 264 112,90 Kč. Příjem rozpočtovaný v rámci IROP 2021+ na investiční akci 378V023003012: Realizace stavby – Černá Pole nebyl naplněn.

**Přehled plnění rozpočtu příjmů v roce 2023 (vyjádření v tis. Kč)**

| | 2022 | 2023 | | | Plnění k rozpočtu po změnách (%) | Rozdíl skutečností |
|---|---|---|---|---|---|---|
| | Skutečnost | Schválený rozpočet | Rozpočet po změnách | Skutečnost | | |
| Příjmy celkem | 318,47 | 4 549,81 | 4 549,81 | 18 479,98 | 406,17 | 18 161,51 |
| **Podseskupení** | | | | | | |
| 211 – Příjem z vlastní činnosti | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 |
| 221 – Přijaté sankční platby | 29,00 | 400,00 | 400,00 | 300,00 | 75,00 | 271,00 |
| 232 – Ostatní nedaňové příjmy | 266,50 | 0,00 | 0,00 | 585,33 | 0,00 | 318,83 |
| 413 – Neinvestiční převody z vlastních fondů a ve vztahu k útvarům bez právní osobnosti | 22,97 | 0,00 | 0,00 | 5,15 | 0,00 | -17,81 |
| 311 – Příjem z prodeje dlouhodobého majetku | 0,00 | 0,00 | 0,00 | 14,10 | 0,00 | 14,10 |
| 415 – Neinvestiční přijaté transfery ze zahraničí | 0,00 | 0,00 | 0,00 | 17 575,40 | 0,00 | 17 575,40 |
| 421 – Investiční přijaté transfery od rozpočtů ústřední úrovně | 0,00 | 4 149,81 | 4 149,81 | 0,00 | 0,00 | 0,00 |

### Výdaje

Schválený rozpočet celkových výdajů NÚKIB byl v roce 2023 ve výši 616 610 013 Kč.

Během roku 2023 byl schválený rozpočet upravován rozpočtovými opatřeními MF na objem 621 099 995 Kč. Dále byl rozpočet snížen vázáním prostředků na platy a příslušenství za neobsazená pracovní místa v objemu 6 025 963 Kč, a to na částku 615 074 032 Kč. K 31. prosinci 2023 bylo z upraveného rozpočtu celkových výdajů vyčerpáno 563 784 022,18 Kč, tedy v relativním vyjádření 90,8 %. V průběhu roku 2023 bylo provedeno

12 rozpočtových opatření MF a 4 rozpočtová opatření v rámci vázání prostředků státního rozpočtu za neobsazená pracovní místa.

Konečný rozpočet celkových výdajů kapitoly za rok 2023, tedy rozpočet včetně zapojených Nároků z nespotřebovaných výdajů (dále jen „NNV“) ve výši 50 624 065,68 Kč, byl v objemu 683 273 494,40 Kč. Čerpání konečného rozpočtu bylo v relativním vyjádření na 89,4 %, v absolutním vyjádření ve výši 610 517 028,08 Kč.

**Základní přehled plnění rozpočtu výdajů v roce 2023 (vyjádření v tis. Kč)**

| | 2022 | 2023 | | | | Plnění k rozpočtu po změnách (%) | Plnění ke konečnému rozpočtu (%) | Rozdíl skutečností |
|---|---|---|---|---|---|---|---|---|
| | Skutečnost | Schválený rozpočet | Rozpočet po změnách | Konečný rozpočet | Skutečnost | | | |
| Výdaje celkem | 592 817,90 | 616 610,01 | 621 100,00 | 683 273,49 | 610 517,03 | 98,3 | 89,4 | 17 699,13 |
| Běžné výdaje | 441 481,74 | 498 073,91 | 502 563,89 | 541 553,41 | 507 899,76 | 101,1 | 93,8 | 66 418,03 |
| z toho platy včetně příslušenství | 267 024,24 | 316 431,90 | 317 479,05 | 315 842,76 | 310 895,54 | 97,9 | 98,4 | 43 871,29 |
| z toho běžné výdaje bez platů a příslušenství | 174 457,49 | 181 642,00 | 185 084,84 | 225 710,66 | 197 004,23 | 106,4 | 87,3 | 22 546,73 |
| Kapitálové výdaje | 151 336,16 | 118 536,11 | 118 536,11 | 141 720,08 | 102 617,26 | 86,6 | 72,4 | -48 718,89 |

### Výdaje na platy včetně příslušenství

Výdaje na platy, ostatní platby za provedenou práci a příslušenství byly rozpočtovány ve výši 316 431 904 Kč pro 356 pracovních míst.

Vázáním prostředků na platy a příslušenství za neobsazená pracovní místa v objemu 6 025 963 Kč byl rozpočet snížen na částku 310 405 941 Kč. Konečný rozpočet výdajů na platy, ostatní platby za provedenou práci a příslušenství ve výši 315 842 756,34 Kč byl čerpán v objemu 310 895 535,72 Kč, tedy v relativním vyjádření na 98,4 %.

V období od 1. ledna 2023 do 31. prosince 2023 nastoupilo na NÚKIB 80 nových zaměstnanců a 52 zaměstnanců skončilo pracovní poměr. Průměrný plat k průměrnému ročnímu přepočtenému počtu 329,59 zaměstnanců činil 57 511,00 Kč měsíčně.

### Běžné výdaje

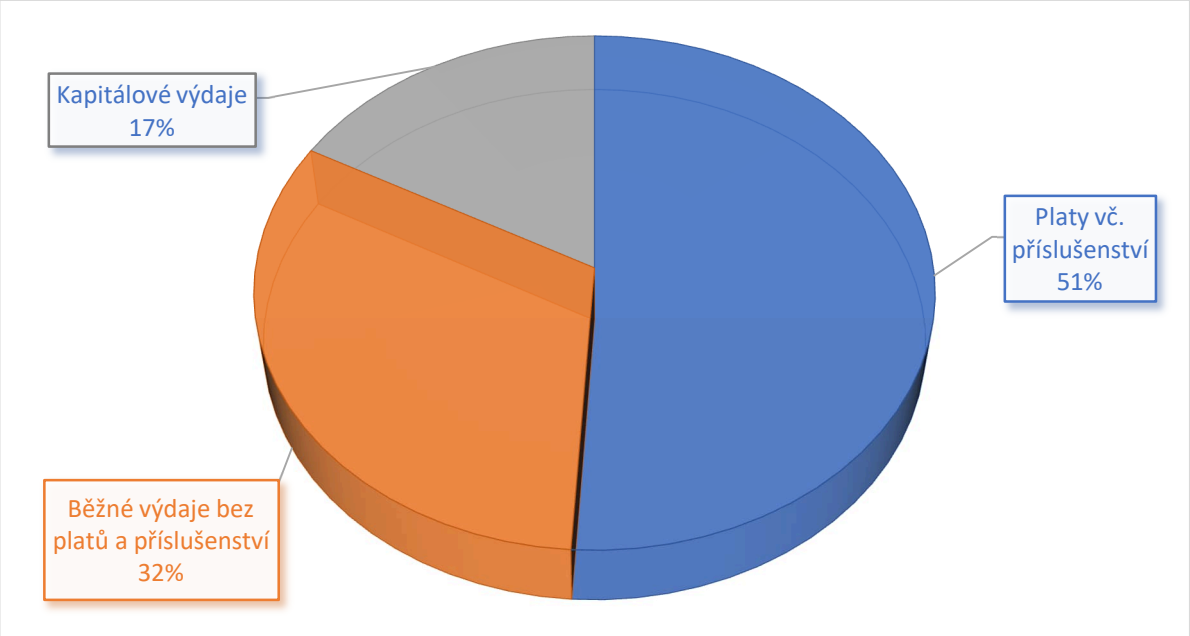
Běžné výdaje (bez výdajů na platy, ostatní platby za provedenou práci a příslušenství) byly rozpočtovány ve výši 181 642 002 Kč. Rozpočtovými opatřeními byly upraveny na 185 084 840 Kč. Zapojením NNV byly upraveny na konečný rozpočet ve výši 225 710 655,80 Kč. Konečný rozpočet běžných výdajů byl čerpán v objemu 197 004 227,50 Kč, v relativním vyjádření na 87,3 %.

### Kapitálové výdaje

Kapitálové výdaje vedené ve Správě majetku ve vlastnictví státu (dále jen „SMVS“) byly rozpočtovány v roce 2023 ve výši 118 536 107 Kč. Zapojením NNV pak byly kapitálové výdaje v roce 2023 upraveny na konečný rozpočet výdajů v SMVS v objemu 141 720 082,26 Kč. Konečný rozpočet kapitálových výdajů byl čerpán v objemu 102 617 264,84 Kč, v relativním vyjádření 72,4 %.

Nejvýznamnější objem finančních prostředků byl vynaložen na subtitul ICT v objemu 45 489 880 Kč. Dále bylo vynaloženo 34 750 270 Kč na nemovitou infrastrukturu NÚKIB a 20 273 690 Kč na projekty v rámci výzkumu a vývoje, tj. kryptografické techniky, měřící techniky nebo nehmotných výsledků, a 2 103 420 Kč na zabezpečovací techniku.

**Podíl jednotlivých složek čerpání na celkových výdajích 2023**

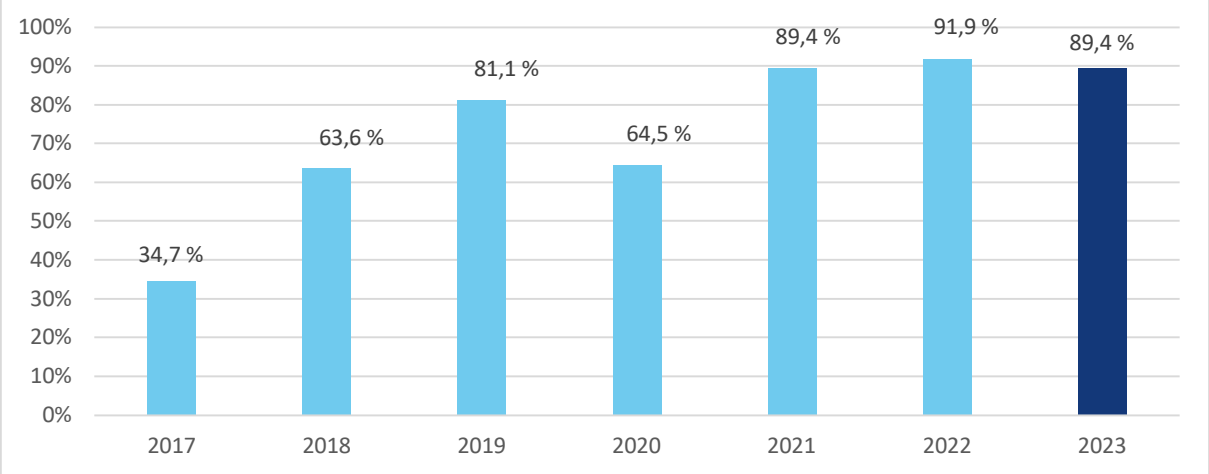



**Evidence nároků z nespotřebovaných výdajů**

Počáteční stav nároků z nespotřebovaných výdajů k 1. lednu 2023 byl ve výši 52 285 250,85 Kč. Celkem byly za rok 2023 vyčerpány z NNV finanční prostředky v objemu 46 733 005,90 Kč. K 31. prosinci 2023 činil zůstatek nároků z nespotřebovaných výdajů 3 891 059,78 Kč. K 1. lednu 2024 činí stav NNV 74 010 611,11 Kč.

Všechny nečerpané NNV plánuje NÚKIB využít v roce 2024, a to včetně účelově určených finančních prostředků nevyčerpaných z roku 2023 na zapojení občanů České republiky do civilních misí EU a dalších mezinárodních vládních organizací a také účelově určených finančních prostředků nevyčerpaných z roku 2023 na navýšení běžných výdajů rozpočtu kapitoly NÚKIB.

**Vývoj čerpání konečného rozpočtu výdajů v letech 2017–2023**



## 3.13 Investice a rozvoj

V roce 2023 pokračoval NÚKIB v přípravě a realizaci celé řadě 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 byla během roku 2023 zpracována projektová dokumentace pro 5. etapu rekonstrukce objektu Cejl, která se týkala přízemních prostor v oblasti dvorního traktu, zejména úprav skladových prostor a vybudování nových kancelářských prostor.

**Objekt Gorkého, Brno**

Na začátku roku 2023 byla dokončena kompletní rekonstrukce dle projektové dokumentace, zohledňující bezpečnostní a technické požadavky zaměstnanců NÚKIB a proběhlo předání stavby. Celkem bylo vybudováno 86 kancelářských míst.

**Administrativní budova NÚKIB, Brno – Černá Pole**

Objekt budovaný v souladu s vládou schválenou Koncepcí rozvoje NÚKIB. Po řadě jednání se podařilo v závěru roku získat pravomocné stavební povolení a zpracovatel dokumentace pokračoval v pracích na dokumentaci pro provedení stavby.

## 3.14 Personální zabezpečení

NÚKIB měl k 31. prosinci 2023 přidělených 356 pracovních míst. Skutečná obsazenost na pracovních místech k výše uvedenému datu byla 352. V souladu s Koncepcí rozvoje NÚKIB došlo od 1. ledna 2023 k navýšení počtu pracovních míst NÚKIB o 25. Do pracovního poměru v období od 1. ledna 2023 do 31. prosince 2023 bylo přijato 80 nových zaměstnanců. Dalších 6 zaměstnanců vykonávalo činnost na základě uzavřených dohod o pracovní činnosti a s 15 osobami byla uzavřena dohoda o provedení práce.

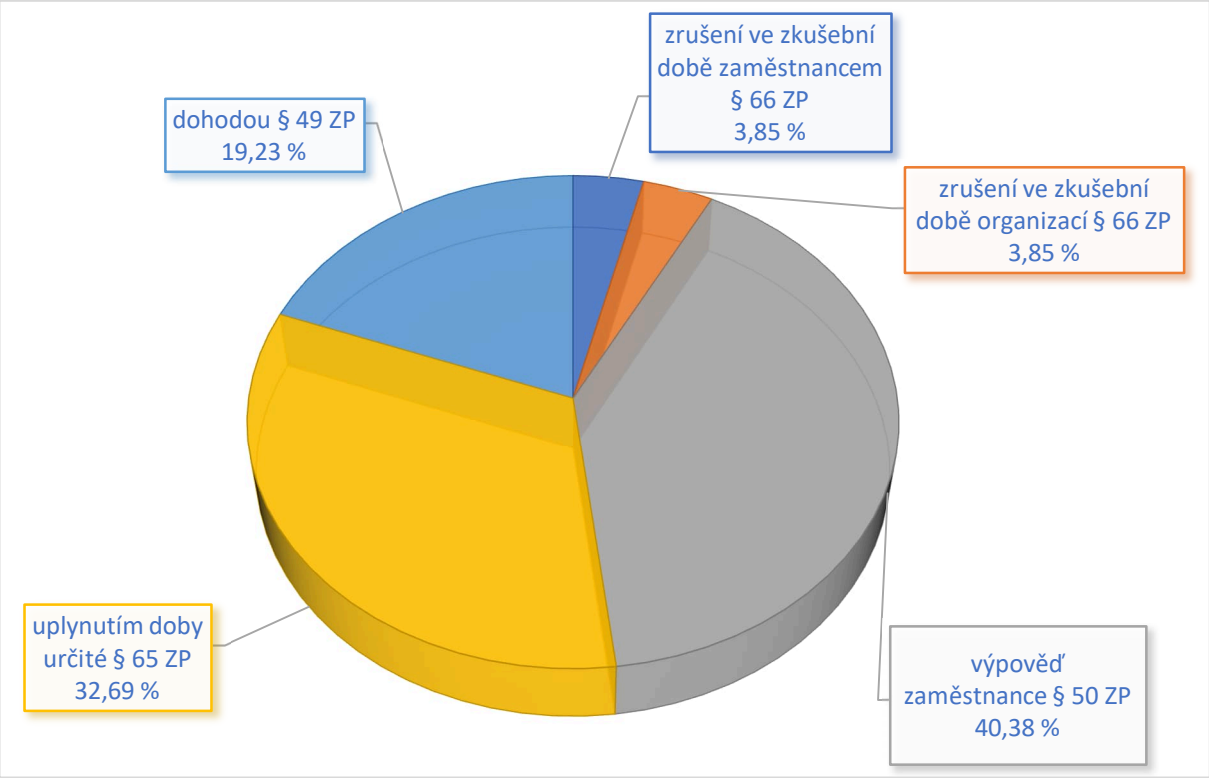
### Základní přehled

| | |
|---|---|
| Evidenční stav zaměstnanců na systemizovaných pracovních místech k 31. 12. ve fyzických počtech | 352 |
| Počet zaměstnanců dočasně mimo systemizovaná pracovní místa (mateřská a rodičovská dovolená, uvolnění k výkonu veřejné funkce) | 16 |
| Ukončení pracovních poměrů v průběhu roku 2023 | 52 |
| Nástupy do pracovního poměru v průběhu roku 2023 | 80 |
| Návraty z mateřské dovolené, z rodičovské dovolené a neplaceného volna v průběhu roku 2023 | 6 |
| Odchody na mateřskou či rodičovskou dovolenou v průběhu roku 2023 | 9 |

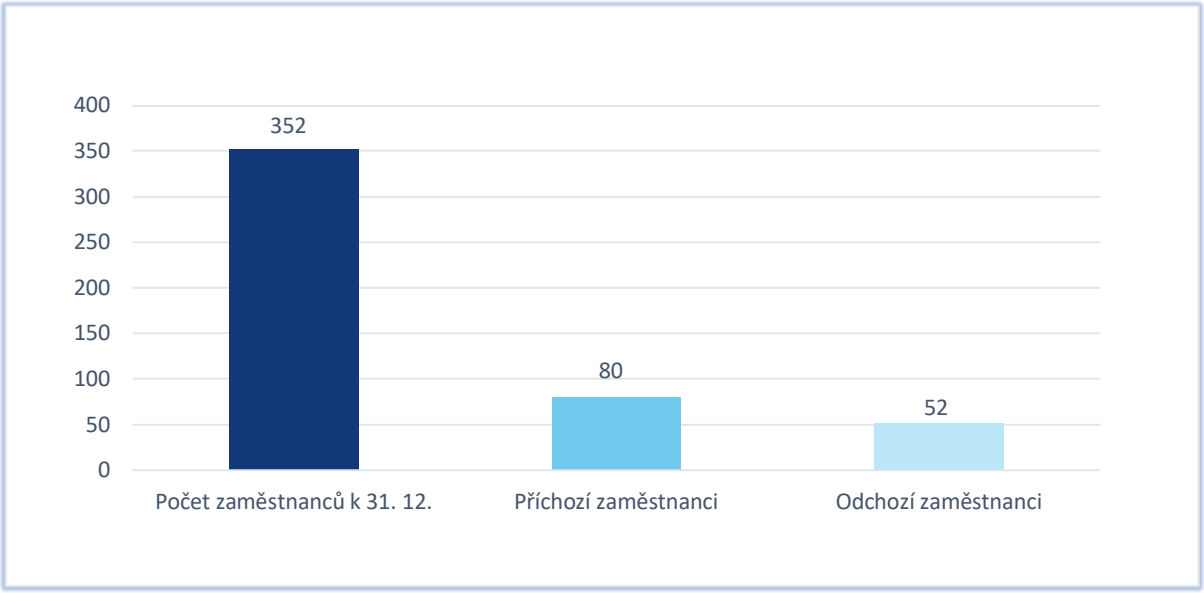
Do konce roku 2023 ukončilo pracovní poměr 52 zaměstnanců, tj. 15,21 % z počtu zaměstnanců evidovaných na systemizovaných pracovních místech. Z tohoto počtu 2 zaměstnanci ukončili pracovní poměr ve zkušební době, se 2 zaměstnanci ukončil ve zkušební době pracovní poměr zaměstnavatel, 17 zaměstnanců ukončilo pracovní poměr

uplynutím doby určité, 21 zaměstnanců výpovědí ze strany zaměstnance a 10 pracovních poměrů bylo ukončeno dohodou na žádost zaměstnance.

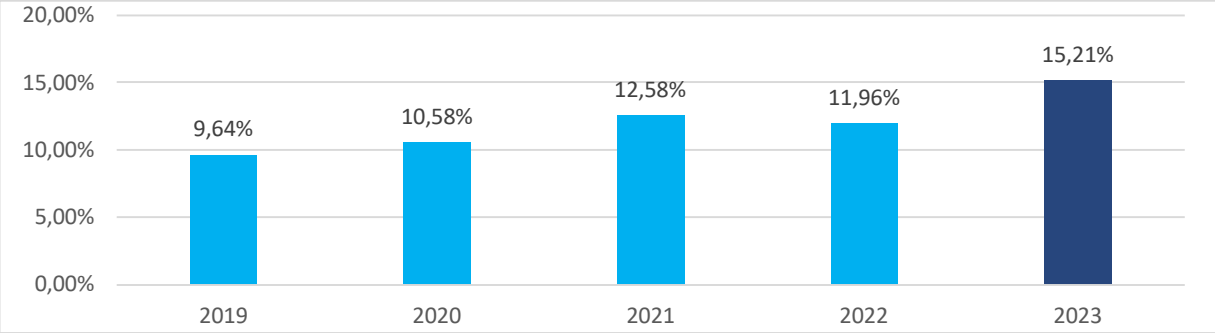
### Způsoby ukončení pracovního poměru




### Nástupy a odchody zaměstnanců v roce 2023



### Fluktuace zaměstnanců NÚKIB v letech 2019–2023




### Věková struktura zaměstnanců k 31. 12. 2023 (včetně zaměstnanců dočasně mimo systemizovaná pracovní místa)

| Věková kategorie | Počet zaměstnanců k 31. 12. 2023 | Podíl zaměstnanců v % | Z toho | |
|---|---|---|---|---|
| | | | muži | ženy |
| méně než 20 let | 0 | 0,00 % | 0 | 0 |
| 20–29 let | 97 | 26,36 % | 57 | 40 |
| 30–39 let | 120 | 32,61 % | 70 | 50 |
| 40–49 let | 79 | 21,47 % | 46 | 33 |
| 50–59 let | 50 | 13,59 % | 31 | 19 |
| 60–65 let | 18 | 4,89 % | 14 | 4 |
| 66 a více let | 4 | 1,09 % | 3 | 1 |
| **Celkem** | 368 | 100,00 % | 221 | 147 |

Průměrný věk zaměstnance činil 38,8 roku.

### Kvalifikační struktura zaměstnanců k 31. 12. 2023

| **Dosažené vzdělání k 31. 12. 2023** (zahrnuti jsou též zaměstnanci dočasně na MD, RD a uvolnění k výkonu veřejné funkce) | Počet zaměstnanců k 31. 12. 2023 | Procentní struktura |
|---|---|---|
| v doktorském studijním programu | 16 | 4,35 % |
| v magisterském studijním programu | 243 | 66,03 % |
| v bakalářském studijním programu | 43 | 11,68 % |
| vyšší odborné vzdělání | 4 | 1,09 % |
| střední vzdělání s maturitní zkouškou | 61 | 16,58 % |
| střední vzdělání s výučním listem | 1 | 0,27 % |
| základní vzdělání | 0 | 0,00 % |
| **Celkem** | 368 | 100 % |

**Vzdělávání a rozvoj zaměstnanců**

V rámci vzdělávání zaměstnanců byla realizována školení individuální i hromadná. U hromadných školení se jednalo o školení vyplývající ze zákona (školení bezpečnosti a ochrany zdraví při práci, požární ochrany, odborné způsobilosti řidičů, GDPR) a školení vyplývající z normativních aktů NÚKIB (administrativní bezpečnost, fyzická a personální bezpečnost, informační bezpečnost, základy kybernetické bezpečnosti).

V návaznosti na identifikaci vzdělávacích potřeb, určení priorit a rozsahu vzdělávání, byla organizována hromadná tematická školení (Soft Skills, smluvní podmínky FIDIC, kurz české interpunkce, specializované bezpečnostní techniky pro nasazení a správu hybridního řešení Exchance Online, zvládání stresu a time management, prezentační dovednosti, ISO/IEC 27001 Lead Auditor, šikana a nevhodné chování na pracovišti) a vzdělávání individuální.

Zaměstnanci se zúčastnili také zahraničních školení SANS, jejichž prostřednictvím získali znalosti a zkušenosti z oblastí širokého spektra technických i netechnických cvičení kybernetické bezpečnosti, vytváření analytických a informačních materiálů pro rozhodující činitele a organizace v české státní správě i v zahraničí.

**Zaměstnávání osob se zdravotním postižením**

V roce 2023 měl NÚKIB naplnit povinný podíl zaměstnávání osob se zdravotním postižením stanovený v zákoně č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů, ve výši 13,19 osoby. Plnění povinného podílu bylo splněno zaměstnáváním osob se zdravotním postižením ve výši 2,71 osoby a odběrem výrobků a služeb, který v přepočtu odpovídá zaměstnání 17,21 osob.

## 3.15 Interní audit a vnitřní kontrola

V průběhu roku byl vykonán mimořádný audit investičních zakázek, následný audit zaměřený na prověření realizace opatření k odstranění nedostatků zjištěných v průběhu auditů realizovaných v předchozích letech (audit spisové služby, pokladny a veřejných zakázek). Taktéž byl realizován audit dodržování zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů. Koncem roku byl zahájen audit fondu kulturních a sociálních potřeb.

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.

V únoru roku 2023 byla MF odeslána zpráva o výsledcích finančních kontrol na NÚKIB za předchozí kalendářní rok.

Ve spolupráci s interním auditem a vedoucími zaměstnanci byla identifikována a vyhodnocena rizika vyskytující se na NÚKIB, která jsou východiskem pro každoroční zpracování mapy rizik.

Koncem roku 2023 byl zpracován Plán interního auditu pro rok 2024 vycházející ze střednědobého plánu interního auditu pro období 2022–2024.

Finanční kontrolu vykonávanou podle zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (dále jen „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 2023 byl zajišťován výkon řídící 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 o finanční kontrole a vyhlášky č. 416/2004 Sb., kterou se provádí 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 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 zkratek

| | |
|---|---|
| AI | Artificial Intelligence (umělá inteligence) |
| BIS | Bezpečnostní informační služba |
| BIVOJ | Bezpečný, inovativní, pro veřejnou správu, odolný, jednotný |
| BRS | Bezpečnostní rada státu |
| CERT | Computer Emergency Response Team |
| CSIRT | Computer Security Incident Response Team |
| CVD | Coordinated Vulnerability Disclosure (koordinované zveřejňování zranitelností) |
| CZ PRES | předsednictví České republiky v Radě Evropské unie |
| ČTÚ | Český telekomunikační úřad |
| DDoS | Distributed Denial of Service |
| DIA | Digitální a informační agentura |
| DNS | Domain Name System |
| ECCC | European Cybersecurity Comptence Centre and Network |
| EU | Evropská unie |
| EU-CyCLONe | European Cyber Crisis Liaison Organisation Network (Síť styčných organizací pro řešení kybernetických krizí) |
| EUSPA | European Agency For Space Program (Agentura Evropské unie pro Kosmický program) |
| FBI | Federal Bureau of Investigation (Federální úřad pro vyšetřování) |
| GDPR | General Data Protection Regulation |
| GOVSATCOM | Govemmental Satellite Communications |
| GRON | Galileo Robust Operation Network |
| GSMC | Galileo Security Monitoring Centre (Bezpečnostní a monitorovací centrum programu Galileo) |
| ICT | Information and Communication Technologies (informační a komunikační technologie) |
| IRIS$^2$ | Infrastructure for Resilience, Interconnectivity and Security by Satellite |
| JTA | Join Test Activites |
| KM | kryptografický materiál |
| KP | kryptografický prostředek |
| MF | Ministerstvo financí |
| MO | Ministerstvo obrany |
| MPO | Ministerstvo průmyslu a obchodu |
| 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) |
| 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 |
| PRS | Public Regulated Service (Veřejně regulovaná služba Evropského programu družicové navigace Galileo) |
| SMVS | správa majetku ve vlastnictví státu |
| SW | software |
| TAIEX | Technical Assistance and Information Exchange (Technická pomoc a výměna informací) |
| TEMPEST | Telecommunication Electronics Materials Protected from Emanating Spurious Transmissions |
| UI | utajovaná informace |
| USA | United States of America (Spojené státy americké) |
| VKB | Výbor pro kybernetickou bezpečnost |
| VZ | Vojenské zpravodajství |
| ZKB | zákon o kybernetické bezpečnosti |
| ZoOUI | zákon o ochraně utajovaných informací a bezpečnostní způsobilosti |