



Národní úřad  
pro kybernetickou  
a informační bezpečnost



# ZPRÁVA O ČINNOSTI 2025

# Obsah

|                                                                                      |           |
|--------------------------------------------------------------------------------------|-----------|
| <b>1. Úvodní slovo ředitele</b>                                                      | <b>3</b>  |
| <b>2. Činnost NÚKIB v číslech</b>                                                    | <b>5</b>  |
| <b>3. Oblasti činnosti</b>                                                           | <b>7</b>  |
| 3.1 Strategie a politiky                                                             | 8         |
| 3.2 Kybernetická bezpečnost                                                          | 9         |
| 3.2.1 Vyhodnocení a řešení kybernetických bezpečnostních událostí a incidentů        | 9         |
| 3.2.2 Kontrola, dohled a metodická činnost                                           | 9         |
| 3.2.2.1 Penetrační testování                                                         | 9         |
| 3.2.2.2 Portál NÚKIB                                                                 | 10        |
| 3.3 Bezpečnost informačních a komunikačních systémů                                  | 11        |
| 3.3.1 Kontrola, dohled a metodická činnost                                           | 11        |
| 3.3.1.1 Certifikace informačních a komunikačních systémů                             | 11        |
| 3.3.1.2 Certifikace kryptografických prostředků a pracovišť                          | 11        |
| 3.3.1.3. Ochrana proti kompromitujícímu vyzařování a certifikace stínicích komor     | 12        |
| 3.3.2 Národní distribuční středisko                                                  | 13        |
| 3.3.3 Vývoj kryptografických prostředků                                              | 13        |
| 3.4 Bezpečnost satelitních služeb                                                    | 14        |
| 3.4.1 Veřejně regulovaná služba Evropského programu družicové navigace Galileo (PRS) | 14        |
| 3.4.2 GOVSATCOM a Union Secure Connectivity                                          | 14        |
| 3.5 Správní řízení                                                                   | 15        |
| 3.6 Vzdělávání, osvěta a autorizace pro povolání a pracovní činnosti                 | 16        |
| 3.6.1 Vzdělávání                                                                     | 16        |
| 3.6.2 Osvěta                                                                         | 16        |
| 3.6.3 Autorizace                                                                     | 17        |
| 3.7 Cvičení                                                                          | 18        |
| 3.8 Vědecká činnost, výzkum, vývoj a inovace                                         | 19        |
| 3.9 Legislativa a vládní agenda                                                      | 20        |
| 3.10 Komunikace                                                                      | 22        |
| 3.11 Spolupráce, mezinárodní spolupráce                                              | 23        |
| 3.12 Ekonomické zabezpečení                                                          | 26        |
| 3.12.1 Příjmy                                                                        | 26        |
| 3.12.2 Výdaje                                                                        | 26        |
| 3.12.3 Projekty spolufinancované EU                                                  | 28        |
| 3.13 Personální zabezpečení                                                          | 29        |
| 3.14 Interní audit a vnitřní kontrola                                                | 29        |
| 3.15 Veřejnosprávní kontrola                                                         | 29        |
| <b>4. Seznam použitých zkratk</b>                                                    | <b>30</b> |



# 1. Úvodní slovo ředitele

## VÁŽENÉ DÁMY, VÁŽENÍ PÁNOVÉ,

ROK 2025 BYL PRO NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST (DÁLE JEN „NÚKIB“ NEBO „ÚŘAD“) OPĚT ROKEM MIMOŘÁDNĚ DYNAMICKÝM, PLNÝM ZMĚN A NOVÝCH VÝZEV. PŘINESL NEJEN PŘÍLEŽITOSTI K DALŠÍMU ROZVOJI, ALE TAKÉ ZVÝŠENÉ NÁROKY NA FLEXIBILITU, ODOLNOST A SCHOPNOST RYCHLE REAGOVAT NA PROMĚNLIVÉ PROSTŘEDÍ V OBLASTI KYBERNETICKÉ A INFORMAČNÍ BEZPEČNOSTI. CHARAKTERIZOVALA HO REALIZACE ZÁSADNÍCH SYSTÉMOVÝCH ZMĚN V OBLASTI REGULACE A STRATEGICKÉHO ŘÍZENÍ KYBERNETICKÉ BEZPEČNOSTI V ČESKÉ REPUBLICE. KYBERNETICKÝ PROSTOR SE NADÁLE STÁVÁ KLÍČOVÝM PROSTŘEDÍM, KTERÉ OVLIVŇUJE FUNGOVÁNÍ STÁTU, EKONOMIKY I KAŽDODENNÍ ŽIVOT OBČANŮ, A S TÍM ROSTE I ODPOVĚDNOST INSTITUCÍ, JEŽ SE PODÍLEJÍ NA JEHO OCHRANĚ.

Stanovené cíle a úkoly by nebylo možné zvládat bez nasazení, odbornosti a odpovědného přístupu zaměstnanců, kteří se na plnění úkolů aktivně podíleli. Jejich profesionalita, flexibilita a schopnost spolupracovat představují klíčový pilíř úspěchu realizovaných aktivit, a na úvod proto chci všem zaměstnancům poděkovat za jejich práci, přínos a odhodlání NÚKIB dále rozvíjet.

Za klíčový milník pro NÚKIB považuji schválení nového zákona o kybernetické bezpečnosti. Tento krok završil několikaletou intenzivní spolupráci s řadou partnerů napříč veřejnou správou, soukromým sektorem i odbornou veřejností. Nový zákon o kybernetické bezpečnosti lépe odpovídá současným hrozbám, rozšiřuje ochranu klíčových oblastí státu a současně klade vyšší nároky na všechny, kteří se na zajištění kybernetické bezpečnosti podílejí. Pro NÚKIB znamená také výrazné posílení odpovědnosti i nových úkolů.

Neméně důležité bylo schválení aktualizované Národní strategie kybernetické bezpečnosti České republiky (dále jen „NSKB“), kde NÚKIB byl gestorem zpracování. Nová NSKB nahrazuje předchozí strategii z roku 2021 a zajištění kontinuity této strategie je důkazem nedílné součásti kybernetické bezpečnosti. Strategie vymezuje hlavní priority pro následující období a vytváří rámec pro koordinovaný postup veřejné správy i spolupráci se soukromým sektorem a akademickou sférou.

NÚKIB se v roce 2025 nadále zaměřoval na prevenci a řešení kybernetických bezpečnostních incidentů.

Úřad evidoval více, než dvě stovky incidentů. Díky včasné detekci, analytické činnosti a úzké spolupráci s národními i mezinárodními partnery se dařilo omezovat jejich dopady na chod veřejné správy a další klíčové služby.

Za významný krok směrem k moderní státní správě považuji spuštění Portálu NÚKIB, k němuž došlo 1. listopadu 2025. Portál zjednodušuje komunikaci s regulovanými subjekty, zpřehledňuje procesy a pomáhá lépe se orientovat v zákonných povinnostech.

Za to byl oceněn 2. místem v soutěži Egovernment The Best za projekt digitalizace veřejné správy, což dokazuje, že i v oblasti regulace lze realizovat uživatelsky přívětivá řešení.

Současně Úřad pokračoval v systematickém rozvoji svých odborných kapacit, zejména v oblasti kryptografie, certifikačních služeb, výzkumu a technologického výhledu, včetně příprav na nástup postkvantové kryptografie. Pozornost byla věnována také přípravě legislativy v oblasti Veřejně regulované služby Evropského programu družicové navigace Galileo (dále jen „PRS“), která představuje významný prvek rozvoje národních schopností v oblasti bezpečnosti satelitních služeb. Nedílnou součástí činnosti zůstávala také osvěta a vzdělávání, které NÚKIB dlouhodobě považuje za klíčový nástroj zvyšování celkové odolnosti společnosti.

Vzhledem k nadnárodní povaze kybernetických hrozeb zůstávala i v roce 2025 jednou z priorit mezinárodní spolupráce. Aktivní zapojení NÚKIB do struktur Evropské unie (dále jen „EU“), North Atlantic Treaty Organization (dále jen „NATO“) a bilaterálních partnerství přispívá k posilování důvěry, sdílení informací a koordinaci postupů při řešení kybernetických bezpečnostních incidentů.

Poděkování patří také našim partnerům ve veřejném i soukromém sektoru. Pouze prostřednictvím spolupráce a sdílené odpovědnosti je možné dlouhodobě posilovat kybernetickou bezpečnost České republiky (dále jen „ČR“) a čelit výzvám, které nám digitální svět přináší.

Věřím, že výsledky dosažené v roce 2025 a spolupráce všech zapojených aktérů přispějí k dalšímu posilování bezpečného a důvěryhodného digitálního prostředí v ČR.

Děkuji za Váš zájem o naši činnost.

Ing. Lukáš Kintr

ředitel Národního úřadu pro kybernetickou a informační bezpečnost



## 2. Činnost NÚKIB v číslech

**203**

kybernetických incidentů řešených NÚKIB

**189**

méně významných kybernetických incidentů řešených NÚKIB

**12**

významných kybernetických incidentů řešených NÚKIB

**2**

velmi významné kybernetické incidenty řešené NÚKIB

**74**

bezpečnostních událostí

**29**

samostatných investigací kybernetických hrozeb

**22**

kontrol a auditů podle ZKB

**36**

penetračních testů

**4 505**

podaných ohlášení v Portálu NÚKIB

**217**

řízení o certifikaci informačních systémů

**161**

vydaných certifikátů informačních systémů

**7**

vydaných certifikátů kryptografických prostředků

**18**

vydaných certifikátů kryptografických pracovišť

**31 027**

vygenerovaných kryptografických klíčů

**551**

ks distribuovaného nového kryptografického materiálu

**100**

ks jiného kryptografického materiálu

**42 530**

absolvovaných kurzů Dávej kyber!

**1 872**

absolvovaných kurzů Šéfuj kyber!

**253**

absolvovaných kurzů Bezpečně v kyber!

**4 267**

absolvovaných kurzů Startuj kyber – zdr.

**5 086**

absolvovaných kurzů Dávej kyber – zdr.

**54 008**

absolvovaných kurzů NÚKIB

**190**

posouzených materiálů v mezirezortním připomínkovém řízení

**82**

tiskových zpráv a aktualit  
vydaných NÚKIB

**11**

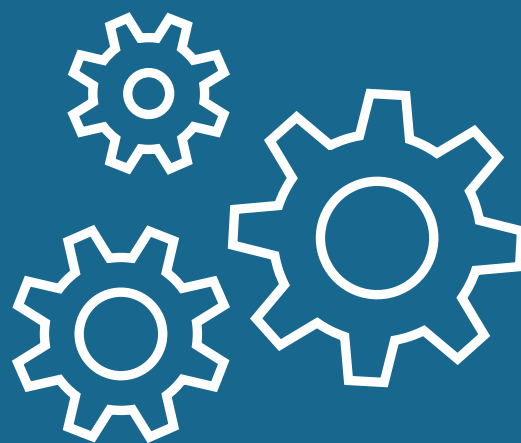
cvičení kybernetické bezpečnosti  
provedených NÚKIB

**373**

účastníků cvičení kybernetické bezpečnosti  
uspořádaných NÚKIB

**28**

uložených nápravných opatření dle ZKB



## 3. Oblasti činnosti

# 3.1 Strategie a politiky

NÚKIB jakožto národní gestor kybernetické bezpečnosti vytváří strategie a politiky definující dlouhodobý směr, cíle a konkrétní opatření k zajištění kybernetické bezpečnosti ČR. V uplynulém roce se NÚKIB aktivně podílel na přípravě řady klíčových strategických dokumentů a přispíval k odborné debatě v rámci mnoha pracovních skupin. Mezi nejvýznamnější v této oblasti patřily následující:

## Národní strategie kybernetické bezpečnosti

V roce 2025 byla dokončena příprava aktualizace NSKB a v září téhož roku byla schválena vládou ČR. NSKB je vrcholným národním strategickým dokumentem pro kybernetickou bezpečnost a nedílnou součástí strategického rámce Česka. Na její přípravě se v duchu celostátního a celospolečenského přístupu podílely více než čtyři desítky relevantních subjektů z veřejného, soukromého, akademického i neziskového sektoru. Ve fázi sběru podnětů byla do přípravy NSKB zapojena i široká veřejnost. Nová NSKB nahrazuje předchozí strategii z roku 2021 a v reakci na zhoršující se globální bezpečnostní situaci a technologické změny posledních let zdůrazňuje zejména potřebu krizové připravenosti, technologické a personální udržitelnosti a intenzivnější spolupráce na vnitrostátní i mezinárodní úrovni.

## Akční plán (dále jen „AP“) k NSKB

V návaznosti na aktualizaci NSKB probíhala v roce 2025 také příprava nového AP k NSKB na období let 2026–2030, který tento vrcholný strategický dokument implementuje. Nový AP stanoví konkrétní, měřitelné a dosažitelné úkoly sloužící k postupné realizaci všech strategických cílů NSKB. Jednotlivé úkoly byly průběžně konzultovány s potenciálními gestory a dalšími subjekty zapojenými do přípravy NSKB, přičemž důraz byl kladen zejména na vyhodnotitelnost jednotlivých úkolů. Přípravu koordinuje NÚKIB a jeho schválení vládou ČR se očekává do poloviny roku 2026.

## Vyhodnocení AP k NSKB za rok 2025 a celkové vyhodnocení za období 2021–2025

Souběžně s přípravou nového AP proběhlo také vyhodnocení plnění AP k NSKB za rok 2025 a s ohledem na konec strategického období i souhrnně za období let 2021–2025. Byl vypracován celkový přehled plnění, včetně důvodů zdržení nebo neúplného splnění některých úkolů a souhrnná statistika úspěšnosti plnění úkolů v těchto letech. Každoroční úspěšnost plnění úkolů, kterých na celé období připadlo 105, se pohybovala mezi 80 až 95 %.

## Národní politika koordinovaného zveřejňování zranitelností

V prosinci 2025 zveřejnil NÚKIB Národní politiku koordinovaného zveřejňování zranitelností (dále jen „CVD“), jejímž cílem je zvyšování bezpečnosti produktů informačních a komunikačních technologií (dále jen „ICT“) a ochrana objevitelů zranitelností před negativními právními dopady. Národní politika CVD představuje efektivní nástroj pro navyšování bezpečnosti produktů ICT, jelikož podporuje spolupráci jejich vlastníků a správců s objeviteli zranitelností. Součástí celého procesu je tzv. koordinátor pro účely CVD, jímž se stal podle nového zákona o kybernetické bezpečnosti vládní Computer Emergency Response Team (dále jen „CERT“), který je součástí NÚKIB.

## Implementační plán Národní politiky kryptografické ochrany utajovaných informací

V návaznosti na schválení Národní politiky kryptografické ochrany utajovaných informací v České republice (dále jen „NP KOUÍ“) Bezpečnostní radou státu (dále jen „BRS“) v listopadu 2024 připravil NÚKIB v průběhu roku 2025 Implementační plán NP KOUÍ, který slouží k přenesení cílů politiky do konkrétních kroků. V průběhu roku byl plán navržen a konzultován s relevantními subjekty a v závěru roku 2025 byl připraven k předložení BRS, která by měla dokument schválit. Jeho plnění by mělo být zahájeno v průběhu prvního pololetí roku 2026.

## Minimální požadavky na kryptografické algoritmy

NÚKIB v roce 2025 aktualizoval dokument Minimální požadavky na kryptografické algoritmy, čímž reagoval na vývoj hrozeb v oblasti kryptografie a nástup postkvantových standardů šifrování. Aktualizace z doporučení mimo jiné odstranila zastaralé algoritmy, zpřesnila parametry doporučovaných řešení a doplnila moderní mechanismy pro integritu a bezpečné ukládání hesel. Ačkoli nejde o obecně závazný právní předpis, vyhlášky k zákonu o kybernetické bezpečnosti ukládají povinnost tyto minimální požadavky zohledňovat, přičemž příloha dokumentu s minimálními požadavky poskytuje praktický výklad zejména v oblasti postkvantové kryptografie.

Přechod na kvantově odolná řešení je současně i jednou z priorit ČR v oblasti kybernetické bezpečnosti na následující roky. Je zakotven v nové NSKB i Národní strategii pro kvantové technologie ČR a NÚKIB jej podporuje doporučením využívat přechodná hybridní schémata. V roce 2025 byla také zahájena příprava národního plánu přechodu na postkvantově odolnou kryptografii.

## 3.2 Kybernetická bezpečnost

### 3.2.1 Vyhodnocení a řešení kybernetických bezpečnostních událostí a incidentů

V roce 2025 NÚKIB evidoval celkem 203 kybernetických incidentů, z nichž 12 bylo významných a 2 velmi významné. Pokles oproti předchozímu roku je pravděpodobně způsoben odkloněním pozornosti proruských hacktivistických skupin od českých cílů.

Nosným trendem nadále zůstává ransomware. Během roku bylo zaznamenáno 31 úspěšných útoků, přičemž nejčastěji se objevovaly varianty Qilin a INC. Vývoj ransomwaru směřuje stále více k Ransomware as a Service modelu a k méně fragmentované struktuře operátorů, což analytikům NÚKIB značně ztěžuje orientaci v jednotlivých skupinách a jejich oblíbených metodách útoku.

Dalším trendem je mírný nárůst útoků cílených na autentizační tokeny a session cookies místo tradičního prolamování hesel, zejména v cloudových prostředích.

Kromě incidentů NÚKIB evidoval také 74 kyberbezpečnostních událostí a otevřel 29 samostatných investigací kybernetických hrozeb.

V květnu 2025 vláda ČR provedla veřejnou atribuci škodlivé kybernetické kampaně Čínské lidové republiky proti jedné z neutajovaných komunikačních sítí Ministerstva zahraničních věcí (dále jen „MZV“). Tato kampaň probíhala minimálně od roku 2022. Závěry analýzy provedené NÚKIB, Vojenským zpravodajstvím (dále jen „VZ“), Úřadem pro zahraniční styky a informace a Bezpečnostní informační službou (dále jen „BIS“) ukázaly, že za škodlivou aktivitou stála velmi pravděpodobně skupina Advanced Persistent Threat 31 (dále jen „APT31“), veřejně spojovaná se zpravodajskou službou Ministerstva státní bezpečnosti, která je spojována s dalšími útoky v EU či NATO. Solidaritu a podporu ČR vyjádřila EU i členské státy, stejně jako spojenci v NATO.

### 3.2.2 Kontrola, dohled a metodická činnost

V průběhu roku 2025 uskutečnil NÚKIB celkem 22 kontrol a auditů prováděných podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti, a jeho prováděcí vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat, ve znění pozdějších předpisů (dále jen „ZKB“).



V oblasti regulace cloud computingu podle zákona č. 365/2000 Sb., o informačních systémech veřejné správy, NÚKIB za rok 2025 posoudil a následně vydal stanoviska k 36 poskytovatelům a 61 žádostem týkajícím se nabídek cloud computingu.

Vedle vlastní kontrolní činnosti se NÚKIB i nadále zaměřoval na poskytování metodické podpory povinným osobám, která spočívala zejména v průběžném zodpovídání odborných dotazů, přípravě a publikaci podpůrných materiálů a realizaci auditů u vybraných subjektů.

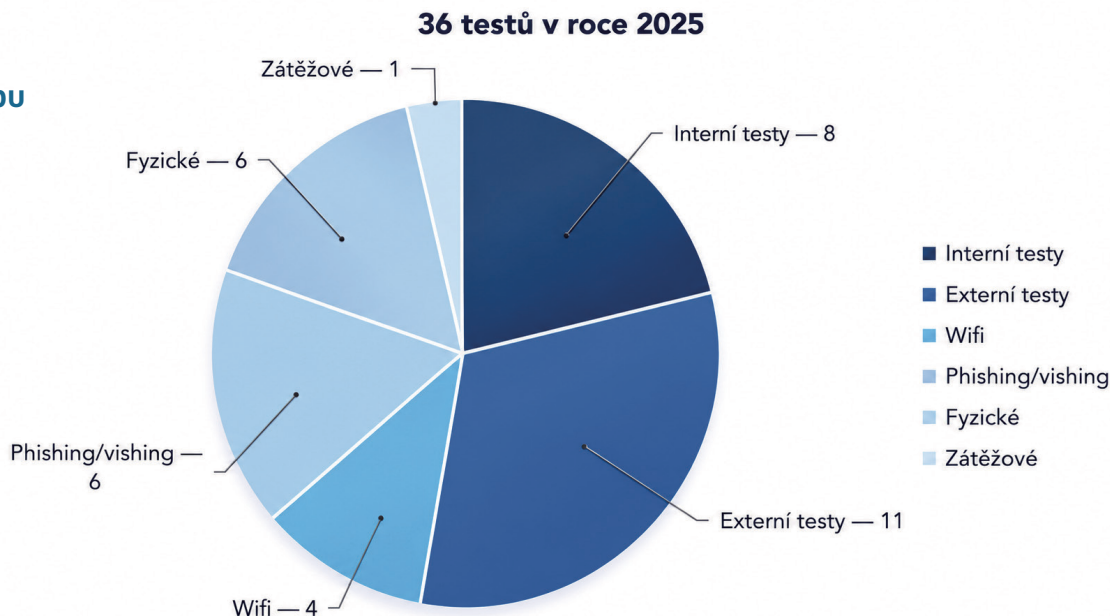
V návaznosti na aktualizaci právních předpisů v oblasti kybernetické bezpečnosti NÚKIB postupně vydával soubor metodických materiálů určených povinným subjektům s cílem usnadnit výklad nových a upravených povinností, sjednotit aplikační praxi a poskytnout praktickou podporu při zavádění požadovaných bezpečnostních opatření.

#### 3.2.2.1 Penetrační testování

V roce 2025 proběhlo 36 penetračních testů, z toho 8 interních, 11 externích, 4 testy síťového zabezpečení wi-fi, 6 fyzických a 6 phishingových kampaní (5 phishingových kampaní a jednou byly rozmístěny flashdisky) a 1 zátěžový test v spolupráci s Vysokým učením technickým v Brně (dále jen „VUT“). Celkem bylo otestováno 10 subjektů.

Oproti roku 2024 došlo k padesátiprocentnímu nárůstu poptávky po komplexních penetračních testech, které zahrnují kromě interních a externích také fyzické testování, wi-fi infrastrukturu a phishingové kampaně.

## Přehled testů proběhlých v roce 2025 dle jejich typu



### 3.2.2.2 Portál NÚKIB

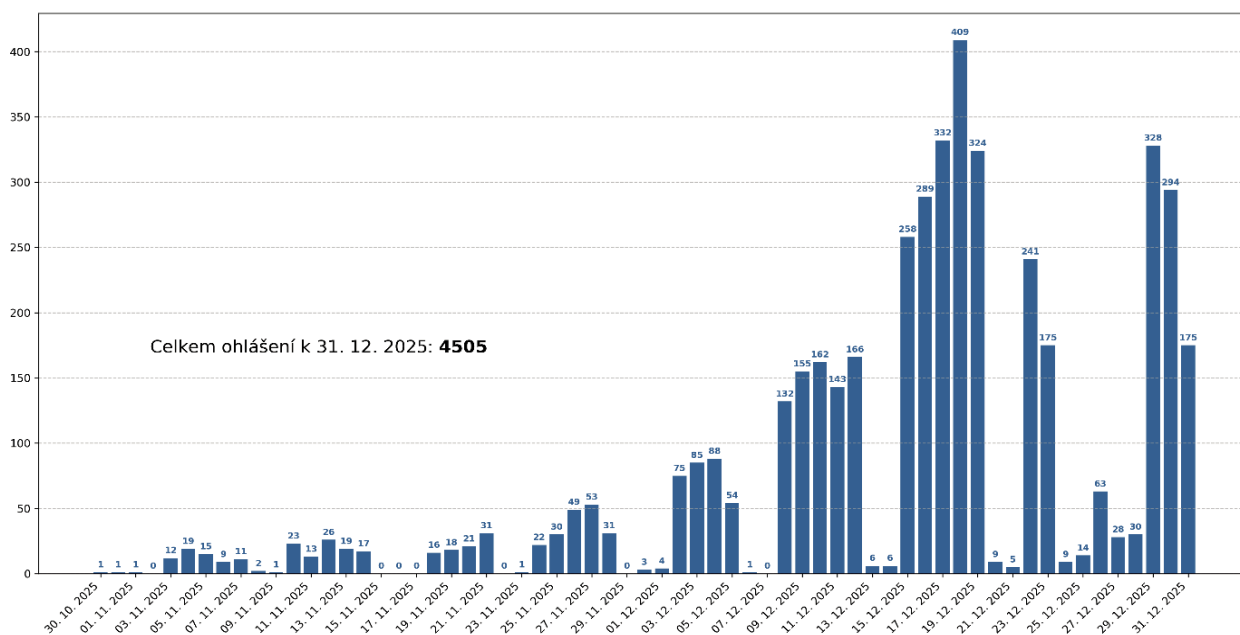
Komunikační a informační platforma Portál NÚKIB se od 1. listopadu 2025 stala klíčovým nástrojem pro komunikaci mezi NÚKIB a povinnými subjekty dle zákona o kybernetické bezpečnosti. V roce 2025 bylo tedy hlavním cílem připravit Portál na nabytí účinnosti nového zákona, což zahrnovalo zejména vývoj a implementaci formulářů umožňujících regulovaným subjektům plnit jejich zákonné povinnosti, jako je ohlášení regulované služby či hlášení kybernetických incidentů.

Součástí příprav bylo také napojení formulářů na externí systémy, zejména Identitu občana a základní registry, a příprava infrastruktury Portálu na očekávaný nárůst

počtu uživatelů ze stovek na tisíce. V průběhu roku byly také publikovány podpůrné materiály, které usnadňují orientaci v nových povinnostech a práci s Portálem. Spuštění formulářů v sekci Chci vyřídit proběhlo bez komplikací a během prvních dvou měsíců od jejich uvedení do provozu bylo evidováno celkem 4 505 podaných ohlášení. První ohlášení podal jménem NÚKIB ředitelem Úřadu Lukáš Kintr.

Portál NÚKIB získal 2. místo v soutěži Egovernment The Best, kterou každoročně vyhlašuje magazín Egovernment za projekty digitalizace veřejné správy. Toto ocenění potvrzuje význam Portálu jako moderního a efektivního nástroje veřejné správy v oblasti kybernetické bezpečnosti.

## Přehled počtu podaných ohlášení za den na Portál v období od 31. 10. 2025 do 31. 12. 2025



## 3.3 Bezpečnost informačních a komunikačních systémů

### 3.3.1 Kontrola, dohled a metodická činnost

NÚKIB v roce 2025 organizačně zajistil vydání Certificate of Crypto-Authorisation, poučení k němu, konzultační činnost a debriefing pro subjekty veřejné správy i pro subjekty soukromého sektoru.

Školení pracovníků kryptografické ochrany a zkoušky odborné způsobilosti.

NÚKIB v roce 2025 organizačně zajistil a provedl celkem 24 prezentací pro skupiny pracovníků kryptografické ochrany a po následující zkoušce odborné způsobilosti vydal 155 osvědčení o zvláštní odborné způsobilosti pracovníka kryptografické ochrany. Školení, která jsou v neutajovaném režimu, proběhla on-line formou.

V roce 2025 byla provedena aktualizace rozsahu smluv (z hlediska typů kryptografických prostředků) k provádění odborné zkoušky a vydávání osvědčení o zvláštní odborné způsobilosti pracovníků kryptografické ochrany uzavřených s Ministerstvem obrany (dále jen „MO“) a Ministerstvem vnitra (dále jen „MV“).



#### 3.3.1.1 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 Národním bezpečnostním úřadem (dále jen „NBÚ“).

V roce 2025 probíhalo řízení o certifikaci u 217 informačních systémů. K 75 žádostem o certifikaci informačního systému, jejichž zpracování bylo zahájeno v roce 2024, přibýlo v roce 2025 dalších 142 žádostí, a to 48 ze státní správy nebo samosprávy a 94 od podnikatelů. Ve většině případů se jednalo o žádosti o opakovanou certifikaci již provozovaných informačních systémů. Ve 32 případech byla podána žádost o certifikaci nově budovaného informačního systému.

V roce 2025 bylo vydáno celkem 161 certifikátů informačních systémů pro žadatele ze státní správy nebo samosprávy, podnikatele, včetně akreditací informačních systémů cizí moci.

#### 3.3.1.2 Certifikace kryptografických prostředků a pracovišť

V roce 2025 bylo certifikováno 7 kryptografických prostředků a 18 kryptografických pracovišť. Byla vydána tři schválení zástavby kryptografického prostředku do mobilního/rozmístitelného systému a pět schválení materiálu k zajištění funkce kryptografického prostředku.

### 3.3.1.3. Ochrana proti kompromitujícímu vyzařování a certifikace stínicích komor

#### Přehled měření v oblasti kompromitujícího vyzařování v roce 2025

| Typ měření <sup>1</sup>                     | Počet           |
|---------------------------------------------|-----------------|
| Zónové měření                               | 13 lokalit      |
| Kryptografické prostředky                   | 3 typy          |
| Komponenty ICT                              | > 40 systémů    |
| Audiotecnika                                | 2 typy zařízení |
| Technické kontroly i v rámci certifikace IS | 12 objektů      |
| Mobilní systémy                             | 5 typů systémů  |
| Instalační záznamy                          | > 10 lokalit    |
| Stínicí komory                              | 18 certifikátů  |

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

#### TEMPEST měření elektronických zařízení

Úřad prováděl v roce 2025 Telecommunication Electronics Materials Protected from Emanating Spurious Transmissions (dále jen „TEMPEST“) měření podle standardů NATO řady Security Design and Installation Publication, EU řady Information Assurance Steering Group 7 a podle metodiky bezpečnostních standardů NBÚ. Objektem měření byla především zařízení orgánů státu. Jednalo se jak o měření komerčních zařízení (většinou pro účely výběrových řízení), tak speciálních informačních systémů (zejména vojenských).

Celkem bylo v roce 2025 provedeno více než 40 měření různých typů zařízení. Z toho bylo prováděno TEMPEST měření samostatných zařízení, v kombinaci s kryptografickým prostředkem PCS1 a Local Area Network Personal Computer System (dále jen „LANPCS“) Box či nové systémy pro zabezpečené videokonference GearLab pro Armádu ČR, nový hardware pro informační systém VegaT-2G. Tato měření byla prováděna podle metodiky standardu Security Design and Installation Publication 27/3. Požadavky tohoto standardu splnila 95 % zařízení.

Další TEMPEST měření byla prováděna v rámci certifikace nebo akreditace informačních systémů pro zpracování utajovaných informací stupně utajení Důvěrné nebo Tajné, buď pro orgány státu (např. Úřad vlády ČR, MZV, MO, MV, Ministerstvo průmyslu a obchodu (dále jen „MPO“), zpravodajské služby aj.), nebo pro podnikatele. Bylo provedeno měření i pro zahraniční uživatele (ze Slovinska). Z celkového počtu hodnocených zařízení byla většina vyžádána MO.

#### Zónové měření, instalační záznamy, obranné prohlídky

Úřad dále prováděl ohodnocování prostorů metodou zónového měření ve 13 lokalitách. Jednalo se o prostory, ve kterých se nacházela zařízení zpracovávající utajované informace. Tento druh měření byl především použit u objektů jednotlivých ministerstev a krajských ředitelství policie.

Prováděno bylo rovněž zónové hodnocení prostorů na základě podkladů dodaných akreditovanými pracovišti MO, BIS a VZ.

Bylo provedeno hodnocení instalace informačních systémů zpracovávajících utajované informace stupně utajení Důvěrné a Tajné a v rámci certifikace těchto systémů byly zpracovány instalační záznamy z více než 10 lokalit. Dále byly posouzeny instalační záznamy z akreditovaných pracovišť (MO, BIS, VZ, MV).

V roce 2025 byly provedeny technické kontroly v několika objektech jak v ČR, tak mimo ni na základě žádostí orgánů státní správy nebo v rámci certifikace informačních systémů.

### 3.3.2 Národní distribuční středisko

Výroba kryptografického materiálu

V roce 2025 NÚKIB vygeneroval celkem 31 027 kryptografických klíčů a hesel uložených na 4 546 nosičích různých typů a dalších 100 ks jiného kryptografického materiálu (provozní dokumentace kryptografického prostředku, instalační a šifrovací software). Kryptografický materiál je určen pro NÚKIB a orgány státu k zajištění ochrany utajovaných informací v komunikačních a informačních systémech.

NÚKIB v roce 2025 vzal do evidence a zajistil distribuci celkem 551 ks nového kryptografického a Controlled Cryptographic Item materiálu a dále zabezpečil servis a opravy na území ČR u 736 ks kryptografických prostředků a mimo ČR u 27 ks kryptografických prostředků.

NÚKIB vzal do evidence a zajistil distribuci celkem 40 ks kryptografického materiálu EU a zajistil přepravu 2 ks zásilek kryptografického prostředku 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.

### 3.3.3 Vývoj kryptografických prostředků

V roce 2025 probíhaly vývojové projekty aplikované kryptografie dle schváleného Výzkumného záměru. Zejména se jednalo o vývojové projekty prostředků a komponent rodiny LANPCS; dále komunikátoru OSK II a notifikačního zařízení. Tato hlavní činnost byla doplněna interními výzkumně-vývojovými projekty:

- vývoj návrhových, překladových, verifikačních a testovacích kryptologických pracovišť;
- výzkum paměťové bezpečnosti programovacích jazyků a
- vývoj programů a metodik pro generování, verifikaci a testování strukturálních prvků pro kryptografická primitiva.

## 3.4 Bezpečnost satelitních služeb

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

V roce 2025 se NÚKIB intenzivně podílel na přípravě samostatného národního legislativního rámce pro službu Galileo PRS, jehož cílem je jasně vymezit roli státu, podmínky přístupu ke službě a související bezpečnostní požadavky. Legislativní práce byly úzce provázány s tvorbou strategických a koncepčních dokumentů Příslušného orgánu PRS a se zpracováním studií využitelnosti služeb PRS a Governmental Satellite Communications (dále jen „GOVSATCOM“), které slouží jako odborný podklad pro finální podobu právní úpravy.

Po celý rok 2025 NÚKIB zajišťoval provoz utajovaného spojení s Galileo Security Monitoring Centre prostřednictvím sítě Galileo Robust Operation Network (dále jen „GRON“). Pro tuto technologii byla v provozu jak neutajovaná část GRONU (Unclassified), tak utajovaná část GRONS (Secret). Současně byla provozována navazující platforma Point of Contact Platform (dále jen „POCP“), zatím v neutajované variantě POCPU (Unclassified). Utajovaná část POCPs (Secret) bude zprovozněna před dosažením plně operační fáze služby PRS FOC (Full Operational Capability).

V roce 2025 byla vypsána veřejná zakázka na národní informační systém pro PRS, tzv. Point of Contact Internal System. V rámci zadávacího řízení byla vybrána společnost, která bude projekt realizovat, a byla s ní uzavřena smlouva splňující všechny náležitosti pro systém pracující s utajovanými informacemi.

V roce 2025 pokračovala také příprava projektu PursuitX v rámci programu Horizon Europe (Joint Technical Activity). NÚKIB se zapojil do konsorcia několika členských států, které disponují technologiemi GRON/POCP a přijímači PRS pro příjem signálu ve vesmíru PRS Signal in Space. Cílem projektu je testování připravenosti služby a celého systému na dosažení počáteční operační způsobilosti PRS Initial Operational Capability.

NÚKIB také v průběhu roku testoval zapůjčené operační přijímače PRS od společnosti Leonardo (P3RSe) a zařízení Key Transfer Device.



Na úrovni Evropské unie došlo v roce 2025 k posunu v přípravě a schvalování klíčových programových dokumentů nezbytných pro dosažení počátečních operačních schopností služby PRS, včetně dokumentu Concept of Operations. Zástupci NÚKIB se zároveň aktivně účastnili jednání Security Accreditation Board a Security Accreditation Panel při Agentuře Evropské unie pro Kosmický program (European Agency for the Space Programme – EUSPA), kde jsou řešeny otázky bezpečnosti a akreditace komponent evropského kosmického programu, zejména v souvislosti s přechodem služby PRS do fáze Initial Operational Capability a Open Service Full Operational Capability.

### 3.4.2 GOVSATCOM a Union Secure Connectivity

V roce 2025 probíhaly odborné práce a konzultace k budoucímu zahrnutí GOVSATCOM (a IRIS<sup>2</sup>) do národní legislativy, a to včetně vymezení okruhu uživatelů a návaznosti na evropskou regulaci.

V návaznosti na tuto přípravu proběhlo školení a testování platformy GOVSATCOM HUB, která slouží jako informační systém pro příslušné orgány GOVSATCOM Competent Govsatcom Authority a oprávněné uživatele k vyhledání a vyžádání satelitní komunikační služby, včetně možnosti získání terminálového zařízení pro danou službu. Současně Evropská komise v roce 2025 uzavřela smlouvy s poskytovateli služeb (Resource Providers), tedy s členskými státy disponujícími komunikačními satelity a s komerčními poskytovateli z EU, na což NÚKIB po přechodu služby do informačního systému navázal přípravou testování u českých uživatelů.

## 3.5 Správní řízení

### **Rozhodování v prvním stupni ve věcech vymáhání plnění povinností dle ZKB a ZoOUI**

V návaznosti na nedostatky zjištěné při kontrolách v oblasti kybernetické bezpečnosti dle ZKB NÚKIB v roce 2025 pravomocně uložil povinným osobám nebo orgánům v pěti případech celkem 28 nápravných opatření k odstranění nedostatků a vydal 6 rozhodnutí o přestupcích na úseku ZKB, kterými rozhodl o spáchání celkem 11 přestupků. Ve čtyřech případech byly pravomocně uloženy pokuty v celkové výši 610 000 Kč.

V roce 2025 NÚKIB vydal dvě rozhodnutí o přestupcích na úseku zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů (dále jen „ZoOUI“), kterými rozhodl o spáchání dvou přestupků. Pokuty byly uloženy v celkové výši 208 000 Kč.



### **Činnost rozkladové komise ředitele NÚKIB**

Rozkladová komise ředitele NÚKIB v roce 2025 projednala v rámci řízení o rozkladech proti rozhodnutí NÚKIB celkem 7 rozkladů. Jednalo se o tři případy přestupků dle ZKB, jeden případ uložení povinnosti dle § 15a ZKB, jeden případ přestupku na úseku ZoOUI a dva případy rozkladů proti rozhodnutí NÚKIB o odmítnutí poskytnutí informací dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů.

## 3.6 Vzdělávání, osvěta a autorizace pro povolání a pracovní činnosti

### 3.6.1 Vzdělávání

E-learningové kurzy zůstaly i v roce 2025 hlavním nástrojem pro vzdělávání široké veřejnosti v oblasti kybernetické bezpečnosti. V závěru roku došlo k dočasnému omezení poskytování e-learningových služeb prostřednictvím osvětového portálu (portál osveta.nukib.gov.cz) a dostupnost vzdělávacích materiálů byla zajištěna náhradním způsobem.

Kurzy NÚKIB připravené v českém jazyce byly veřejně dostupné a zdarma prostřednictvím internetu. Tato otevřenost je přínosná zejména pro organizace veřejné správy, které tak mohou zvyšovat povědomí svých zaměstnanců bez dodatečných rozpočtových nákladů.

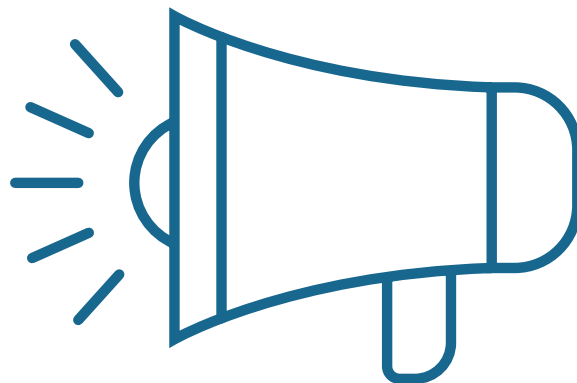
#### Přehled počtu absolvovaných on-line kurzů

| KURZ                 | 2025  |
|----------------------|-------|
| Dávej kyber!         | 42530 |
| Šéfuj kyber!         | 1872  |
| Bezpečně v kyber!    | 253   |
| Startuj kyber – zdr. | 4267  |
| Dávej kyber – zdr.   | 5086  |
| CELKEM               | 54008 |

NÚKIB se účastnil celkem 133 prezenčních vzdělávacích akcí zaměřených na kybernetickou bezpečnost, na kterých fyzicky proškolil přibližně 5 000 osob, mezi nimiž byli zaměstnanci MO, Ministerstva financí, Kanceláře prezidenta republiky apod.

### 3.6.2 Osvěta

NÚKIB se v roce 2025 účastnil evropského veletrhu pomaturitního a celoživotního vzdělávání Gaudeamus Brno 2025 s cílem prezentovat Úřad jako možného zaměstnavatele, nabídnout možnost odborných stáží a poukázat na základní znalosti v oblasti kyberbezpečnosti. Dále se NÚKIB zúčastnil veletrhu středních škol TAK KAM?! v Brně. Pro akci byl vytvořen nový koncept a nové propagační materiály a osvětové letáky s cílem rozšířit povědomí o kybernetické bezpečnosti mezi žáky základních škol, pedagogy a rodiči.



V září se NÚKIB zapojil do akce Týden pro digitální Česko, v rámci které uspořádal jeden vlastní webinář a účastnil se pěti akcí dalších partnerů.

Na konferenci CYBER\_CON ředitel NÚKIB oceněnil čtyři studentky a studenty středních škol za jejich aktivní zájem o kybernetickou bezpečnost.

V říjnu 2025 NÚKIB uspořádal čtvrtý ročník Festivalu bezpečného internetu s tématem a mottem „Sleduj svou digitální stopu“. Celkem se do festivalu přihlásilo 42 subjektů. Plakátovou kampaň v on-line/pdf podobě obdrželo 25 knihoven/senior pointů/family pointů. NÚKIB poprvé navázal spolupráci s iniciativou Moderní sebeobrana a zapojil influencery do propagace a tvorby obsahu. V říjnu vznikla série čtyř videí pro sociální sítě (Instagram, LinkedIn, Facebook) na témata sexting, kyberšikana, hate speech a kybergrooming a zároveň čtyři newslettery rozeslané téměř 7 tisícům odběratelů; na Instagramu videa souhrnně dosáhla přes 500 tisíc zhlédnutí, 16 tisíc likes, 460 repostů a 8 880 přeposlání.

Na sociálních médiích již tradičně proběhlo několik minikampaní, například u příležitosti Dne žen a dívek v ICT, Dne hesla či Dne dětí.

### 3.6.3 Autorizace

NÚKIB jako orgán příslušný k rozhodování o udělení, prodloužení platnosti nebo odnětí autorizace pro povolání a pracovní činnosti v oblasti kybernetické bezpečnosti v roce 2025:

1. dokončil profesní a hodnoticí standardy 6 profesních kvalifikací z oblasti kybernetické bezpečnosti:
  - a. Manažer/manažerka kybernetické bezpečnosti (kód: 18-015-T),
  - b. Analytik/analytička kybernetické bezpečnosti (kód: 18-016-T),
  - c. Architekt/architektka kybernetické bezpečnosti (kód: 18-017-T),
  - d. Technik/technička kybernetické bezpečnosti (kód: 18-018-N),
  - e. Auditor/auditorka kybernetické bezpečnosti (kód: 18-019-T),
  - f. Pracovník/pracovnice bezpečnostního dohledového centra informačních systémů (kód: 18-020-M),
2. zahájil technickou aktualizaci profesních a hodnoticích standardů profesních kvalifikací z důvodu změny legislativy,
3. posoudil dvě žádosti o autorizace,
4. vydal první rozhodnutí o autorizaci pro profesní kvalifikaci manažera kybernetické bezpečnosti.

## 3.7 Cvičení

### Locked Shields 2025

Toto hybridní cvičení je pořádáno NATO Cooperative Cyber Defence Centre of Excellence (dále jen „NATO CCD COE“) a na jeho přípravě se podílejí přední firmy z technologického průmyslu, zástupci akademického sektoru a řady státních institucí. Cílem bylo prohloubit spolupráci mezi všemi zúčastněnými subjekty. NÚKIB tvořil společný tým s partnerskými organizacemi a kolegy z Albánie. Do cvičení, jehož součástí je ochrana počítačových systémů před útoky v reálném čase a simulace taktických a strategických rozhodnutí v kritických situacích, se v roce 2025 zapojilo přibližně 4000 účastníků ze 41 zemí světa. V konkurenci 17 týmů se česko-albánský tým umístil na 14. místě.



### NATO Cyber Coalition

Cyber Coalition je 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.

### VCISC

NÚKIB v roce 2025 uspořádal cvičení zaměřené na schopnost poskytnutí dálkové podpory při kybernetických incidentech v rámci mechanismu Virtual Cyber Incident Support Capability (dále jen „VCISC“). Jedná se o mechanismus, jenž umožňuje spojencům v NATO čelícím rozsáhlé škodlivé kybernetické aktivitě požádat ostatní členy aliance o vzdálenou pomoc. Tento mechanismus byl schválen na summitu ve Vilniusu v roce 2023 a od té doby je alianci k dispozici. VCISC je zároveň významným nástrojem posilujícím kolektivní obranu NATO v kyberprostoru.

### 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 2025 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.

### Národní koncepce cvičení kybernetické bezpečnosti

NÚKIB v roce 2025 intenzivně připravoval ve spolupráci s partnery celonárodní dokument „Národní koncepce cvičení kybernetické bezpečnosti“. Koncepce si klade za cíl systematicky rozvíjet cvičení kybernetické bezpečnosti na základě efektivní spolupráce široké komunity s důrazem na inovace a sdílení znalostí.

## 3.8 Vědecká činnost, výzkum, vývoj a inovace

V rámci výzkumu a vývoje v oblasti bezpečnosti ICT bylo v roce 2025 zahájeno 9 nových projektů, které byly realizovány dodavatelským způsobem. Spolupráce v těchto projektech byla navázána jak s akademickou sférou, tak i se soukromými společnostmi, které se specializují na bezpečnostní výzkum a vývoj. Mezi hlavní partnery patří například České vysoké učení technické v Praze či společnost S.ICZ, a. s.

Projekty jsou zaměřeny na problematiku TEMPEST, vývoj kryptografických prostředků a kryptologickou analýzu. Většina projektů vychází z výzkumu a výstupů předchozích let a navazuje na dosažené výsledky. Tato kontinuita je klíčová pro udržení vysoké úrovně inovací a kvalitního pokroku v dané oblasti.

V roce 2025 bylo rovněž úspěšně ukončeno řešení čtyř významných projektů zahájených v předchozím období. Jednalo se o projekty zabývající se ochranou utajovaných informací a vývojem nové generace národních kryptografických prostředků, které byly realizovány s cílem přinést nové, vysoce relevantní výsledky v dané oblasti.

Současně probíhaly také interní výzkumné a vývojové projekty na odborném pracovišti, zaměřující se na vývoj kryptografických prostředků a ochranu utajovaných informací. Tyto projekty doplňovaly externí spolupráci a přispívaly k posilování výzkumného potenciálu týmu NÚKIB a budování postavení v oblasti bezpečnosti ICT.

NÚKIB v roce 2025 podpořil celkově 24 návrhů projektů předložených do výzev programů výzkumu a vývoje ze strany akademických a výzkumných institucí (VUT, České vysoké učení technické v Praze, Vysoká škola báňská – Technická univerzita Ostrava, MU, CESNET, zájmové sdružení právnických osob, Technologické centrum Praha) a soukromých subjektů (Datlab, s. r. o., a Flowmon Networks, a. s.). Projekty NÚKIB podporoval zejména z pozice aplikačního garanta nebo uživatelské organizace, ve vybraných projektech se NÚKIB zapojil i do samotné realizace projektu.

NÚKIB dále plnil roli „asociovaného partnera“ v evropském projektu Cyber-Security Excellence Hub in Estonia and South Moravia financovaného z programu Horizont Europe. Zkušenosti s působením v tomto projektu NÚKIB zúročil při zapojení do projektu Quantum-Resistant Cryptography in Practice, koordinovaného ze strany VUT, kde se již v roli plnohodnotného člena řešitelského konsorcia podílel na praktickém nasazení postkvantové kryptografie v reálných aplikacích a infrastrukturách.



Pro prohlubování spolupráce mezi veřejnou a akademickou sférou a soukromým sektorem NÚKIB zorganizoval dvě jednání Skupiny kyberbezpečnostního výzkumu a inovací Cyber Research and Innovations in Security. Tato akce, určená expertům působícím zejména ve výzkumu a vývoji v kybernetické a informační bezpečnosti, poskytuje prostor pro sdílení aktuálních vývojových a bezpečnostních trendů ze strany státu, sdílení příležitostí pro spolupráci na výzkumných projektech a předávání zkušeností mezi jednotlivými organizacemi tvořícími národní výzkumný ekosystém.

Za účelem zviditelnění českých výzkumných organizací v zahraničí byly realizovány tři výzkumné mise v rámci podpory ekonomické a vědecké diplomacie. Projekty na podporu ekonomické diplomacie. Mise do Nizozemska a na Taiwan se orientovaly na rozvoj schopností Česka v oblastech kvantových a postkvantových technologií. Mise do Kanady se zaměřovala na bezpečnost satelitních služeb a možnosti realizace výzkumných projektů v této oblasti.

V roce 2025 pokračovala realizace dvou projektů financovaných 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. Druhý projekt je zaměřen na podporu implementace evropského rámce certifikací kybernetické bezpečnosti. NÚKIB v roce 2025 vypsál již druhou dotační výzvu, která se zaměřovala na podporu subjektů implementujících Akt o kybernetické odolnosti. Na těchto projektech NÚKIB úzce spolupracuje s konsorciálním partnerem CyberSecurityHubCZ.

## 3.9 Legislativa a vládní agenda

Rok 2025 byl v oblasti legislativy významně ovlivněn volbami do Poslanecké sněmovny Parlamentu České republiky (dále jen „PSP ČR“). V prvním pololetí tohoto roku bylo cílem NÚKIB dokončit legislativní proces vládního návrhu zákona o kybernetické bezpečnosti a vládního návrhu zákona, kterým se mění některé zákony v souvislosti s přijetím zákona o kybernetické bezpečnosti. Již v lednu 2025 prošly návrhy obou zákonů úspěšně druhým čtením v PSP ČR. V dubnu 2025 pak garanční výbor doporučil návrhy zákonů spolu s některými pozměňovacími návrhy PSP ČR ke schválení. Tentýž měsíc pak prošly návrhy zákonů také třetím čtením a následně v květnu byly postoupeny Senátu k projednání. Senát oba návrhy zákonů v červnu 2025 projednal jak ve svých výborech, tak na schůzi Senátu a následně je postoupil k podpisu prezidentovi republiky. Prezident oba návrhy zákonů 26. června 2025 podepsal. V červenci byly potom oba schválené a podepsané zákony odeslány do Sbírky zákonů a 4. srpna 2025 zveřejněny s účinností od 1. listopadu 2025.

Tímto byl uzavřen více než tři roky trvající proces, který obsahoval:

- veřejné konzultace: NÚKIB obdržel více než 1000 podnětů od přibližně 100 subjektů (více než polovina zohledněna),
- mezirezortní připomínkové řízení: NÚKIB obdržel 886 připomínek od více než 50 subjektů a za účelem jejich vypořádání absolvoval téměř 30 jednání (soulasně vypořádány přibližně 2/3 připomínek z celkového počtu),
- obhajobu návrhů zákonů u poradních orgánů vlády, v PSP ČR a v Senátu,
- vystoupení na více než 70 konferencích,
- odpovědi na téměř 700 písemných dotazů týkajících se nové regulace,
- přípravu více než 20 podpůrných materiálů
- a další kroky spojené s přípravou nové regulace.

Návrhy zákonů by ovšem nebyly kompletní a funkční bez prováděcích právních předpisů. V souvislosti s revizí regulace v oblasti kybernetické bezpečnosti jich NÚKIB připravoval celkem 9, a to tyto:



- vyhláška o regulovaných službách,
- vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností,
- vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností,
- vyhláška o Portálu Národního úřadu pro kybernetickou a informační bezpečnost a požadavcích na některé úkony,
- vyhláška o bezpečnostních pravidlech pro orgány veřejné správy využívající služby poskytovatelů cloud computingu,
- vyhláška o některých požadavcích pro zápis do katalogu cloud computingu,
- vyhláška o bezpečnostních úrovních informačních systémů veřejné správy,
- nařízení vlády o nepominutelných funkcích stanoveného rozsahu,
- nařízení vlády o regulovaných službách, které splňují podmínky strategicky významné služby, a o částech strategicky významných služeb tvořících nezbytný rozsah zajištění dostupnosti strategicky významných služeb (nařízení o strategicky významných službách).

Jejich legislativní proces je pevně spjatý s návrhem zákona, který má provádět, a proto NÚKIB již k návrhu zákona přiložil do jeho legislativního procesu teze těchto prováděcích předpisů. Legislativní proces samotných prováděcích právních předpisů započal v květnu 2025, a to meziresortním připomínkovým řízením, které bylo ukončeno v červnu 2025. Následně probíhalo v průběhu léta 2025 vypořádání připomínek, které NÚKIB k návrhům obdržel. Opět se jednalo o stovky připomínek. Po jejich vypořádání byly návrhy prováděcích právních předpisů v září 2025 předloženy pracovním komisím Legislativní rady vlády a následně byly odeslány do Sbirky zákonů ke zveřejnění. Výjimkou jsou obě nařízení vlády, která jsou stále v procesu vypořádání připomínek a jejich legislativní proces tak zatím nebyl ukončen.

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

Vedle výše uvedených činností NÚKIB v roce 2025 posoudil v meziresortním připomínkovém řízení 190 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 České republiky. NÚKIB je však jedním z gestorů v této oblasti a již na úrovni směrnic má tento předpis předpokládanou vysokou míru propojenosti se zákonem o kybernetické bezpečnosti, 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.

V roce 2025 vstoupily v platnost dva nové unijní předpisy, na jejichž vyjednávání se NÚKIB v posledních letech kontinuálně podílel.

Konkrétně se jednalo o akt o kybernetické solidaritě a cílenou revizi aktu o kybernetické bezpečnosti rozšiřující evropský rámec pro certifikaci kybernetické bezpečnosti o řízení bezpečnostní služby. V souvislosti s aktem o kybernetické bezpečnosti bylo rovněž publikováno první certifikační schéma založené na Common Criteria, čímž bylo umožněno uvést evropský certifikační rámec v život. Akt o kybernetické odolnosti, který vstoupil v platnost na konci roku 2024, získal v roce 2025 konkrétnější obrysy díky přijaté prováděcí legislativě a NÚKIB zahájil jednání o podobě jeho implementace na národní úrovni, především v otázce, kdo bude zastávat jaké role. Česká republika dále k 1. listopadu 2025 plně transponovala směrnici NIS2.

V rámci přípravy na dlouho avizovanou celkovou revizi aktu o kybernetické bezpečnosti ČR prostřednictvím NÚKIB v roli gestora v roce 2025 zveřejnila poziční non-paper a také se zapojila do veřejné konzultace Evropské komise. ČR považuje revizi aktu o kybernetické bezpečnosti za nezbytnou, přičemž zdůrazňuje nutnost jasného vymezení mandátu The European Union Agency for Cybersecurity (dále jen „ENISA“) a zajištění dostatečných zdrojů pro ni. Prioritou je rovněž zefektivnění Evropského rámce pro kybernetickou certifikaci. Klíčové je smysluplné provázání certifikací s požadavky s režimem aktu o kybernetické odolnosti. Zásadním požadavkem ČR bude respektování národních mechanismů pro řízení rizik v dodavatelských řetězcích.

V listopadu 2025 zveřejnila Evropská komise tzv. Digitální simplifikační balíček, který obsahuje legislativní i nelegislativní iniciativy v oblasti datových pravidel, ochrany osobních údajů a kybernetické bezpečnosti. Součástí balíčku je Digitální omnibus, který mj. navrhuje zřízení jednotného rozhraní pro oznamování incidentů – tzv. Single-Entry Point.

V uvedené agendě byl NÚKIB spoluterestem návrhu a má odpovědnost za část hlášení incidentů.

NÚKIB se také zapojil v rámci Skupiny pro spolupráci zřízené směrnicí NIS2 do dokončování práce na souboru opatření pro zvýšení bezpečnosti dodavatelského řetězce ICT (tzv. ICT Supply Chain Security Toolbox).

## 3.10 Komunikace

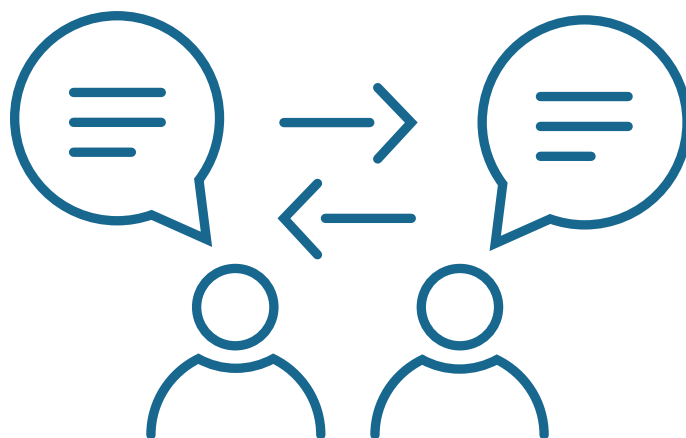
Komunikace NÚKIB se v roce 2025 uskutečňovala především vystoupeními zástupců vedení Úřadu v médiích a prostřednictvím klasické tiskové agendy: odpovídáním na dotazy novinářů, pomocí aktualit a tiskových zpráv na webu a úřadových profilů na sociálních sítích. NÚKIB vydal 82 tiskových zpráv a aktualit, odpověděl na více než 400 dotazů novinářů, publikoval téměř 300 příspěvků na sociálních sítích.

Stále velmi živou platformou reputačně významné expertní komunikace zůstávají tematické konference s přednáškami i panelovými debatami. Specifickou příležitostí k šíření povědomí o Úřadu i jeho agendách jsou pak konference a další akce pořádané úřadem – jmenujme alespoň ty největší: mezinárodní Prague Cyber Security Conference a domácí CYBER\_CON. Mimo těchto akcí proběhl také 2. ročník úzce zaměřené Konference evropských certifikací, zaměřený na akt o kybernetické odolnosti.

O kontinuální zájem novinářů i pořadatelů odborných akcí se postaral stále narůstající význam kyberbezpečnostní problematiky. Novináři i odborná veřejnost se zajímali o útoky a incidenty, bezpečnost dodavatelského řetězce, kyberbezpečnost produktů, relevantní legislativu a její důsledky pro život firem a institucí. Své stálé místo v médiích má obsah zaměřený na velmi praktickou osvětu.

Výraznými momenty zájmu médií pak byly v roce 2025 květnová národní atribuce škodlivé kybernetické kampaně čínské skupiny APT31 proti kritické infrastruktuře státu, dvě varování a účinnost nového zákona o kybernetické bezpečnosti. Všechny tyto milníky byly využity k reaktivní i aktivní komunikaci.

Poslední jmenovaná položka, nový ZKB, byl páteřním tématem komunikace celý rok. Z rámce běžných komunikačních výstupů vybočují podrobné videonávody připravené odbory kontroly a regulace. Tento produkt je cílovou skupinou velmi pozitivně hodnocen.



Dalším větším počinem byla tvorba podcastu NÚKIB CAST informujícího v zatím osmi dílech veřejnost o odborných problematikách s potenciálně širokým dosahem: takovými tématy jsou například certifikace v kybernetické bezpečnosti, aktivity NÚKIB v Národním koordinačním centru výzkumu a vývoje v oblasti kybernetické bezpečnosti; cloudy a další.

Na sociálních sítích nacházela prostor osvěta a vzdělávání v kybernetické bezpečnosti. Zaměstnanci NÚKIB pravidelně informovali o odborných i diplomatických aktivitách zaměstnanců, ale také o volných pozicích na úřadě.

K povzbuzení zájmu o úřadové profily bylo využito příležitostné využívání virálních postů. Tím postupně došlo k rozšiřování okruhu sledujících a reagujících čtenářů. Samostatnou komunikací na sociálních sítích rozběhlo Národní koordinační centrum, pokračoval profil oddělení vzdělávání i odboru vládní CERT.

## 3.11 Spolupráce, mezinárodní spolupráce

### Projekt Kyberliga

Projekt Kyberliga realizovaný pod záštitou a ve spolupráci s NÚKIB cílí na vytvoření komunity dobrovolníků složené z expertů a expertek na kybernetickou bezpečnost. Hlavním cílem Kyberligy je podpora kybernetické bezpečnosti ČR a poskytování platformy pro bezpečnou, důvěryhodnou a aktivní komunitu, která bude sdílet nejlepší praxi, budovat know-how a podporovat růst a rozvoj na osobní i systémové úrovni. V roce 2025 bylo finalizováno konceptuální uchopení Kyberligy, vč. nastavení jejích pravidel a procesů a konzultace nastavení s možnými členy. V průběhu podzimu došlo ke spuštění pilotního provozu s malým počtem členů s důrazem na ověření praktického fungování.

### Prague Cyber Security Conference 2025

V roce 2025 NÚKIB pořádá již šestý ročník mezinárodní Prague Cyber Security Conference (dále jen „PCSC“), který opět propojil vládní představitele, odborníky i zástupce soukromého sektoru z desítek zemí světa. Hlavními tématy pod hlavičkou „Invisible frontlines“ byly neviditelné fronty kybernetických konfliktů, posilování odolnosti kritické infrastruktury, ochrana energetických a telekomunikačních sítí, dopady umělé inteligence a význam mezinárodní spolupráce v boji s kybernetickými hrozbami.

### Konference CYBER\_CON 2025

V roce 2025 proběhl již 11. ročník konference CYBER\_CON, kterou ve spolupráci s partnery ze skoukromého sektoru organizuje NÚKIB. Jedná se o stěžejní národní platformu k propojení české komunity kybernetické bezpečnosti z veřejného, soukromého i akademického sektoru. Dvoudenní program probíhal paralelně na třech scénách, kde se vystřídalo celkem více než 80 řečníků. V hlavním sále Rotundy brněnského Výstaviště zaznělo 21 odborných příspěvků a proběhly dva diskusní panely, včetně debaty zástupců poslaneckých klubů o budoucnosti kybernetické bezpečnosti z pohledu státu. V přílehlých sálech se konalo 9 workshopů, kde si účastníci vyzkoušeli praktické nástroje k řešení kybernetických útoků či analýze síťového provozu, a okolní prostory nabídly přednáškovou a diskusní zónu nebo prezentační a konzultační stánky NÚKIB a partnerů konference.



V květnu 2025 také upozornil NÚKIB spolu s českými zpravodajskými službami a partnery z United States of America (dále jen „USA“), Spojeného království, Německa, Polska, Austrálie, Kanady, Dánska, Estonska, Francie a Nizozemska na dlouhodobou ruskou kybernetickou kampaň cílenou na subjekty podporující Ukrajinu.

V roce 2025 měl NÚKIB 7 zaměstnanců v zahraničí, tzv. kyberatašů a národních experty, a to ve Washingtonu, Tel Avivu, Canbeře, Tallinnu (NATO CCD COE) a Bruselu (při EU, NATO a v ENISA), což umožnilo efektivně budovat nadstandardní spolupráci s klíčovými partnery NÚKIB.

### EU

V roce 2025 se NÚKIB ve spolupráci s Ministerstvem zdravotnictví na jednáních Rady EU významně podílel na finalizaci Evropského akčního plánu pro kybernetickou bezpečnost nemocnic a poskytovatelů zdravotní péče, zaměřeného na posílení odolnosti sektoru vůči kybernetickým hrozbám, zejména ransomwaru.

V červnu 2025 Rada EU přijala nový rámec pro kybernetické krizové řízení ve formě doporučení Rady o plánu EU pro řešení kybernetických bezpečnostních krizí – tzv. Cyber Blueprint, který aktualizuje a nahrazuje původní doporučení Komise z roku 2017. Cyber Blueprint stanovuje rámec pro koordinovanou reakci EU na kybernetické incidenty velkého rozsahu, včetně jasného rozdělení rolí relevantních kyberbezpečnostních aktérů na unijní úrovni či koordinace s dalšími unijními mechanismy krizového řízení a spolupráce s NATO. Tento nový rámec NÚKIB vyjednával.

I v roce 2025 se NÚKIB aktivně zapojil do aktivit ENISA prostřednictvím správní rady, sítě styčných důstojníků a vyslaného národního experta. Pokračovaly aktivity v rámci projektu podpůrných služeb (ENISA Support Action), díky kterým byly vybraným subjektům poskytovány bezplatné služby penetračního testování, kybernetických cvičení a pomoci při analýze rizik. Projekt, spuštěný v roce 2022 jako pilotní iniciativa pro subjekty regulované směrnici NIS a NIS2, se postupně přesune pod tzv. rezervu EU pro kybernetickou bezpečnost, která byla v roce 2025 poprvé využita k podpoře Moldavska. Mechanismus rezervy EU zakotvuje již zmíněný Akt o kybernetické solidaritě a umožňuje rychlou, koordinovanou a přeshraniční podporu členským státům EU, ale i přidruženým zemím programu Digitální Evropa.

V červnu 2025 zveřejnila Evropská komise návrh nařízení o bezpečnosti, odolnosti a udržitelnosti kosmických činností v Unii (EU Kosmický akt), jehož součástí je i důraz na kybernetickou bezpečnost. NÚKIB spolupracuje s národními i mezinárodními partnery při jeho vyjednávání, které ve druhé polovině roku probíhalo na půdě Rady EU. V roce 2025 se vládní CERT s podporou dalších celků organizace aktivně podíleli na technické spolupráci v rámci tzv. CSIRTs Network (dále jen „CNW“), která sdružuje vládní a národní CERT/CSIRT týmy členských států EU. V CNW dochází ke sdílení technických informací a spolupráci při řešení kyberbezpečnostních incidentů a hrozeb.

## NATO

I v roce 2025 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.

V dubnu uspořádal NÚKIB cvičení zaměřené na schopnost podpory při kybernetických incidentech na dálku (VCISC). Cílem bylo prověřit připravenost spojenců poskytovat si vzájemnou pomoc prostřednictvím mechanismu VCISC při vážných kybernetických incidentech a otestovat koordinaci a sdílení informací mezi aliančními partnery.

Během roku 2025 NÚKIB inicioval a řídil jednání národních stakeholderů věnující se přípravě na implementaci NATO Integrated Cyber Defence Centre, jehož vznik byl oznámen v roce 2024.

NÚKIB se podílel také na posilování NATO zapojením do interního hodnocení fungování Aliance v oblasti kybernetické bezpečnosti a obrany.

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

## Organizace spojených národů (dále jen „OSN“)

NÚKIB se i v roce 2025 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. V říjnu 2025 se pak ČR připojila k Úmluvě OSN proti kyberkriminalitě, dokumentu představujícímu vůbec první celosvětový právně závazný rámec pro spolupráci při vyšetřování a stíhání trestné činnosti v digitálním prostoru.

## Organizace pro bezpečnost a spolupráci v Evropě (dále jen „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.

## Bilaterální spolupráce

V souladu s NSKB posiloval NÚKIB stávající partnerství zejména v regionech a zemích s přítomností českých kyberatašů. 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 březnu 2025 došlo v rámci PCSC 2025 k podpisu memoranda o spolupráci mezi NÚKIB a ukrajinským State Service of Special Communications and Information Protection of Ukraine, jehož obsahem je zejména spolupráce na výměně informací a sdílení zkušeností a dobré praxe mj. v oblasti řešení incidentů, analýzy hrozeb a zvyšování úrovně kybernetické bezpečnosti kritické infrastruktury. V návaznosti na toto memorandum NÚKIB uspořádal workshop, kde spolu s dalšími zahraničními partnery sdílel své zkušenosti z oblasti implementace požadavků směrnice NIS2, unijní spolupráce v oblasti zvládnutí kybernetických bezpečnostních incidentů nebo řízení kybernetických krizí.

## Austrálie a Indo-Pacifik

Působení kyberataše pro Indo-Pacifik se sídlem v australské Canbeře přispělo k vytváření nových a posilování stávajících bilaterálních vztahů v regionu.

NÚKIB se připojil k několika australským technickým dokumentům (zaměřeným na základy moderní obranyschopné infrastruktury, bezpečnost hraničních síťových prvků nebo využívání platform Security Information and Event Management a Security Orchestration, Automation and Response), naopak australské partnery podpořili českou atribuci škodlivých aktivit skupině APT31. V roce 2025 se také uskutečnila první oficiální návštěva vedení NÚKIB v Austrálii a jednání s Australským centrem pro kybernetickou bezpečnost (Australian Signals Directorate). Tato mise potvrdila rostoucí význam česko-australského partnerství v kybernetické bezpečnosti.

NÚKIB pokračoval v prohlubování spolupráce s klíčovými partnery v Japonsku, kde se diskutovala možnost formálního stvrzení spolupráce uzavřením memoranda o spolupráci, Korejské republice, kde vedení NÚKIB převzalo štafetu organizace NATO Cyber Champions Summit pro rok 2026, ale i Singapuru nebo Taiwanu. Významnou událostí byla účast technického týmu NÚKIB na mezinárodním kybernetickém cvičení Allied Power Exercise, kde ČR reprezentovali experti z vládního CERT.

## USA a Kanada

Rok 2025 se nesl především ve znamení nástupu nové americké administrativy a očekávání ohledně pokračování blízké spolupráce USA s evropskými partnery. Delegace NÚKIB absolvovala sérii jednání se zástupci amerických bezpečnostních institucí, včetně Národní bezpečnostní rady Bílého domu a Zvláštní komise pro strategické soupeření mezi USA a Čínou při Sněmovně reprezentantů, na kterých si obě strany potvrdily vůli i nadále úzce spolupracovat a vyměňovat si zkušenosti i informace v oblasti boje proti kybernetickým hrozbám. Zástupci NÚKIB se účastnili RSA Conference, nejvýznamnější kyberbezpečnostní konference na světě, a po boku špiček americké administrativy a mezinárodních partnerů vystoupili na International Cyber Security Forum. Dobré vztahy obou zemí stvrdilo i jednání delegace českého MZV v USA ke konci roku.

Ke konci roku se NÚKIB spolu s dalšími národními partnery připojil k upozornění amerického Federálního úřadu pro vyšetřování na kybernetické útoky proruských hacktivistických skupin mířených na kritickou infrastrukturu.

I v roce 2025 NÚKIB prohluboval spolupráci s Kanadou, která v současné geopolitické situaci klade daleko větší důraz na udržování dobrých vztahů se svými evropskými partnery. Vedení NÚKIB zde jednalo s federálními úřady, soukromým sektorem i akademickou sférou o rozvoji spolupráce v oblasti posílení sdílení informací a rozvoji kybernetické bezpečnosti obou států. V rámci programu PROPED MZV ČR došlo i k diskusím zaměřeným na spolupráci v oblasti satelitní bezpečnosti.

## Izrael

Spolupráce s izraelskými partnery je nadále podpořena přítomností kyberataše přímo v regionu. I v roce 2025 pokračoval strukturovaný dialog ve všech oblastech kybernetické bezpečnosti, zejména pak v oblasti regulace. Zástupci NÚKIB se účastnili prestižní konference Cyber Week a AI Week a během své návštěvy jednali jak s Israel National Cyber Directorate, tak se soukromými firmami. Izraelští partneři jsou otevření sdílení svých unikátních zkušeností, stejně jako pokročilých nástrojů a vybavení, které jsou NÚKIB v českých podmínkách jen obtížně dostupné.

## Rozvojová spolupráce a budování kybernetických kapacit

NÚKIB se v roce 2025 zapojil do mnoha rozvojových projektů a sdílel své zkušenosti zejména s partnery v regionu západního Balkánu a Indo-Pacifiku, ale menší měrou také v Africe nebo Asii. Západní Balkán však i nadále zůstává prioritním regionem pro směřování rozvojové pomoci NÚKIB. Na rozvojových aktivitách NÚKIB i nadále spolupracuje s mezinárodními organizacemi (zejména NATO a EU) a klíčovými státy s obdobnými postoji, včetně USA a Estonska.

NÚKIB se stejně jako v loňském roce aktivně podílel na rozvojových projektech CyberVAC MZV. Za účasti zástupců NÚKIB se realizoval projekt v Jordánsku, NÚKIB sám pak navrhl a ve spolupráci s dalšími národními partnery zrealizoval projekt zaměřený na posílení spolupráce s partnery v geopoliticky exponovaném Bhútánu.

## 3.12 Ekonomické zabezpečení

### 3.12.1 Příjmy

Schválený rozpočet celkových příjmů Úřadu byl v roce 2025 ve výši 29 438 075 Kč. Tvořily ho daňové příjmy, nedaňové příjmy a přijaté transfery. Významnou součástí přijatých transferů jsou neinvestiční a investiční transfery ze zahraničí z projektů Czech National Quantum Communication Infrastructure (dále jen „CZQCI“) a Portálu NÚKIB z Národního plánu obnovy.



#### Přehled plnění rozpočtu příjmů v roce 2025 (vyjádření v tis. Kč)

|                                                                                   |           |
|-----------------------------------------------------------------------------------|-----------|
| Příjmy celkem                                                                     | 21 115,83 |
| Příjem ze správních a soudních poplatků                                           | 9,00      |
| Přijaté sankční platby                                                            | 610,00    |
| Ostatní nedaňové příjmy                                                           | 277,08    |
| Neinvestiční převody z vlastních fondů a ve vztahu k útvarům bez právní osobnosti | 361,24    |
| Neinvestiční přijaté transfery ze zahraničí                                       | 1 318,59  |
| Investiční přijaté transfery od rozpočtů ústřední úrovně                          | 0,00      |
| Investiční přijaté transfery ze zahraničí                                         | 18 539,92 |

### 3.12.2 Výdaje

Schválený rozpočet celkových výdajů Úřadu byl v roce 2025 ve výši 678 826 085 Kč.

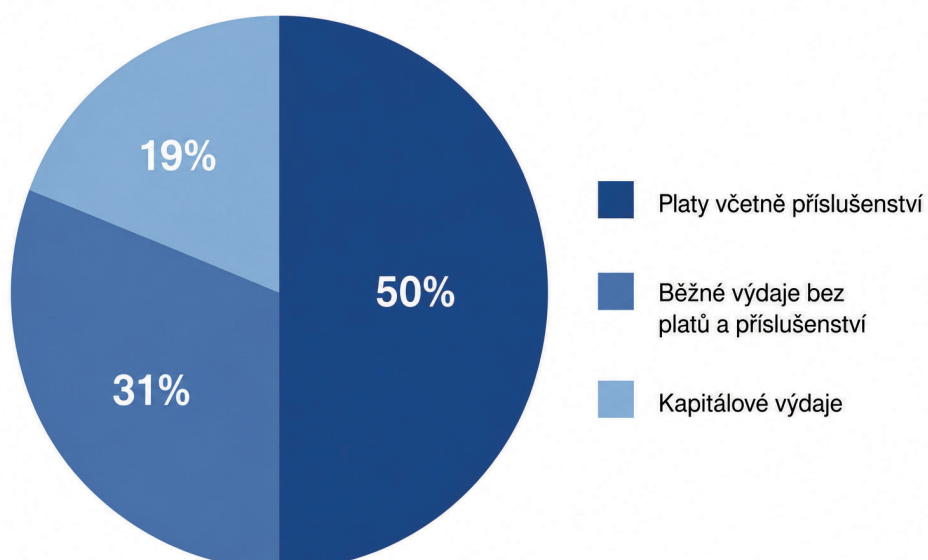
Konečný rozpočet celkových výdajů kapitoly za rok 2025, včetně zapojených nároků z nespotřebovaných výdajů ve výši 126 175 920,53 Kč a zapojených prostředků rezervního fondu ve výši 330 000,00 Kč byl v objemu 794 845 086,53 Kč. Čerpání konečného rozpočtu bylo v relativním vyjádření (čerpání vůči konečnému rozpočtu) na 86,9 %, v absolutním vyjádření ve výši 691 001 636,92 Kč.

Konečný rozpočet výdajů kapitoly bez prostředků EU/FM za rok 2025 byl v objemu 702 416 713,23 Kč. Čerpání konečného rozpočtu bylo v relativním vyjádření na 90,6 %, v absolutním vyjádření ve výši 636 149 136,52 Kč.

## Základní přehled plnění rozpočtu výdajů v roce 2025 (vyjádření v tis. Kč)

|                                                      | Schválený rozpočet | Rozpočet po změnách | Konečný rozpočet  | Výsledné čerpání rozpočtu | Čerpání rozpočtu v % vyjádření |
|------------------------------------------------------|--------------------|---------------------|-------------------|---------------------------|--------------------------------|
| <b>Výdaje celkem</b>                                 | <b>678 826,09</b>  | <b>672 740,68</b>   | <b>794 845,09</b> | <b>691 001,64</b>         | <b>86,9 %</b>                  |
| SR část                                              | 649 863,01         | 638 777,61          | 702 416,71        | 636 149,14                | 90,6 %                         |
| EU část                                              | 28 963,08          | 33 963,08           | 92 428,37         | 54 852,50                 | 59,3 %                         |
| <b>Běžné výdaje</b>                                  | <b>561 197,16</b>  | <b>566 889,27</b>   | <b>585 238,08</b> | <b>562 278,83</b>         | <b>96,1 %</b>                  |
| SR část                                              | 556 148,41         | 553 962,19          | 560 546,76        | 547 577,48                | 97,7 %                         |
| EU část                                              | 5 048,76           | 12 927,08           | 24 691,32         | 14 701,35                 | 59,5 %                         |
| <b>z toho platy včetně příslušenství</b>             | <b>349 371,65</b>  | <b>352 684,34</b>   | <b>352 336,11</b> | <b>348 426,36</b>         | <b>98,9 %</b>                  |
| SR část                                              | 349 371,65         | 350 184,34          | 347 566,33        | 343 674,54                | 98,9 %                         |
| EU část                                              | 0,00               | 2 500,00            | 4 769,78          | 4 751,82                  | 99,6 %                         |
| <b>z toho běžné výdaje bez platů a příslušenství</b> | <b>211 825,51</b>  | <b>214 204,94</b>   | <b>232 901,98</b> | <b>213 852,48</b>         | <b>91,8 %</b>                  |
| SR část                                              | 206 776,75         | 203 777,86          | 212 980,44        | 203 902,95                | 95,7 %                         |
| EU část                                              | 5 048,76           | 10 427,08           | 19 921,54         | 9 949,53                  | 49,9 %                         |
| <b>Kapitálové výdaje</b>                             | <b>117 628,92</b>  | <b>105 851,41</b>   | <b>209 607,00</b> | <b>128 722,81</b>         | <b>61,4 %</b>                  |
| SR část                                              | 93 714,60          | 84 815,41           | 141 869,95        | 88 571,65                 | 62,4 %                         |
| EU část                                              | 23 914,32          | 21 036,00           | 67 737,05         | 40 151,15                 | 59,3 %                         |

## Podíl jednotlivých složek na celkových výdajích v roce 2025



### 3.12.3 Projekty spolufinancované EU

#### 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)**

Účelem projektu je realizace technických bezpečnostních opatření podle zákona o kybernetické bezpečnosti a výkon státní správy v oblasti bezpečnosti informačních a komunikačních systémů.

#### Nástroj 16700 – Program digitální Evropa

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

Projekt byl realizován v období od 1. listopadu 2023 do 31. prosince 2025 a jeho cílem bylo 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.

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

Projekt je realizován v období 1. prosince 2023 až 28. února 2027 a podporuje budování testovacích a certifikačních schopností v České republice, a to skrze 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).

#### Nástroj 17011 – Národní plán obnovy – Komponenta 1.1 Digitální služby občanům a firmám, investice č. 1 Digitální služby pro koncové uživatele

##### **Projekt: Portál NÚKIB (reg. č. CZ.31.1.0/0.0/0.0/24\_158/0011581)**

Cílem projektu je vytvoření jednotného informačního systému, který zajistí všechny funkce nutné pro naplnění legislativy.

#### Nástroj 17014 – Národní plán obnovy – grant Digitální ekonomika a společnost, inovativní start-upy a nové technologie

##### **Projekt: CZQCI (č. 101091684 – CZQCI)**

Projekt je realizován v období 1. března 2023 až 31. srpna 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 k převzetí role subjektu implementace a naplnění administrativních úkonů pro zajištění zprostředkování dotace z Národního plánu obnovy řešiteli projektu CZQCI (CyberSecurity Hub, z. ú.).

### 3.13 Personální zabezpečení

#### Základní přehled ke dni 31. 12. 2025

|                                                                                                 |         |
|-------------------------------------------------------------------------------------------------|---------|
| Evidenční stav zaměstnanců na systemizovaných pracovních místech k 31. 12. ve fyzických počtech | 385     |
| Ukončení pracovních poměrů v průběhu roku 2025                                                  | 49      |
| Nástupy do pracovního poměru v průběhu roku 2025                                                | 55      |
| Návraty z mateřské dovolené, z rodičovské dovolené a neplaceného volna v průběhu roku 2025      | 9       |
| Odchody na mateřskou či rodičovskou dovolenou v průběhu roku 2025                               | 7       |
| Fluktuace v roce 2025                                                                           | 12,98 % |

V roce 2025 NÚKIB zaměstnával osoby se zdravotním postižením podílem ve výši 6,09 osoby a odebíral výrobky a služby od chráněných trhů v přepočtu zaměstnání 9,51 osob.

#### 3.14 Interní audit a vnitřní kontrola

Realizované interní audity vycházely ze schváleného střednědobého a ročního plánu interního auditu dle zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole).

Nebyly zjištěny nedostatky a rizika, které by měly dopad na nesplnění rozhodujících úkolů a cílů NÚKIB a auditní činnost je zajištěna přiměřeným a účinným systémem řídicí kontroly.

Výsledky auditů 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 auditech nebyly zjištěny skutečnosti, které by nasvědčovaly neoprávněnému nakládání s finančními prostředky, ani podezření na podvodné či korupční jednání.

#### 3.15 Veřejnosprávní kontrola

Veřejnosprávní kontrola je vykonávána v souvislosti s rolí NÚKIB jako poskytovatele veřejné finanční podpory, zejména v rámci činnosti Národního koordinačního centra a zprostředkovatele dotace projektu CZQCI – vybudování české národní kvantové komunikační infrastruktury.

V roce 2025 bylo provedeno 8 průběžných a 7 následných veřejnosprávních kontrol příjemců veřejné finanční podpory z výzev administrovaných NÚKIB, při kterých nebyly zjištěny skutečnosti, které by naplňovaly znaky porušení rozpočtové kázně.

Získané poznatky byly NÚKIB využity k metodickému zpřesnění podmínek poskytování veřejné finanční podpory v navazujících dotačních výzvách.



## 4. Seznam použitých zkratek

|              |                                                                                                                                                                                       |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AP           | Akční plán                                                                                                                                                                            |
| APT31        | Advanced Persistent Threat (státem podporovaná hackerská skupina)                                                                                                                     |
| BIS          | Bezpečnostní informační služba                                                                                                                                                        |
| BRS          | Bezpečnostní rada státu                                                                                                                                                               |
| CERT         | Computer Emergency Response Team                                                                                                                                                      |
| CNW          | CSIRTs Network                                                                                                                                                                        |
| CSIRT        | Computer Security Incident Response Team                                                                                                                                              |
| CVD          | Coordinated Vulnerability Disclosure (koordinované zveřejňování zranitelností)                                                                                                        |
| CZQCI        | Czech National Quantum Communication Infrastructure                                                                                                                                   |
| ČR           | Česká republika                                                                                                                                                                       |
| ENISA        | The European Union Agency for Cybersecurity                                                                                                                                           |
| EU           | Evropská unie                                                                                                                                                                         |
| EUSPA        | European Agency For Space Program (Agentura Evropské unie pro Kosmický program)                                                                                                       |
| GOVSATCOM    | Governmental Satellite Communications                                                                                                                                                 |
| GRON         | Galileo Robust Operation Network                                                                                                                                                      |
| ICT          | Information and Communication Technologies (informační a komunikační technologie)                                                                                                     |
| IS           | Informační systém                                                                                                                                                                     |
| LANPCS       | Local Area Network Personal Computer System                                                                                                                                           |
| MO           | Ministerstvo obrany                                                                                                                                                                   |
| MPO          | Ministerstvo průmyslu a obchodu                                                                                                                                                       |
| MU           | Masarykova univerzita v Brně                                                                                                                                                          |
| MV           | Ministerstvo vnitra                                                                                                                                                                   |
| MZV          | Ministerstvo zahraničních věcí                                                                                                                                                        |
| NATO CCD COE | Cooperative Cyber Defence Centre of Excellence (NATO Centrum excelence pro kybernetickou obranu)                                                                                      |
| NATO         | North Atlantic Treaty Organization (Severoatlantická aliance)                                                                                                                         |
| NBÚ          | Národní bezpečnostní úřad                                                                                                                                                             |
| NIS          | Network and Information Security (směrnice Evropského parlamentu a Rady Evropské unie o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii) |
| NIS2         | Network and Information Security 2 (směrnice Evropského parlamentu a Rady Evropské unie o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii)              |
| NP KOUÍ      | Národní politika kryptografické ochrany utajovaných informací                                                                                                                         |
| NSKB         | Národní strategie kybernetické bezpečnosti                                                                                                                                            |
| NÚKIB        | Národní úřad pro kybernetickou a informační bezpečnost                                                                                                                                |
| OBSE         | Organizace pro bezpečnost a spolupráci v Evropě                                                                                                                                       |
| OSN          | Organizace spojených národů                                                                                                                                                           |
| PCSC         | Prague Cyber Security Conference                                                                                                                                                      |
| POCP         | Point of Contact Platform (platforma kontaktních míst systému Galileo)                                                                                                                |
| PRS          | Public Regulated Service (Veřejně regulovaná služba Evropského programu družicové navigace Galileo)                                                                                   |
| PSP ČR       | Poslanecká sněmovna Parlamentu České republiky                                                                                                                                        |
| TEMPEST      | Telecommunication Electronics Materials Protected from Emanating Spurious Transmissions                                                                                               |
| USA          | United States of America (Spojené státy americké)                                                                                                                                     |
| VCISC        | Virtual Cyber Incident Support Capability                                                                                                                                             |
| VUT          | Vysoké učení technické v Brně                                                                                                                                                         |
| VZ           | Vojenské zpravodajství                                                                                                                                                                |
| ZKB          | do 31.10.2025 zákon č. 181/2014 Sb., o kybernetické bezpečnosti, od 1.11.2025 zákon č. 264/2025 Sb., o kybernetické bezpečnosti                                                       |
| ZoOUI        | zákon č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti                                                                                                    |

