NÁRODNÝ
BEZPEČNOSTNÝ
ÚRAD

Konsolidovaná výročná správa za rok 2025

NÁRODNÝ
BEZPEČNOSTNÝ
ÚRAD

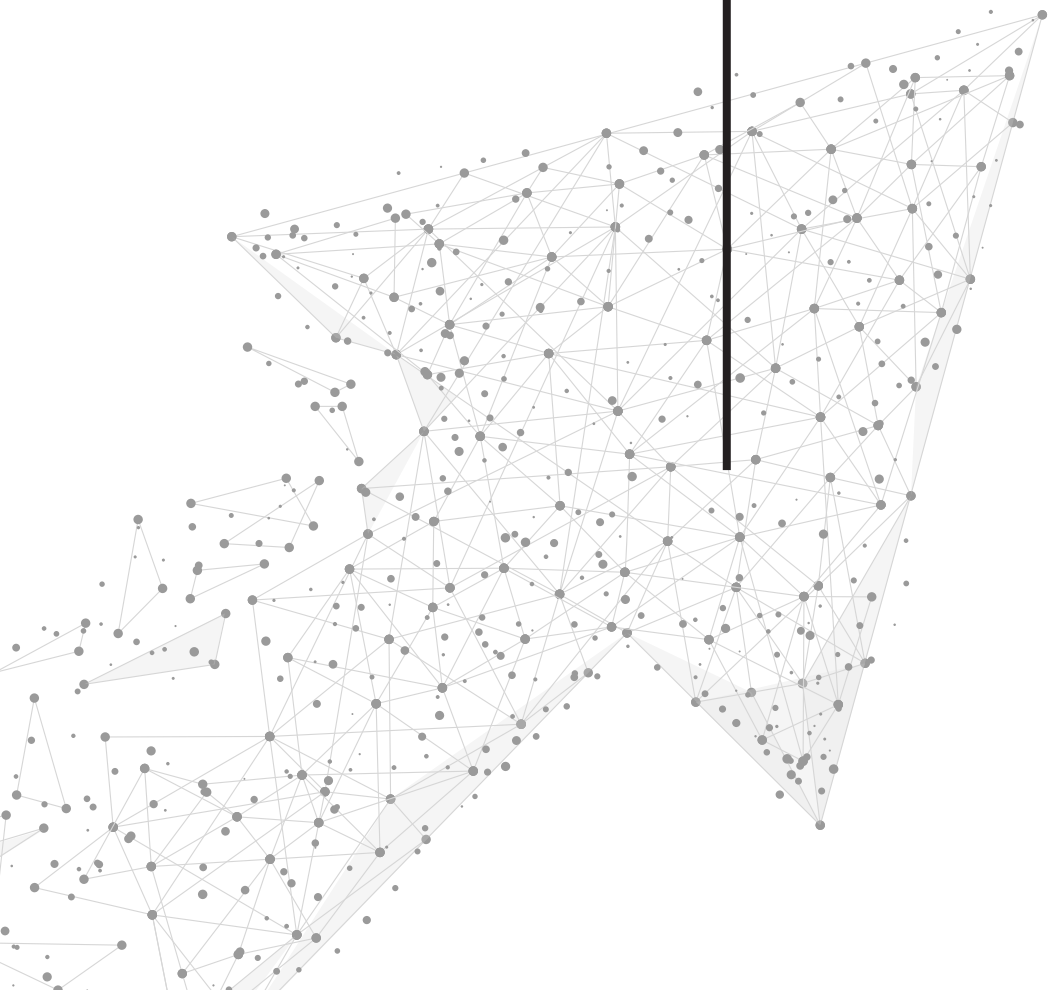
Konsolidovaná výročná správa za rok 2025

OBSAH

IDENTIFIKÁCIA ORGANIZÁCIE	4
ĽUDSKÉ ZDROJE	11
LEGISLATÍVA	16
OCHRANA UTAJOVANÝCH SKUTOČNOSTÍ	20
ŠIFROVÁ OCHRANA INFORMÁCIÍ	26
DÔVERYHODNÉ SLUŽBY	28
KYBERNETICKÁ BEZPEČNOSŤ	32
MEDZINÁRODNÁ SPOLUPRÁCA	47
HOSPODÁRENIE	62
KONTROLA A AUDIT	67
PRIORITY NA ROK 2026	71

01.

IDENTIFIKÁCIA ORGANIZÁCIE



Národný bezpečnostný úrad (NBÚ) zodpovedá za tvorbu a realizáciu štátnej politiky pre oblasti ochrany utajovaných skutočností, kybernetickej bezpečnosti, šifrovej služby a dôveryhodných služieb. V oblasti ochrany utajovaných skutočností vykonáva bezpečnostné previerky fyzických osôb a podnikateľov, vyjadruje sa o navrhovaných osobách podľa medzinárodných zmlúv, ktorými je Slovenská republika viazaná a vedie evidencie súvisiace s ochranou utajovaných skutočností.

Certifikuje komunikačné a informačné systémy pre manipuláciu s utajovanými skutočnosťami, vydáva súhlas s autorizáciou štátneho orgánu alebo autorizáciou podnikateľa na certifikáciu technických prostriedkov a vykonávanie overovania zhody mechanických zábranných prostriedkov a technických zabezpečovacích prostriedkov s bezpečnostnými štandardami, vykonáva certifikáciu technických, systémových, mechanických zábranných a technických zabezpečovacích prostriedkov.

Úrad vykonáva posudzovanie podmienok u podnikateľov a štátnych orgánov vrátane posudzovania zabezpečenia ochrany vymieňaných utajovaných skutočností a posudzovania podmienok na ochranu pred nežiaducim elektromagnetickým vyžarovaním technických prostriedkov a prostriedkov šifrovej ochrany informácií.

Zabezpečuje správu a realizáciu prevádzky zverených informačných systémov úradu vrátane správy používateľských účtov, zabezpečuje správu a prevádzku systémov utajovaného vládneho a utajovaného zahraničného spojenia a vykonáva bezpečnostný dohľad sieťových a aplikačných parametrov komunikačných a informačných systémov na ochranu utajovaných skutočností.

Vlastnou kontrolnou činnosťou úrad overuje podmienky zabezpečenia ochrany utajovaných skutočností v štátnych a samosprávnych orgánoch aj u podnikateľov a vydáva metodické usmernenia k jednotlivým aspektom bezpečnosti utajovaných skutočností.

Realizuje aj aktivity posilňujúce bezpečnostné povedomie a vykonáva skúšku bezpečnostného zamestnanca.

Pri medzinárodnej výmene utajovaných skutočností plní úrad funkciu centrálneho registra výmeny utajovaných skutočností v Slovenskej republike a podieľa sa na ochrane zahraničných informácií.

Na úseku regulácie a metodiky úrad vydáva bezpečnostné štandardy, stanoviská a metodiky k všeobecne záväzným právnym predpisom a dokumentom, ktoré patria do pôsobnosti úradu, pripravuje návrhy všeobecne záväzných právnych predpisov do legislatívneho procesu, pripomienkuje a vypracúva stanoviská k návrhom legislatívnych materiálov v rámci medzirezortného pripomienkového konania.

Metodické usmernenia úrad poskytuje štátnym orgánom, podnikateľom i fyzickým osobám vo všetkých oblastiach jeho pôsobnosti. Úrad zverejňuje anonymizované metodiky a odborné stanoviská aj na webovom sídle úradu.

V oblasti šifrovej ochrany informácií úrad plní úlohy ústredného šifrového orgánu Slovenskej republiky. Vykonáva certifikáciu jej prostriedkov, vydáva bezpečnostné štandardy a koordinuje výskum a vývoj prostriedkov šifrovej ochrany.

V neposlednom rade plní úlohu garanta národnej autority v medzinárodnej spolupráci a zabezpečuje funkciu Národnej distribučnej autority, ktorá je vstupným a kontaktným bodom Slovenskej republiky pri výmene a distribúcii prostriedkov šifrovej ochrany informácií a šifrových materiálov prostredníctvom Národnej distribučnej autority a plní úlohy Národnej distribučnej autority pre distribúciu NATO a EÚ COMSEC materiálu. V oblasti dôveryhodných služieb plní úrad úlohy orgánu dohľadu.

Realizuje úlohy súvisiace s udeľovaním a odňatím kvalifikovaného štatútu pre služby poskytované kvalifikovaným poskytovateľom dôveryhodných služieb, ktorý zverejňuje v dôveryhodnom zozname s informáciami o dôveryhodných službách.

Ďalej zastrešuje certifikáciu zariadení na vyhotovovanie kvalifikovaných elektronických podpisov a kvalifikovaných elektronických pečatí, vytvára, vedie a zverejňuje zoznam oprávnení na účel vydávania mandátnych certifikátov.

Úrad ďalej prevádzkuje Koreňovú certifikačnú autoritu Slovenskej republiky, ktorá vedie databázu exspirovaných kvalifikovaných certifikátov poskytovateľmi, ktorí sú pod dohľadom úradu a o ktorých stave platnosti poskytuje neobmedzene dlho informáciu o ich platnosti počas ich intervalu použitia, umožňuje vydať kvalifikovaným poskytovateľom dôveryhodných služieb certifikáty verejných kľúčov.

V oblasti kybernetickej bezpečnosti je úrad Národnou autoritou pre kybernetickú bezpečnosť. Riadi a koordinuje výkon štátnej správy v oblasti kybernetickej bezpečnosti, určuje štandardy a vydáva politiku správania sa v kybernetickom priestore. Úrad je vnútroštátnym orgánom pre certifikáciu kybernetickej bezpečnosti podľa európskych schém certifikácie kybernetickej bezpečnosti. Pre úroveň záruky „vysoká“ je jediným certifikačným orgánom podľa príslušných schém.

Úrad je hlavným kontaktným bodom pre zahraničie v oblasti kybernetickej bezpečnosti, spolupracuje s ústrednými orgánmi, prevádzkovateľmi základných služieb a poskytovateľmi digitálnych služieb, akredituje jednotky CSIRT a spolupracuje s analytickými bezpečnostnými pracoviskami pre účely výmeny a zdieľania informácií o bezpečnostných incidentoch.

KĽÚČOVÉ PRÁVNE PREDPISY

Zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, súvisiace všeobecne záväzné právne predpisy a platné štandardy
(ďalej len „zákon o ochrane utajovaných skutočností")

Zákon č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách) v znení neskorších predpisov, súvisiace všeobecne záväzné právne predpisy a právne predpisy Európskej únie
(ďalej len „zákon o dôveryhodných službách")

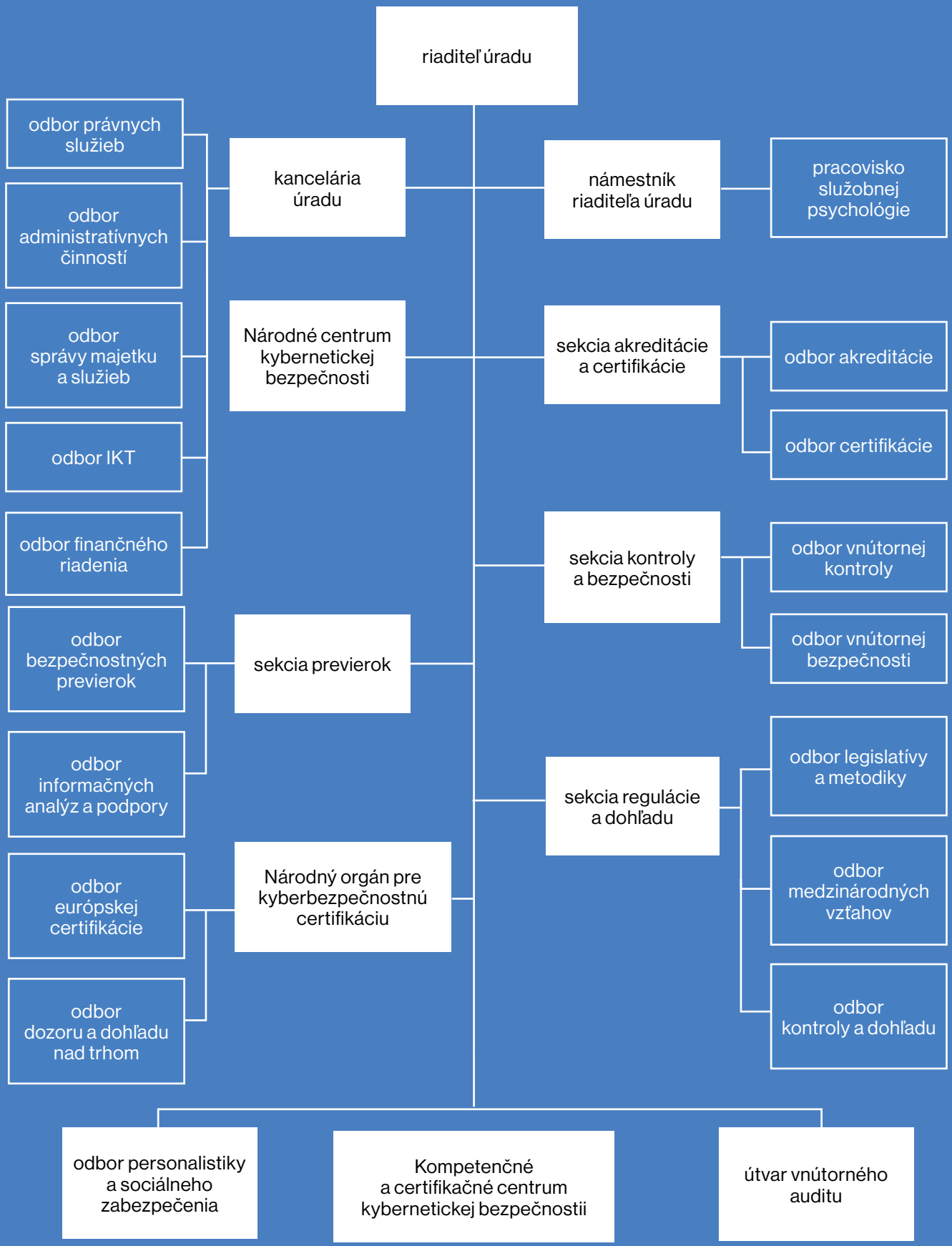
Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, súvisiace všeobecne záväzné právne predpisy, medzinárodné právne predpisy a právne predpisy Európskej únie
(ďalej len „zákon o kybernetickej bezpečnosti")

VEDENIE ÚRADU

Na čele Národného bezpečnostného úradu stojí riaditeľ, ktorý zodpovedá za jeho činnosť. Riadi a reprezentuje úrad navonok. Rozhoduje o spôsobe realizácie hlavných úloh úradu, schvaľuje interné právne predpisy, rozhoduje o vnútornom organizačnom usporiadaní a o personálnych otázkach jeho príslušníkov a zamestnancov. Zastrešuje medzirezortnú spoluprácu a je trvale prizývaným členom Bezpečnostnej rady Slovenskej republiky.

Určuje zásady medzinárodnej spolupráce úradu a v súlade so zahraničnopolitickými prioritami vlády Slovenskej republiky podporuje a rozvíja partnerstvá s inštitúciami zahraničných štátov a medzinárodných organizácií. Riaditeľa v čase jeho neprítomnosti, vo vyhradenom rozsahu, zastupuje námestník riaditeľa úradu, ktorý zodpovedá aj za koordináciu činností útvarov.

ORGANIZAČNÉ ČLENENIE



ÚTVARY ÚRADU

Kancelária úradu

Koordinuje činnosť útvarov úradu, zabezpečuje a vykonáva základné administratívne a organizačné činnosti súvisiace s riadením a činnosťou úradu, zabezpečuje legislatívne a právne záležitosti úradu. Zabezpečuje projektové a programové riadenie v podmienkach úradu.

Zároveň zabezpečuje správu a prevádzku zverených informačných systémov úradu, vrátane systémov utajovaného vládneho a zahraničného spojenia. Vykonáva dohľad nad bezpečnosťou sieťových a aplikačných parametrov komunikačných a informačných systémov, a to aj v oblasti ochrany utajovaných skutočností. Súčasne spolupracuje s analytickými bezpečnostnými pracoviskami pri zdieľaní informácií o bezpečnostných incidentoch.

Sekcia previerok

Vykonáva previerky fyzických a právnických osôb. Okrem osvedčení a potvrdení, ktoré umožňujú prístup k národným utajovaným skutočnostiam, zabezpečuje vydávanie certifikátov o bezpečnostnej previerke fyzickej osoby a certifikátov podnikateľa o priemyselnej bezpečnosti pre oboznamovanie sa s utajovanými skutočnosťami NATO a EÚ a vyjadruje sa o navrhovaných osobách podľa medzinárodných zmlúv, ktorými je Slovenská republika viazaná. Ďalej organizačne pripravuje a realizuje skúšky bezpečnostných zamestnancov na úseku ochrany utajovaných skutočností.

Sekcia regulácie a dohľadu

Sekcia regulácie a dohľadu je vecným útvarom úradu v oblasti ochrany utajovaných skutočností, šifrovej ochrany informácií, kybernetickej bezpečnosti a dôveryhodných služieb.

Vydáva stanoviská a metodiky, podieľa sa na vypracúvaní strategických a koncepčných materiálov, vypracúva bezpečnostné a znalostné štandardy, ktorých ustálené postupy zavádza do medzinárodných štandardov cez pracovné skupiny ISO alebo európske štandardizačné inštitúcie a vydáva certifikačné politiky. Pripomienkuje návrhy legislatívnych a nelegislatívnych materiálov v pripomienkovom konaní a vykonáva legislatívny proces materiálov so zahraničným prvkom.

Vykonáva dohľadovú činnosť na úseku ochrany utajovaných skutočností, šifrovej ochrany informácií, kybernetickej bezpečnosti a dôveryhodných služieb, ktorá je realizovaná formou kontroly, dohľadu, auditu a inšpekcie.

Na medzinárodnej úrovni zastupuje úrad a koordinuje zahraničné aktivity úradu. Styční dôstojníci sekcie regulácie a dohľadu v EÚ, NATO a USA plnia úlohy pri rozvíjaní a budovaní medzinárodných vzťahov a spolupráce úradu v zahraničí. Zabezpečujú komunikáciu medzi NBÚ a zahraničnými partnermi a zastupujú záujmy Slovenskej republiky.

Sekcia kontroly a bezpečnosti

Sekcia kontroly a bezpečnosti zaisťuje vnútornú bezpečnosť úradu, plní úlohy na úseku ochrany utajovaných skutočností, zabezpečuje fyzickú a technickú ochranu objektov úradu, riaditeľa úradu a pracovníkov úradu.

V oblasti vnútornej bezpečnosti získava, sústreďuje, analyzuje a preveruje informácie o bezpečnostných rizikách týkajúcich sa pôsobnosti úradu, príslušníkov a zamestnancov. Objasňuje priestupky na úsekoch v pôsobnosti úradu.

Vykonáva vnútornú kontrolu, vybavuje sťažnosti a petície. Plní úlohy zodpovednej osoby pri vybavovaní oznámení o protispoločenskej činnosti, na úseku ochrany osobných údajov a v oblasti prevencie korupcie. Plní úlohy na úseku BOZP, protipožiarnej ochrany a zabezpečuje služobnú prípravu príslušníkov.

Sekcia participuje na plnení úloh podľa § 2 ods. 7 zákona č. 319/2002 Z. z. o obrane Slovenskej republiky, v rámci ktorého sa na zabezpečenie riadenia obrany štátu vytvára Hlavné miesto riadenia obrany štátu (HMROŠ) určené pre prezidenta Slovenskej republiky, vládu Slovenskej republiky alebo Bezpečnostnú radu Slovenskej republiky, ak je činnosť vlády znemožnená.

Sekcia akreditácie a certifikácie

Vykonáva akreditáciu a certifikáciu v oblasti ochrany utajovaných skutočností pre personálnu bezpečnosť, administratívnu bezpečnosť, fyzickú bezpečnosť, objektovú bezpečnosť, bezpečnosť technických prostriedkov a priemyselnú bezpečnosť, v oblasti šifrovej ochrany informácií, v oblasti kybernetickej bezpečnosti a v oblasti dôveryhodných služieb.

Národné centrum kybernetickej bezpečnosti

Plní úlohy národnej jednotky CSIRT, pričom zabezpečuje komplexné služby v oblasti riadenia bezpečnostných incidentov – od ich detekcie a analýzy, cez koordináciu riešenia a mitigáciu dopadov, až po obnovu prevádzky informačných systémov v úzkej spolupráci s ich vlastníkmi a prevádzkovateľmi.

Zároveň vykonáva analytické činnosti a výskum v oblasti kybernetickej bezpečnosti, podieľa sa na zvyšovaní bezpečnostného povedomia a realizácii vzdelávacích aktivít a plní ďalšie odborné úlohy v tejto oblasti.

NCKB tiež zabezpečuje výkon všeobecnej analytiky, posudzovanie bezpečnostných rizík, vyhodnocovanie politík, ako aj tvorbu prognóz, stratégií a implementačných plánov úradu. Súčasťou jeho pôsobnosti je aj budovanie a rozvoj externých vzťahov a spolupráce s relevantnými partnermi, ako aj zabezpečovanie komunikácie smerom k verejnosti.

Odbor personalistiky a sociálneho zabezpečenia

Realizuje personálnu a mzdovú politiku úradu, sociálne zabezpečenie, vzdelávanie a odmeňovanie. Koordinuje zdravotnú starostlivosť pre príslušníkov a zamestnancov úradu.

Útvar vnútorného auditu

Vykonáva vnútorný audit úradu a plní ďalšie úlohy podľa zákona o finančnej kontrole a audite

Národný orgán pre kyberbezpečnostnú certifikáciu

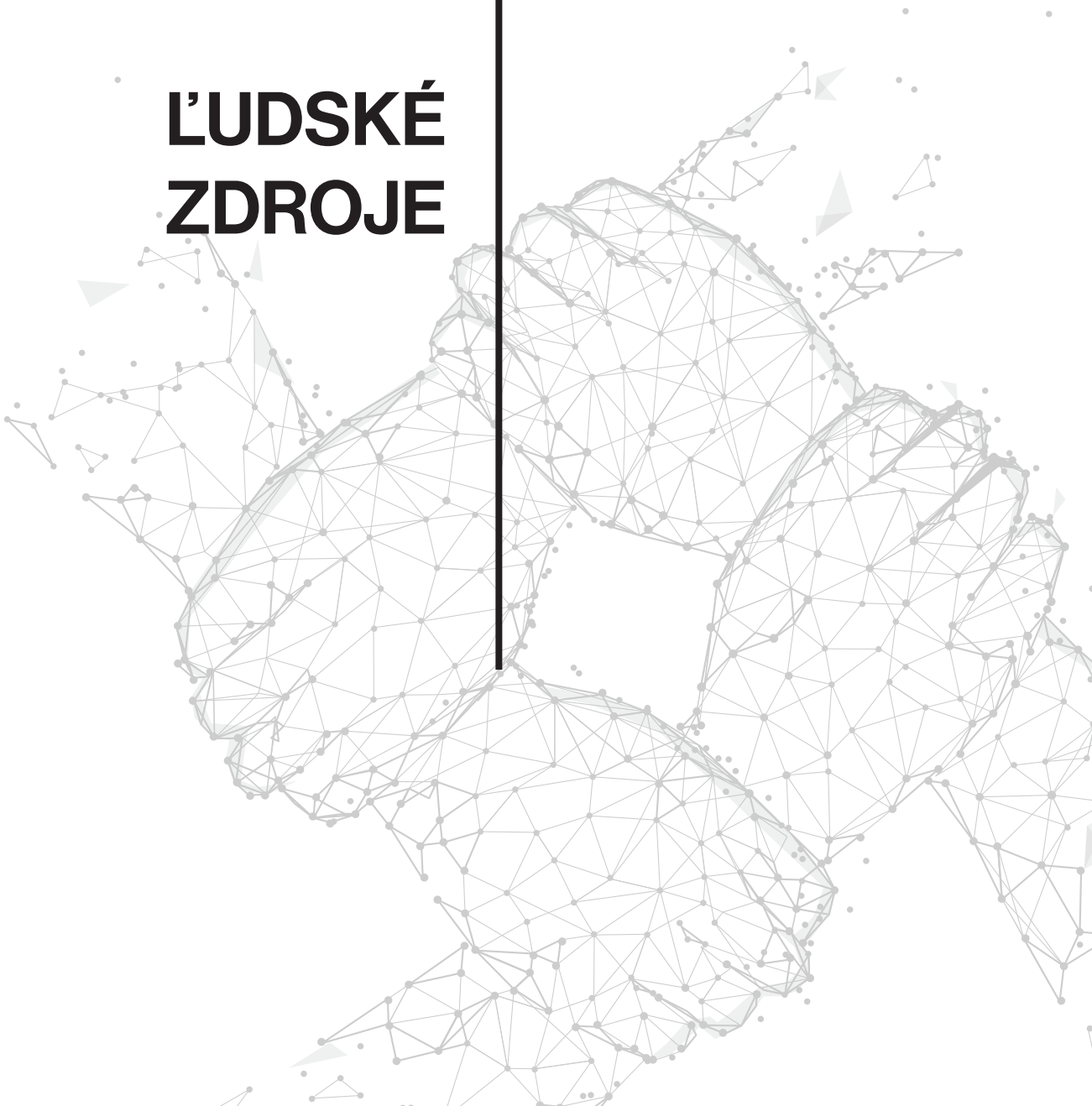
Je vecným útvarom úradu, ktorý plní funkciu vnútroštátneho orgánu pre certifikáciu kybernetickej bezpečnosti podľa osobitného predpisu.

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti (KCCKB) je príspevková organizácia úradu, ktorá vo verejnom záujme napomáha plniť odborné úlohy úradu v oblasti kybernetickej bezpečnosti, ochrany utajovaných skutočností, šifrovej ochrany a dôveryhodných služieb.

02.

ĽUDSKÉ ZDROJE



Prehľad o počte a štruktúre príslušníkov a zamestnancov

	ŠTÁTNA SLUŽBA		ZAMESTNANCI		ŠTÁTNA SLUŽBA A ZAMESTNANCI	
Prípravná štátna služba	**28**	13.27 %				
Stála štátna služba	**178**	84.36 %				
Dočasná štátna služba	**5**	2.37 %				
Spolu	**211**	90.17 %	**23**	9.83 %	**234**	100 %

Veková štruktúra príslušníkov a zamestnancov

	PRÍSLUŠNÍCI		ZAMESTNANCI		ŠTÁTNA SLUŽBA A ZAMESTNANCI	
do 34 rokov	**45**	21.33 %	**9**	39.13 %	**54**	23.08 %
35 - 49 rokov	**105**	49.76 %	**4**	17.39 %	**109**	46.58 %
50 - 59 rokov	**49**	23.22 %	**6**	26.09 %	**55**	23.50 %
60 a viac rokov	**12**	5.69 %	**4**	17.39 %	**16**	6.58 %
Spolu	**211**	90.17 %	**23**	9.83 %	**234**	100 %

Muži a ženy v NBÚ

	PRÍSLUŠNÍCI		ZAMESTNANCI		ŠTÁTNA SLUŽBA A ZAMESTNANCI	
Muži	**102**	85.71 %	**17**	14.29 %	**119**	50.85 %
Ženy	**109**	94.78 %	**6**	5.22 %	**115**	49.15 %
Spolu	**211**	90.17 %	**23**	9.83 %	**234**	100 %

Veková štruktúra príslušníkov a zamestnancov

PRÍSLUŠNÍCI			ZAMESTNANCI
0	0 %	Základné vzdelanie	**0** 0 %
35	16.59 %	Úplné stredné vzdelanie	**7** 30.43 %
7	3.32 %	Vysokoškolské vzdelanie I.st.	**0** 0 %
157	74.41 %	Vysokoškolské vzdelanie II.st.	**16** 69.57 %
12	5.69 %	Vysokoškolské vzdelanie III.st.	**0** 0 %
211		**Spolu**	**23**

PREHLBOVANIE KVALIFIKÁCIE A ZVYŠOVANIE ZRUČNOSTÍ

Úrad príslušníkom a zamestnancom umožňuje udržiavať odbornú pripravenosť, nadobúdať nové zručnosti a prehlbovať kvalifikáciu na odborných kurzoch, seminároch a školeniach doma i v zahraničí.

Príslušníci úradu počas roka 2025 absolvovali e-learningové školenie ku Koncepcii prevencie a boja proti radikalizácii a extrémizmu. Jeho cieľom bolo prehĺbiť povedomie o problematike extrémizmu, podporiť včasné rozpoznávanie prejavov radikalizácie a priblížiť právny aj spoločenský rámec boja proti týmto javom. Súčasťou vzdelávania bolo aj posilnenie internej kultúry úradu, postavenej na princípoch tolerancie, vzájomného rešpektu a bezpečného pracovného prostredia.

V rámci spolupráce sa príslušníci sekcie kontroly a bezpečnosti zúčastnili viacerých súčinnostných rokovaní s Národnou centrálou osobitných druhov kriminality Prezídia Policajného zboru, Úradom boja proti organizovanej kriminalite Prezídia Policajného zboru, Úradom inšpekčnej služby Ministerstva vnútra SR a Úradom vlády SR.

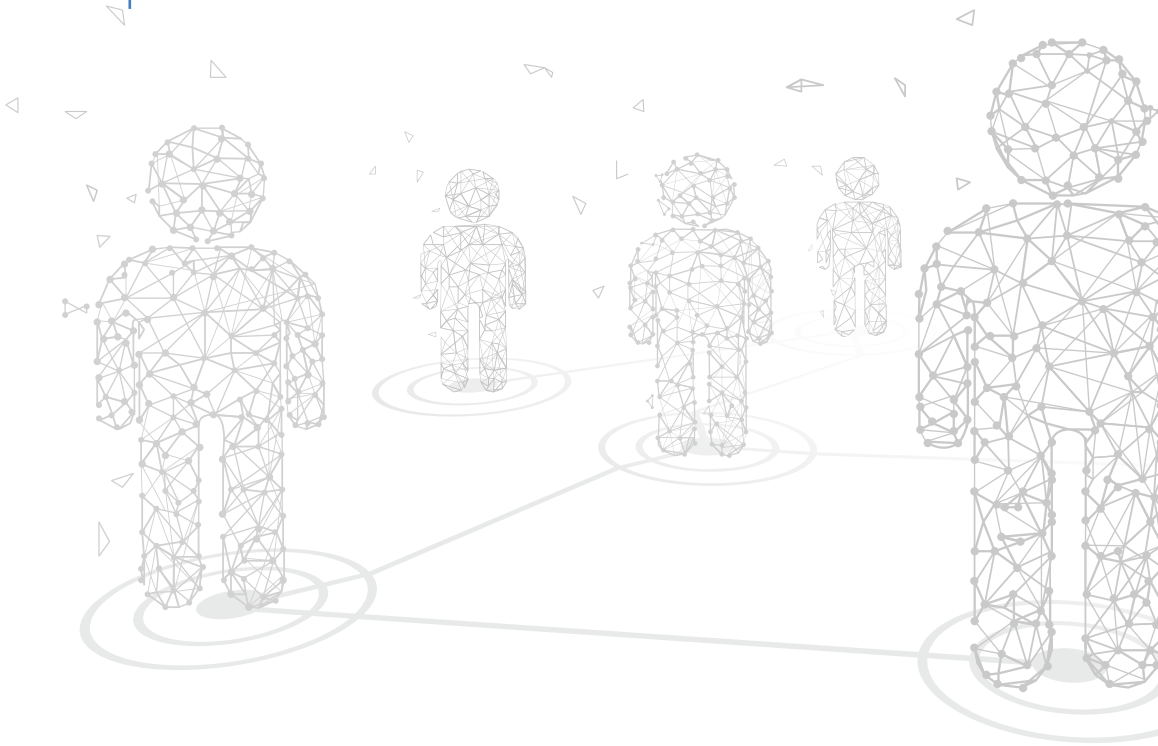
Príslušníci, ktorí vykonávajú fyzickú ochranu úradu sa zúčastnili základného výcviku detekčnej kontroly s využitím RTG z dôvodu zvýšenie bezpečnosti pri kontrole osôb a predmetov.

SLUŽOBNÁ PRÍPRAVA

Príslušníci sekcie kontroly a bezpečnosti plnili úlohy v rámci služobnej prípravy cvičeniami v oblasti telesnej prípravy, streleckej prípravy, špeciálnej prípravy a zdravotníckej prípravy. Na strelecký a špeciálnu prípravu využívali zariadenia ozbrojených bezpečnostných zborov, ozbrojených zborov, Slovenskej informačnej služby alebo Ozbrojených síl Slovenskej republiky.

PRACOVISKO SLUŽOBNEJ PSYCHOLÓGIE

Služobná psychologička počas roka 2025 realizovala 34 psychologických vyšetrení žiadateľov o prijatie do služobného pomeru príslušníka NBÚ, z toho 33 z nich bolo ku koncu roka uzavretých, pričom úspešnosť žiadateľov bola 82 percent. Taktiež vykonala tri dopravno-psychologické vyšetrenia. Bolo poskytnutých viac ako 300 hodín psychologického poradenstva, resp. sedení.



BOJ PROTI KORUPCII

V roku 2025 sme aktualizovali protikorupčný program Národného bezpečnostného úradu. V aktualizovanom programe, ktorého cieľom je ochrana verejného záujmu prostredníctvom zmenšovania priestoru a príležitostí pre korupciu, prijal úrad protikorupčné systémové opatrenia, ktoré spočívajú vo vzdelávaní príslušníkov a zamestnancov úradu v oblasti zvyšovania protikorupčného povedomia a v oblasti oznamovania protispoločenskej činnosti, ako aj posudzovania dôveryhodnosti partnerov vecného vzťahu.

Na zabezpečenie jednotného postupu úrad pri vybavovaní oznámení súvisiacich s oznamovaním protispoločenskej činnosti úrad postupuje podľa „Nariadenia riaditeľa Národného bezpečnostného úradu č. 8/2024 o vnútornom systéme vybavovania oznámení o protispoločenskej činnosti“ (ďalej len „nariadenie riaditeľa NBÚ č. 8/2024“).

Nariadenie riaditeľa NBÚ č. 8/2024 upravuje interný systém vybavovania oznámení protispoločenskej činnosti, najmä spôsob podávania podnetov, preverovanie oznámení, povinnosti a oprávnenia zodpovednej osoby, práva a povinnosti zamestnávateľa, podrobnosti o ochrane oznamovateľa ako aj evidenciu oznámení o protispoločenskej činnosti.

Príslušníci úradu, ktorí plnia úlohy zodpovednej osoby, sa pravidelne zúčastňujú školení Úradu na ochranu oznamovateľov a medzinárodnej organizácie EPAC/EACN aj školení zameraných na boj proti korupcii a ochranu whistleblowerov.

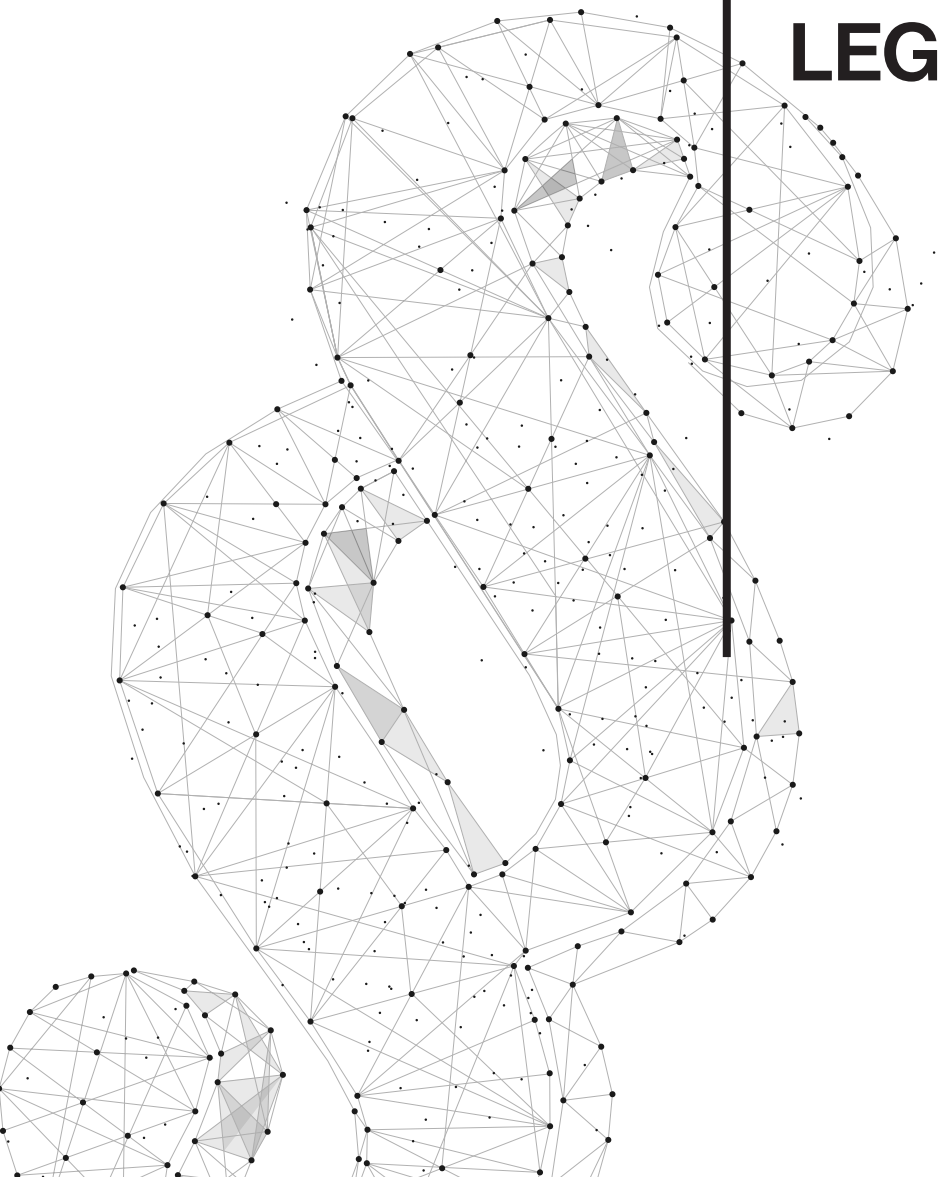
V novembri 2025 sa v priestoroch Eurojustu v Haagu konala 24. výročná medzinárodná konferencia a valné zhromaždenie Európskych partnerov proti korupcii (EPAC) a Európskej siete kontaktných bodov proti korupcii (EACN), ktorej sa zúčastnili príslušníci sekcie kontroly a bezpečnosti. Stretnutie inšpekčných služieb a protikorupčných zložiek bolo zamerané na tematiku „Udržiavanie integrity: Naliehavé výzvy v meniacom sa svete“. Hlavným zámerom konferencie bolo prehĺbenie vzájomnej spolupráce a posilnenie partnerských vzťahov útvarov, ktoré sa podieľajú na prevencii korupcie a na boji s trestnou činnosťou v členských krajinách Európskej únie.

Školenia v oblasti podávania oznámení a boju proti korupcii boli zaradené aj do špecializovaného štúdia príslušníkov úradu a formou e-learningu boli preškolení v uvedenej oblasti všetci príslušníci úradu. Rovnako úrad pristúpil v rámci adaptácie novoprijatých príslušníkov k ich vzdelávaniu v oblasti podávania oznámení a boja proti korupcii.

V rámci úradu sú nastavené vnútorné systémy oznamovania a vzdelávania príslušníkov úradu tak, aby všeobecne záväzné právne predpisy v oblasti ochrany oznamovateľov boli prístupné a zrejmé každému príslušníkovi úradu pre prípad, že by sa rozhodol podľa nich postupovať pri oznámení protispoločenskej činnosti.

03.

LEGISLATÍVA



Národný bezpečnostný úrad pokračoval v systematickom zbere, analýze a vyhodnocovaní informácií z činnosti útvarov úradu, zo spätnej väzby odbornej verejnosti, zo žiadostí o poskytnutie odborného stanoviska či iných podnetov orgánov verejnej moci, právnických osôb a fyzických osôb. V oblasti medzinárodného práva úrad harmonizuje národnú právnu úpravu s medzinárodne uznávanými prameňmi práva.

Úrad inicioval dve novelizácie **zákona o ochrane utajovaných skutočností:**

Zákonom č. 367/2024 Z. z. o kritickej infraštruktúre a o zmene a doplnení niektorých zákonov s účinnosťou od 01.01.2025 sa do **zákona o ochrane utajovaných skutočností** doplnilo nové ustanovenie (§ 3a) upravujúce inštitút limitovanej informácie. Základným cieľom zavedenia inštitútu limitovanej informácie je posilnenie bezpečnosti štátu spôsobom, ktorým bude právo na informácie dotknuté len v nevyhnutne potrebnej miere. V právnom systéme Slovenskej republiky doposiaľ absentovala právna úprava takých informácií, ktoré sú pre štát dôležité a ich voľné (nekontrolovateľné) šírenie by mohlo ohroziť, obmedziť alebo znemožniť plnenie úloh v oblasti bezpečnosti alebo pri zabezpečovaní verejného poriadku.

Zákonom č. 86/2025 Z. z. o ochrane svedka a o zmene a doplnení niektorých zákonov s účinnosťou od 01.05.2025 sa v zákone o ochrane utajovaných skutočností upravilo ustanovenie o iných oprávnených osobách, teda konkrétne, že aj osoba zastupujúca ohrozeného svedka alebo chráneného svedka podľa zákona o ochrane svedka sa môže oboznámiť s utajovanou skutočnosťou v rozsahu nevyhnutne potrebnom na jej využitie, bez splnenia podmienok podľa § 10 zákona o ochrane utajovaných skutočností.

Úrad inicioval novelizácie všeobecne záväzných právnych predpisov vydaných na vykonanie zákona o ochrane utajovaných skutočností:

Primárnym cieľom **vyhlášky Národného bezpečnostného úradu č. 127/2025 Z. z.**, ktorou sa mení a dopĺňa vyhláška Národného bezpečnostného úradu č. 135/2016 Z. z. o skúške bezpečnostného zamestnanca, s účinnosťou od 01.07.2025, bolo zosúladiť právny stav upravujúci agendu bezpečnostných zamestnancov s požiadavkami na elektronický výkon štátnej správy. Vytvorila sa výlučne elektronická komunikácia s úradom prostredníctvom špecializovaného portálu, ktorý umožňuje riešiť celú agendu bezpečnostných zamestnancov ustanovených právnou úpravou od podania žiadosti o skúšku bezpečnostného zamestnanca až po zaslanie zániku poverenia bezpečnostného zamestnanca. Novelou vyhlášky sa reagovalo aj na nie dostatočne vyhovujúci stav bezpečnostného povedomia na úseku ochrany utajovaných skutočností, spôsobený zvýšenou fluktuáciou (a generačnou obmenou) na príslušných pracovných pozíciách, v pôsobnosti ktorých sú vykonávané činnosti z poverenia vedúceho.

Vyhláškou Národného bezpečnostného úradu č. 185/2025 Z. z., ktorou sa mení vyhláška Národného bezpečnostného úradu č. 134/2016 Z. z. o personálnej bezpečnosti, s účinnosťou od 01.08.2025, sa zosúladil právny stav upravujúci agendu vykonávania bezpečnostných previerok fyzických osôb s požiadavkami na elektronický výkon štátnej správy. Vytvorila sa výlučne elektronická komunikácia s Národným bezpečnostným úradom prostredníctvom špecializovaného portálu, ktorý komplexne rieši celú agendu bezpečnostných previerok fyzických osôb ustanovených právnou úpravou od podania žiadosti o vykonanie bezpečnostnej previerky fyzickej osoby až po vydanie osvedčenia, príp. rozhodnutia, ak osoba nespĺňa predpoklady na vznik oprávnenia. Zároveň sa upravil spôsob predkladania žiadostí o vykonanie bezpečnostnej previerky, keďže doterajšia právna úprava umožňovala podávať tieto žiadosti iba na predpísanom tlačive zverejnenom na webovom sídle úradu. S elektronickou komunikáciou súvisí aj úprava niektorých obsahových náležitostí certifikátu o bezpečnostnej previerke, ako aj ustanovení súvisiacich so stratou, krádežou alebo poškodením osvedčení. Z hľadiska vecnej správnosti a zosúladenia s platnou právnou úpravou sa upravilo osobitné ustanovenie súvisiace s vydávaním osvedčení a aplikáciou ustanovení vyhlášky na ďalšie subjekty vykonávajúce bezpečnostné previerky.

Vyhláškou Národného bezpečnostného úradu č. 186/2025 Z. z., ktorou sa mení a dopĺňa vyhláška Národného bezpečnostného úradu č. 301/2013 Z. z. o priemyselnej bezpečnosti a o bezpečnostnom projekte podnikateľa, s účinnosťou od 01.08.2025, sa zosúladil právny stav upravujúci priemyselnú bezpečnosť, najmä v kontexte podrobností o bezpečnostnej previerke podnikateľa s požiadavkami na elektronický výkon štátnej správy. V rámci modernizácie vykonávania bezpečnostných previerok bol vytvorený systém umožňujúci výlučne elektronickú komunikáciu prostredníctvom špecializovaného portálu, ktorý komplexne rieši celú agendu bezpečnostných previerok. Predmetnou vyhláškou sa upravil spôsob predkladania žiadostí o vydanie potvrdenia o priemyselnej bezpečnosti, keďže doterajšia právna úprava umožňovala podávať tieto žiadosti iba na predpísanom tlačive zverejnenom na webovom sídle úradu. S elektronickou komunikáciou súvisí aj nadväzujúca úprava niektorých obsahových náležitostí potvrdenia o priemyselnej bezpečnosti. Vychádzajúc z aplikačnej praxe sa precizovali údaje umožňujúce identifikáciu prebiehajúceho konania, resp. osoby, ak už má vydané platné osvedčenie na oboznamovanie sa s utajovanými skutočnosťami.

Primárnym cieľom **zákona č. 366/2024 Z. z.**, ktorým sa mení a dopĺňa zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektorého zákony, ktorý nadobudol účinnosť 01.01.2025, bolo transponovať smernicu Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2) do právneho poriadku Slovenskej republiky.

Najvýraznejšou zmenou v rámci novely **zákona o kybernetickej bezpečnosti** bola zmena prístupu k identifikácii prevádzkovateľov základnej služby, upravili a precizovali sa bezpečnostné opatrenia tak, aby reflektovali nové bezpečnostné štandardy, vrátane dôrazu na riešenie rizík vyplývajúcich z dodávateľského reťazca, posilnilo sa využívanie analýzy rizík pre aplikáciu bezpečnostných opatrení, zaviedla sa minimálna úroveň bezpečnostných opatrení. Upravilo a precizovalo sa hlásenie kybernetického bezpečnostného incidentu, významnej kybernetickej hrozby, udalosti odvrátenej v poslednej chvíli, zraniteľností a riešenie kybernetického bezpečnostného incidentu, podporilo sa dobrovoľné hlásenie, posilnila sa dohľadová činnosť zavedením foriem dohľadu a posilnila sa funkcia manažéra kybernetickej bezpečnosti.

Úrad realizoval legislatívne procesy k dvom vykonávacím právnym predpisom vo vzťahu k zákonu o kybernetickej bezpečnosti, ktoré sa týkali podrobností o hláseniach a bezpečnostných opatrení; oba vykonávacie právne predpisy nadobudli účinnosť 01.09.2025.

Vyhláška Národného bezpečnostného úradu č. 226/2025 Z. z., ktorou sa ustanovujú podrobnosti o hláseniach, ustanovuje podrobnosti o hláseniach podľa § 24 zákona o kybernetickej bezpečnosti. Táto vyhláška vymedzuje identifikačné kritériá závažného narušenia fungovania prevádzkovateľa základnej služby, náležitosti hlásenia závažného kybernetického bezpečnostného incidentu podľa § 24 ods. 3 písm. a) a b) zákona o kybernetickej bezpečnosti a náležitosti hlásení podľa § 24 ods. 5 a 6 zákona o kybernetickej bezpečnosti (hlásenie významnej kybernetickej hrozby, o ktorej sa dozvie, udalosti odvrátenej v poslednej chvíli, ktorá mohla spôsobiť závažný kybernetický bezpečnostný incident, zraniteľnosť ním prevádzkovaných verejne dostupných sietí a informačných systémov, ktorá podľa dostupných informácií a technických znalostí môže byť zneužitá na spôsobenie závažného kybernetického bezpečnostného incidentu a prevádzkovateľ základnej služby nemohol v primeranom čase prijať opatrenia na jej odstránenie alebo zníženie rizika, dobrovoľné hlásenie kybernetického bezpečnostného incidentu, kybernetickej hrozby alebo udalosti odvrátenej v poslednej chvíli).

Vyhláška Národného bezpečnostného úradu č. 227/2025 Z. z. o bezpečnostných opatreniach precizuje bezpečnostné opatrenia tak, aby reflektovali nové bezpečnostné štandardy, vrátane dôrazu na riešenie rizík vyplývajúcich z dodávateľského reťazca, posilňovania využívania analýzy rizík pre aplikáciu bezpečnostných opatrení a zavedenia minimálnej úrovne bezpečnostných opatrení. Vyhláškou sa vymedzuje rozsah bezpečnostných opatrení v závislosti od toho, či ide o prevádzkovateľa základnej služby alebo prevádzkovateľa kritickej základnej služby a taktiež podľa toho, či ide o informačné a komunikačné technológie alebo operačné technológie. Vo vyhláške sa spresňuje obsah a štruktúra bezpečnostnej dokumentácie podľa § 20 ods. 3 zákona o kybernetickej bezpečnosti.

Zákonom č. 318/2025 Z. z., ktorým sa mení a dopĺňa zákon č. 56/2018 Z. z. o posudzovaní zhody výrobku, sprístupňovaní určeného výrobku na trhu a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony, ktorého legislatívny proces sa realizoval v roku 2025, sa s účinnosťou od 01.01.2026 doplnila do zákona o kybernetickej bezpečnosti kompetencia úradu ako orgánu dohľadu nad trhom pre produkt s digitálnymi prvkami v súlade s čl. 52 ods. 2 nariadenia Európskeho parlamentu a Rady (EÚ) 2024/2847 z 23. októbra 2024 o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami a o zmene nariadení (EÚ) č. 168/2013 a (EÚ) 2019/1020 a smernice (EÚ) 2020/1828 (akt o kybernetickej odolnosti) v platnom znení.

Úrad sa tiež zaoberal prípravou nového zákona, ktorý implementuje do slovenského právneho poriadku **akt o kybernetickej odolnosti** v platnom znení. Cieľom tejto legislatívnej aktivity je upraviť pravidlá výkonu dohľadu nad trhom pre produkt s digitálnymi prvkami z hľadiska jeho kybernetickej bezpečnosti. Podstatou európskej legislatívy v tomto smere je zabezpečiť, aby sa na európsky trh umiestňovali iba také produkty s digitálnymi prvkami, ktoré sú kyberneticky odolné, a to počas celého životného cyklu tohto produktu. Orgánom dohľadu nad trhom je úrad, ktorému sa návrhom zákona upraví postavenie pre výkon dohľadu nad trhom a základné zákonné kompetencie pri výkone tohto dohľadu. Na výkon dohľadu nad trhom sa vzťahuje európska legislatíva upravená nariadením Európskeho parlamentu a Rady (EÚ) 2019/1020 z 20. júna 2019 o dohľade nad trhom a súlade výrobkov a o zmene smernice 2004/42/ES a nariadení (ES) č. 765/2008 a (EÚ) č. 305/2011 v platnom znení, ktorú je rovnako potrebné implementovať do nového zákona. Implementácia aktu o kybernetickej odolnosti do nového zákona vyplýva úradu z čl. 71 aktu o kybernetickej odolnosti v platnom znení. Uplynutím tam uvedených lehôt je európska legislatíva v oblasti kybernetickej odolnosti priamo uplatniteľná vo všetkých štátoch Európskej únie.

Úrad v súvislosti so zákonom o kybernetickej bezpečnosti s účinnosťou od 01.09.2025 aktualizoval **Metodiku analýzy rizík kybernetickej bezpečnosti.**

V súlade s § 7 zákona o kybernetickej bezpečnosti úrad pripravil aj nelegislatívne materiály:

Národná stratégia kybernetickej bezpečnosti na roky 2026 až 2030 je východiskovým strategickým dokumentom, ktorý nadväzuje na predchádzajúce strategické dokumenty v oblasti kybernetickej bezpečnosti a je vypracovaný v súlade s vyvíjajúcim sa právnym rámcom Európskej únie, teda priamo zohľadňuje povinnosti vyplývajúce z kľúčových právnych aktov – smernice NIS 2, aktu o kybernetickej odolnosti, aktu o umelej inteligencii a smernice o odolnosti kritických subjektov. Slovenská republika si stanovila za cieľ stať sa bezpečným a dôveryhodným digitálnym štátom a tomuto bol prispôsobený aj hlavný cieľ stratégie – systematické

posilňovanie odolnosti národného kybernetického priestoru tak, aby bola adekvátne zabezpečená ochrana práv a bezpečnosť občanov v kybernetickom priestore, ochrana kritickej infraštruktúry štátu a prevádzkovateľov základných služieb, ako aj iných životne dôležitých aktív v národnom kybernetickom priestore. Vláda Slovenskej republiky stratégiu schválila uznesením č. 48 zo 04.02.2026.

Národný plán reakcie na rozsiahle kybernetické bezpečnostné incidenty a kybernetické krízy je v zmysle § 7 ods. 6 zákona o kybernetickej bezpečnosti strategickým dokumentom, ktorý určuje ciele a spôsoby riadenia rozsiahlych kybernetických bezpečnostných incidentov a kybernetických kríz. Je určený prevádzkovateľom základnej služby, zainteresovaným orgánom verejnej moci a subjektom, ktoré sú definované v tomto dokumente a ktoré sa podieľajú na národnej reakcii na rozsiahly kybernetický bezpečnostný incident a kybernetickú krízu. Cieľom tohto dokumentu je zabezpečiť rýchlu, efektívnu a koordinovanú reakciu štátu na rozsiahly kybernetický bezpečnostný incident, ktorý by mohol ohroziť národnú bezpečnosť, zabezpečenie demokratického poriadku, ochranu života a zdravia osôb, riadne fungovanie hospodárstva a orgánov verejnej moci.

Okrem uvedených úloh na úseku legislatívy úrad pripomienkuje a vypracúva stanoviská k návrhom legislatívnych a nelegislatívnych materiálov, vrátane aktov EÚ, v rámci **pripomienkového konania**. Celkovo úrad v roku 2025 posúdil a vyhodnotil 530 materiálov v pripomienkovom konaní, pričom zásadné pripomienky boli uplatnené pri 27 materiáloch.

SPRÁVNE A PRIESTUPKOVÉ KONANIE

V roku 2025 evidoval NBÚ sedem podaní vo veci podozrenia z priestupku na úseku ochrany utajovaných skutočností. Z toho päť podaní bolo formou záznamu odložených, jedno podanie bolo formou správy o výsledku objasňovania priestupku po zistení páchateľa priestupku predložené príslušnému správnemu orgánu a objasňovanie v jednom prípade stále pokračuje.

Sekcia kontroly a bezpečnosti v roku 2025 zaevidovala sedem oznámení o neoprávnenej manipulácii s utajovanou skutočnosťou, pričom tieto oznámenia boli objasňované v režime zákona č. 372/1990 Zb. o priestupkoch.



04.

OCHRANA UTAJOVANÝCH SKUTOČNOSTÍ



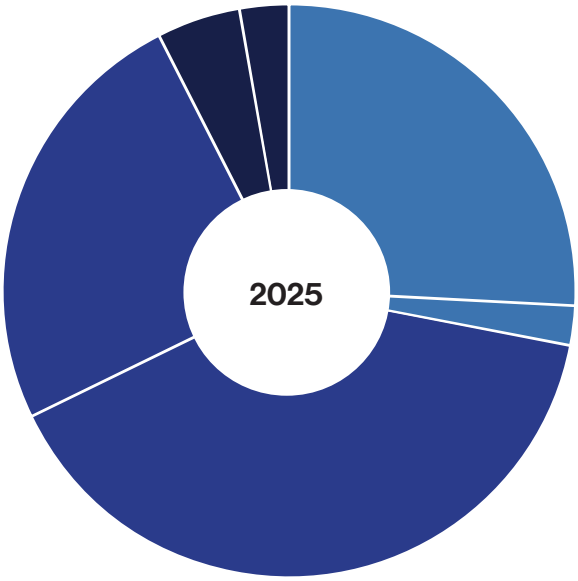
Národný bezpečnostný úrad vykonáva bezpečnostné previerky fyzických osôb a podnikateľov, vyjadruje sa o navrhovaných osobách podľa medzinárodných zmlúv, ktorými je Slovenská republika viazaná a vedie evidencie súvisiace s ochranou utajovaných skutočností.

Okrem osvedčení a potvrdení, ktoré umožňujú prístup k národným utajovaným skutočnostiam, zabezpečuje vydávanie certifikátov o bezpečnostnej previerke fyzickej osoby a certifikátov podnikateľa o priemyselnej bezpečnosti pre oboznamovanie sa s utajovanými skutočnosťami NATO a EÚ a vyjadruje sa o navrhovaných osobách podľa medzinárodných zmlúv, ktorými je Slovenská republika viazaná.

PERSONÁLNA BEZPEČNOSŤ

Národný bezpečnostný úrad vydal **5686 osvedčení** na oboznamovanie sa s utajovanými skutočnosťami, **z toho 2388 pre Ministerstvo obrany SR**.

Stupeň utajenia	2025
DÔVERNÉ	**2100**
z toho Dôverné pre MO SR	181
TAJNÉ	**3199**
z toho Tajné pre MO SR	1991
PRÍSNE TAJNÉ	**387**
z toho Prísne tajné pre MO SR	216
Spolu	**5686**



NBÚ vydal 16 rozhodnutí, z toho sedem pre MO SR. Proti rozhodnutiu úradu podali fyzické osoby šesť odvolaní, dve odvolania sú na úrade v procese prípravy stanoviska, úradom nebolo akceptovaných nula odvolaní. NBÚ vydal nula autoremedúr.

Na Výbore Národnej rady Slovenskej republiky na preskúmanie rozhodnutí NBÚ boli dve odvolania v odvolacom procese. Výbor v troch prípadoch odvolania zamietol, čím potvrdil rozhodnutie NBU. Sedem rozhodnutí zrušil, z čoho tri boli následkom rozhodnutia Najvyššieho správneho súdu Slovenskej republiky.

Na Najvyšší správny súd SR boli podané dve správne žaloby. Najvyšší správny súd v roku 2025 dve správne žaloby zamietol, päť rozhodnutí výboru zrušil (z čoho dve zrušil na základe nálezu Ústavného súdu SR. V jednej veci nerozhodol.

Na Ústavný súd SR bola podaná jedna ústavná sťažnosť. V roku 2025 Ústavný súd SR zrušil dve rozhodnutia Najvyššieho správneho súdu SR.

Navrhovaným osobám bolo v roku 2025 vydaných 6378 certifikátov o bezpečnostnej previerke fyzickej osoby - z toho 3158 certifikátov NATO a 3220 certifikátov EÚ. Z celkového počtu certifikátov NATO úrad vydal 16 certifikátov NATO ATOMAL, ktoré oprávňujú na prístup k informáciám o strategickom jadrovom odstrašovaní NATO a vydávajú sa úzkemu okruhu osôb.

PRIEMYSELNÁ BEZPEČNOSŤ

V roku 2025 vydal úrad 130 potvrdení o priemyselnej bezpečnosti – z toho 11 potvrdení stupňa utajenia Vyhradené, 97 potvrdení stupňa utajenia Dôverné, 20 potvrdení stupňa utajenia Tajné a dve potvrdenie stupňa utajenia Prísne tajné.

V roku 2025 úrad vydal päť rozhodnutí. Proti rozhodnutiu úradu nepodali podnikatelia odvolania.

Vo vzťahu k utajovaným skutočnostiam NATO a EÚ bolo v roku 2025 podnikateľom vydaných spolu 43 certifikátov, z toho 22 certifikátov NATO a 21 certifikátov EÚ, ktoré oprávňujú podnikateľov oboznamovať sa s utajovanými skutočnosťami NATO a/alebo EÚ.

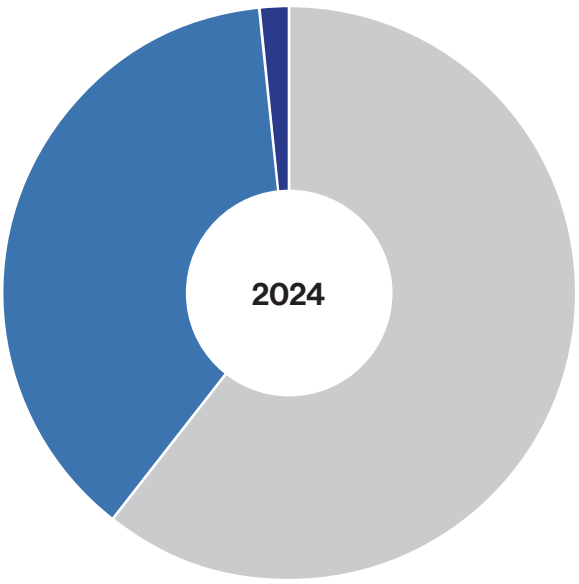
Na Najvyššom správnom súde SR bola v roku 2025 podaná jedna žaloba. Najvyšší správny súd jedno rozhodnutie výboru zrušil a jednu vec nerozhodol.

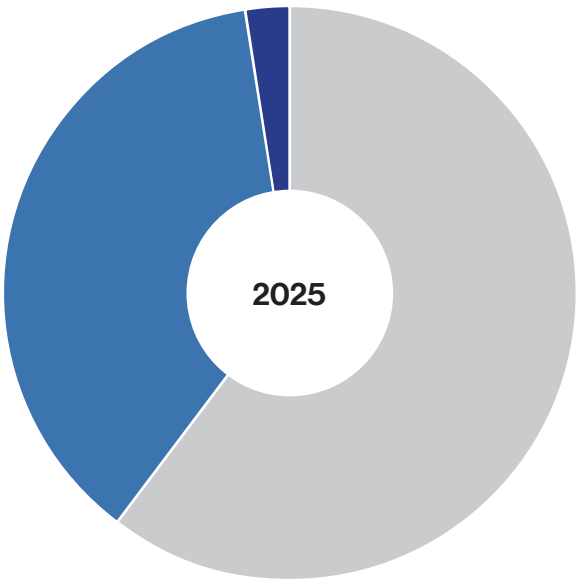
Na Ústavnom súde SR nebola podaná ústavná sťažnosť a súd ani nezrušil žiadne rozhodnutie najvyššieho správneho súdu.

VÝMENA UTAJOVANÝCH SKUTOČNOSTÍ

V roku 2025 úrad prijal a odoslal 1182 utajovaných skutočností. Údaje o vymieňaných utajovaných skutočnostiach v rámci interného prostredia - interná komunikácia medzi útvarmi v celkovom počte nie je uvedená. Od roku 2022 elektronický informačný systém pre správu registratúry umožňuje vytvárať utajované skutočnosti stupňa utajenia Vyhradené aj obsahovo.

Stupeň utajenia	2024	2025
VYHRADENÉ	875	715
DÔVERNÉ	544	438
TAJNÉ	21	29
PRÍSNE TAJNÉ	0	0
Spolu	1440	1182

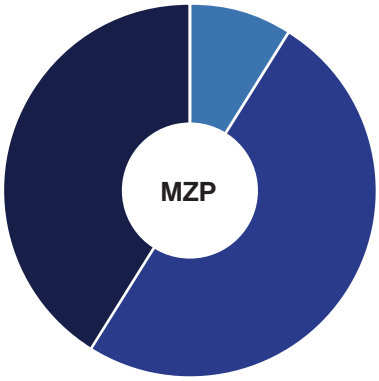


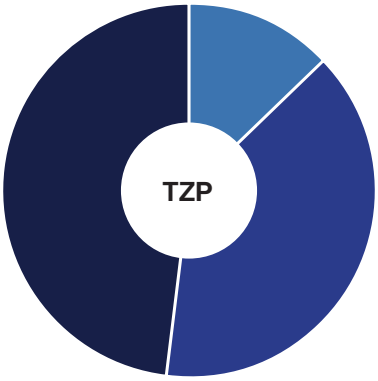


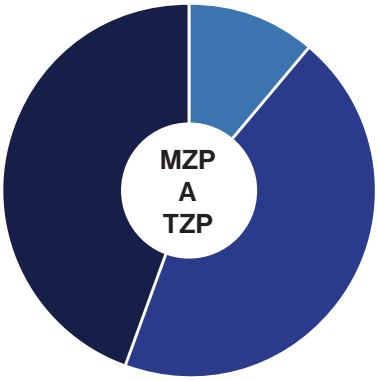
FYZICKÁ BEZPEČNOSŤ A OBJEKTOVÁ BEZPEČNOSŤ

Za rok 2025 úrad vydal **45 certifikátov** mechanických zábranných (MZP) a technických zabezpečovacích prostriedkov (TZP).

Stupeň utajenia	MZP	TZP	MZP A TZP
VYHRADENÉ	0	0	0
DÔVERNÉ	2	3	5
TAJNÉ	11	9	20
PRÍSNE TAJNÉ	9	11	20
Spolu	22	23	45



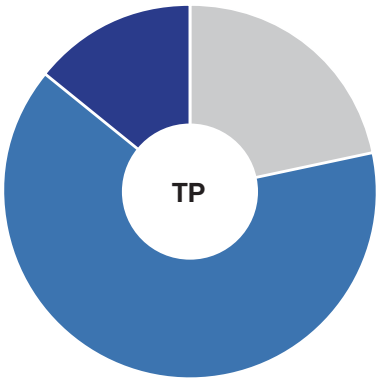




BEZPEČNOSŤ TECHNICKÝCH PROSTRIEDKOV

Za rok 2025 úrad vydal **64 certifikátov** technických prostriedkov a 40 dodatkov k už vydaným certifikátom technických prostriedkov (TP).

Stupeň utajenia	TP
VYHRADENÉ	14
DÔVERNÉ	41
TAJNÉ	9
PRÍSNE TAJNÉ	0
Spolu	64



Akreditácia komunikačných a informačných systémov

V roku 2025 úrad vykonal tri akreditácie komunikačných a informačných systémov v súlade s bezpečnostnými politikami medzinárodných organizácií a spoločenstiev, ktorých je Slovenská republika členom.

Ochrana pred nežiaducim elektromagnetickým vyžarovaním

Na zabezpečenie ochrany utajovaných skutočností pred únikom cez nežiaduce elektromagnetické vyžarovanie sekcia akreditácie a certifikácie v roku 2025 vykonávala merania NEV zariadení technických prostriedkov a prostriedkov šifrovej ochrany informácií (v TEMPEST laboratóriu), ako aj zónové merania chránených priestorov (mobilnou meracou aparatúrou).

K 31.12.2025 bolo prijatých 48 žiadostí (jedna žiadosť môže obsahovať viacero požiadaviek o stanovisko k certifikácii technického prostriedku (TP), vykonanie meraní NEV zariadení TP a o vykonanie zónových meraní priestorov), z ktorých bolo vybavených 40.

V priebehu posudzovaného obdobia boli vykonané merania NEV 119 meraných samostatných zariadení, zostáv zariadení a informačných systémov (TP a PŠOI) v Národnom laboratóriu TEMPEST.

V rámci doručených žiadostí bolo vykonaných 144 zónových meraní priestorov, na základe ktorých bolo kategorizovaných 291 miestností.

V danom období bolo prijatých aj šesť žiadostí o vykonanie technických bezpečnostných prehliadok priestorov, na základe ktorých boli vykonané štyri prehliadky miestností.

Zmluvy o postupovaní utajovaných skutočností

Úrad má celkovo uzatvorených 14 zmlúv o prístupe podnikateľa k utajovaným skutočnostiam, vlani uzatvoril jednu zmluvu a tri dodatky k uzatvoreným zmluvám.

Bezpečnostné povedomie

Úrad pokračoval v posilňovaní bezpečnostného povedomia v oblasti ochrany utajovaných skutočností vykonávaním školiacich aktivít, vlastnou metodickou činnosťou (v písomnej a ústnej forme) a zverejňovaním vzdelávacích materiálov na webovom sídle úradu.

Na základe požiadaviek a spätnej väzby odbornej verejnosti (pozostávajúcej z orgánov verejnej moci a súkromného sektora) bol vypracovaný a verejnosti sprístupnený Plán vzdelávacích aktivít na rok 2025, podľa ktorého sa pravidelne na mesačnej báze vykonávali školenia prezenčnou formou.

Okrem všeobecne prístupných školení pre externé prostredie úrad vykonával prednášky pre vlastných príslušníkov, na požiadanie (iba pre štátne orgány) a v zmysle záväzkov (dohôd a memoránd), ktoré boli zamerané na konkrétne témy alebo činnosti. Rovnako, špecificky zamerané prednášky poskytoval aj svojim zahraničným partnerom

v rámci viacerých bilaterálnych i významných multilaterálnych aktivít (napr. zasadnutie Bezpečnostného výboru NATO v Bratislave). Týchto partnerov zaujal aj celkový systém budovania bezpečnostného povedomia v Slovenskej republike. Zároveň, aj v roku 2025 úrad vycestoval za poslucháčmi a okrem Bratislavy a Košíc prednášal aj v Banskej Bystrici, Kováčovej, Pezinku a vo Veľkom Mederi.

Celkovo bolo vykonaných 19 prednášok v časovom rozsahu od jednej hodiny až po celý týždeň – spolu 172 hodín. Preškolených bolo spolu 1742 osôb.

Pre odbornú verejnosť bola na webovom sídle úradu vytvorená samostatná sekcia, v ktorej sú publikované vzdelávacie materiály pozostávajúce zo súboru podkladov určených na podporu vzdelávacích aktivít a sprostredkovanie odborných poznatkov vo forme prezentácií a iných samovzdelávacích podkladov (návody, príručky a písomné výstupy z kontrolnej činnosti úradu a pod.).

Ďalším efektívnym nástrojom budovania bezpečnostného povedomia je v súlade s legislatívou uskutočňovanie overovania splnenia predpokladov navrhovaných zamestnancov a ich vedomostí prostredníctvom skúšok bezpečnostného zamestnanca. Pre uvedený účel úrad využíva špecializovaný portál Verejný portál Agenda Bezpečnostní zamestnanci. Ide o plne elektronickú službu umožňujúcu orgánu verejnej moci, podnikateľovi alebo fyzickej osobe vyplniť elektronický formulár, elektronicky ho autorizovať a následne odoslať na ďalšie spracovanie. Skúška bezpečnostných zamestnancov sa vykonáva formou on-line testu najmä vo webovej aplikácií a cez špecializovaný portál, pričom vzájomná komunikácia medzi úradom a skúšaným prebieha vo virtuálnej video-konferenčnej miestnosti.

V súvislosti s nadobudnutím účinnosti vyhlášky Národného bezpečnostného úradu č. 127/2025 Z. z., ktorou sa mení a dopĺňa vyhláška Národného bezpečnostného úradu č. 135/2016 Z. z. o skúške bezpečnostného zamestnanca (ďalej len „vyhláška č. 12/2025 Z. z.“) dňom 01.07.2025 prišlo na úrade aj k interným zmenám v kompetenciách útvarov vykonávajúcich uvedenú agendu.

Útvar (sekcia regulácie a dohľadu), ktorý mal pôvodne na starosti tieto skúšky, na ne pozval celkovo 225 uchádzačov, z ktorých 145 úspešne absolvovalo skúšku, 42 bolo neúspešných a 38 osôb sa skúšky nezúčastnilo.

Preškolenie bezpečnostného zamestnanca formou testu ustanovila novela právneho predpisu vykonávať len do konca júna 2025. Za dané obdobie, tzn. za prvý polrok 2025, požiadalo o takéto preškolenie celkovo 170 uchádzačov, z ktorých 120 úspešne absolvovalo preškolenie a 2 uchádzači boli neúspešní. Zostávajúci počet (48) uchádzačov sa preškolenia nezúčastnilo. Úrad vybavil všetky žiadosti o skúšku a preškolenie bezpečnostného zamestnanca.

Nadobudnutím účinnosti vyhlášky č. 127/2025 Z. z. úrad (sekcia previerok) v období od 01.07.2025 do 31.12.2025 pozval na skúšku bezpečnostného zamestnanca 133 uchádzačov (celkový počet uchádzačov. Z nich skúšku úspešne absolvovalo 115 uchádzačov a zvyšok (18) bol neúspešný.

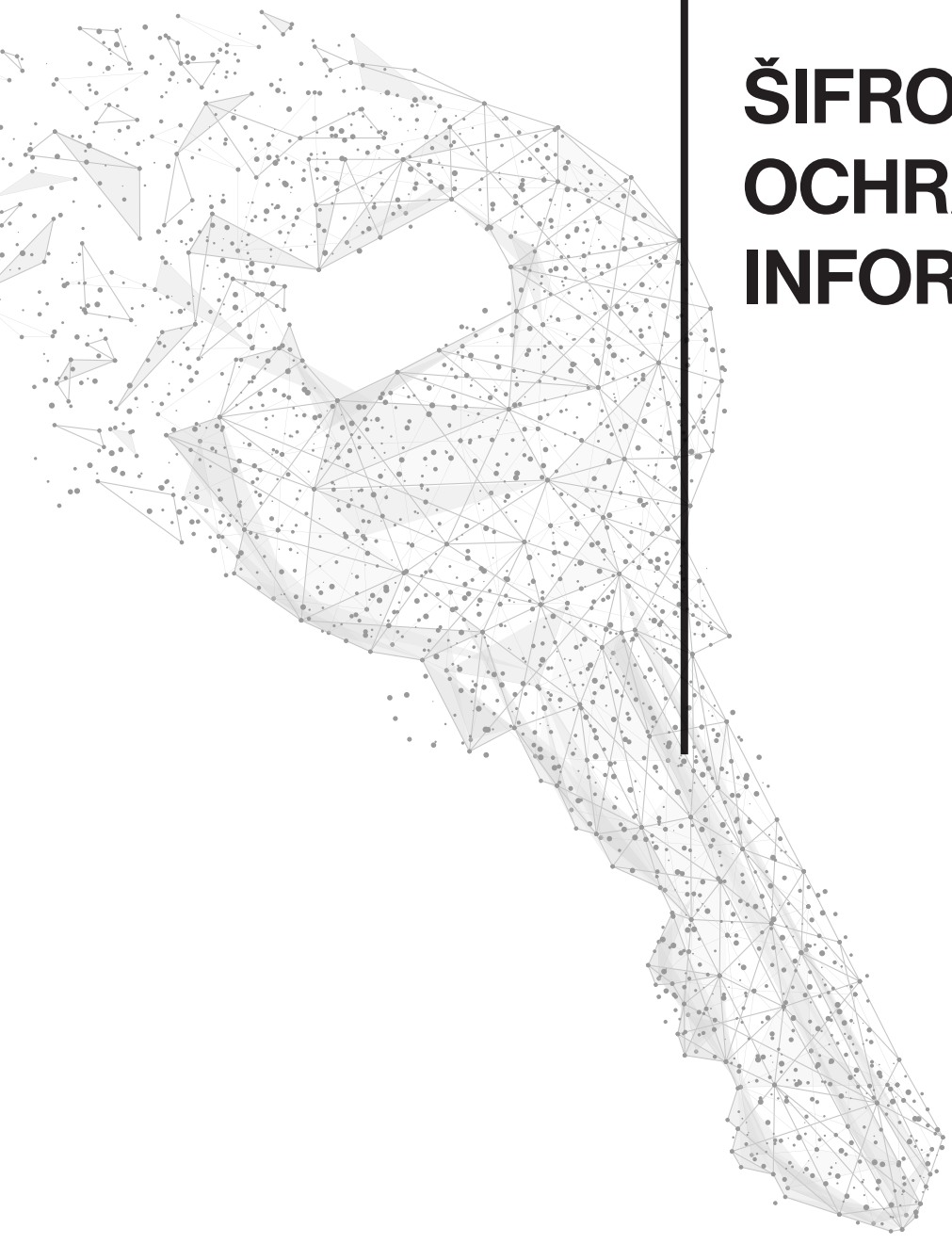
Celkovo úrad pozval 358 uchádzačov, z ktorých 260 skúšku bezpečnostného zamestnanca absolvovalo úspešne, 60 neúspešne a 38 uchádzačov sa skúšky nezúčastnilo.

Úrad riadne a včas vybavil všetky žiadosti o vykonanie skúšky doručené do 31.12.2025 a na základe časových preferencií uchádzačov.

Úrad k 31.12.2025 podľa § 2 ods. 9 vyhlášky č. 135/2016 Z. z. vydal štyri nové potvrdenia o absolvovaní skúšky (tzv. duplikát) na žiadosť držiteľa potvrdenia, z toho jedno potvrdenie v druhom polroku 2025, nakoľko bola táto žiadosť doručená úradu pred nadobudnutím platnosti vyhlášky č. 127/2025 Z. z.

05.

ŠIFROVÁ OCHRANA INFORMÁCIÍ

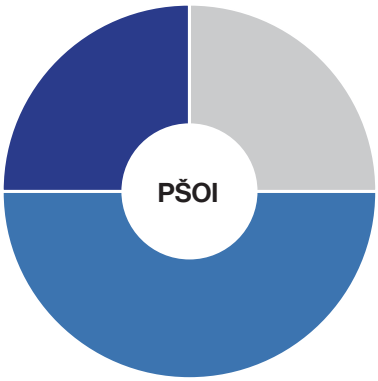


CERTIFIKÁCIA

Systém šifrovej ochrany informácií je v Slovenskej republike založený na overenej štruktúre rezortných šifrových orgánov a ich úzkej spolupráci s NBÚ, ktorý plní rolu ústredného šifrového orgánu. Predmetom komunikácie v roku 2025 boli najmä oblasti certifikácie prostriedkov šifrovej ochrany informácií, vydávanie dodatkov k pravidlám na používanie prostriedkov šifrovej ochrany informácií a otázky ohľadom možností uznávania a preberania zahraničných certifikátov.

Za rok 2025 úrad vydal 16 certifikátov prostriedkov šifrovej ochrany informácií (PŠOI) a nevydal dodatok k už vydaným certifikátom PŠOI.

Stupeň utajenia	PŠOI
VYHRADENÉ	4
DÔVERNÉ	8
TAJNÉ	4
PRÍSNE TAJNÉ	0
Spolu	16



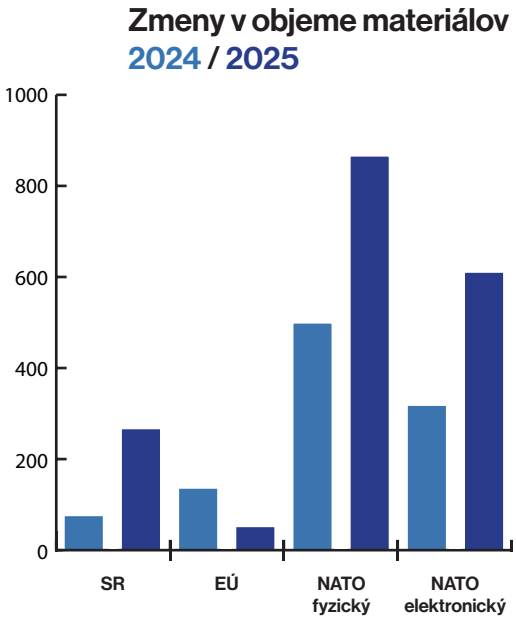
Stupne utajenia vydaných certifikátov k 31.12.2025

NÁRODNÁ DISTRIBUČNÁ AUTORITA

V roku 2025 pokračovala Národná distribučná autorita v štandardných evidenčných a distribučných činnostiach. Bol zaznamenaný značný nárast evidovaných a distribuovaných materiálov v oblasti NATO crypto a národných šifrových materiálov. Je spojený so zmenami v geopolitickej situácii a väčším objemom fyzického a elektronického materiálu primárne pre potreby Ministerstva obrany SR.

	Počet transakcií	Počet kusov
SR	15	80
EÚ	18	140
NATO fyzická distribúcia	63	501
NATO elektronická distribúcia	73	321
Spolu	169	1042

Počty transakcií a kusov šifrového materiálu k 31.12.2025



06.

DÔVERYHODNÉ SLUŽBY

Nariadením Európskeho parlamentu a Rady (EÚ) 2024/1183 z 11. apríla 2024, ktorým sa mení nariadenie (EÚ) č. 910/2014, pokiaľ ide o zriadenie európskeho rámca digitálnej identity sa do európskej právnej úpravy zaviedol pojem **„európska peňaženka digitálnej identity“**. Ide o univerzálny prístup k bezpečnej a dôveryhodnej elektronickej identifikácii a autentifikácii na mobilnom telefóne s úrovňou uistenia „vysoká”. Prostredníctvom európskej peňaženky digitálnej identity užívateľ získa svoje potvrdenie (elektronické osvedčenie atribútov) z autentických zdrojov a od iných spoliehajúcich sa strán a aj od držiteľov digitálnej peňaženky. Z tejto množiny potvrdení vie zaslať spoliehajúcej sa strane len nevyhnutné údaje, napríklad len vek bez zverejnenia ostatných údajov.

Ďalšou povinnou súčasťou európskej peňaženky digitálnej identity bude bezplatné podpísanie kvalifikovaným podpisom. V priebehu roka 2025 sa pracovalo na európskych legislatívnych požiadavkách k oblasti podpisu a pečate v peňaženke, pri ktorých sa vychádzalo zo skúseností z používania aplikácií na podporu bezplatného podpísania, zapečatenia a dlhodobého uchovania kvalifikovaným podpisom, pečaťou a časovou pečiatkou, ako napríklad bezplatnej aplikácie úradu QES a aQES, ktoré sa počas roka 2025 používali v portáloch previerok, bezpečnostných zamestnancov a ich obľúbenosť zverejnená v rebríčku na Apple macOS bola v prvej desiatke všetkých bezplatných aplikácií.

K európskej peňaženke digitálnej identity boli vydané implementačné akty:

- **Vykonávacie nariadenie Komisie (EÚ) 2025/846 zo 6. mája 2025**, ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014, pokiaľ ide o cezhraničné párovanie totožnosti fyzických osôb,

- **Vykonávacie nariadenie Komisie (EÚ) 2025/847 zo 6. mája 2025**, ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014, pokiaľ ide o reakcie na narušenia bezpečnosti európskych peňaženiek digitálnej identity,

- **Vykonávacie nariadenie Komisie (EÚ) 2025/848 zo 6. mája 2025**, ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014, pokiaľ ide o registráciu strán spoliehajúcich sa na peňaženku,

- **Vykonávacie nariadenie Komisie (EÚ) 2025/849 zo 6. mája 2025**, ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014, pokiaľ ide o predkladanie informácií do zoznamu certifikovaných európskych peňaženiek digitálnej identity Komisii a skupine pre spoluprácu,

- **Vykonávacie nariadenie Komisie (EÚ) 2025/1566 z 29. júla 2025**, ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014, pokiaľ ide o referenčné normy na overovanie totožnosti a atribútov osoby, ktorej sa má vydať kvalifikovaný certifikát alebo kvalifikované elektronické osvedčenie atribútov,

- **Vykonávacie nariadenie Komisie (EÚ) 2025/1567 z 29. júla 2025**, ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014, pokiaľ ide o správu zariadení na vyhotovenie kvalifikovaného elektronického podpisu na diaľku a zariadení na vyhotovenie kvalifikovanej elektronickej pečate na diaľku ako kvalifikovaných dôveryhodných služieb,

- **Vykonávacie nariadenie Komisie (EÚ) 2025/1568 z 29. júla 2025**, ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014, pokiaľ ide o dojednania o postupe pre vzájomné preskúmania schém elektronickej identifikácie a pre spoluprácu pri organizácii takýchto preskúmaní v rámci skupiny pre spoluprácu, a ktorým sa zrušuje vykonávacie rozhodnutie Komisie (EÚ) 2015/296,

- **Vykonávacie nariadenie Komisie (EÚ) 2025/1569 z 29. júla 2025**, ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014, pokiaľ ide o kvalifikované elektronické osvedčenia atribútov a elektronické osvedčenia atribútov poskytované subjektom verejného sektora zodpovedným za autentický zdroj alebo v jeho mene,

- **Vykonávacie nariadenie Komisie (EÚ) 2025/1570 z 29. júla 2025**, ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014, pokiaľ ide o oznamovanie informácií o certifikovaných zariadeniach na vyhotovenie kvalifikovaného elektronického podpisu a certifikovaných zariadeniach na vyhotovenie kvalifikovanej elektronickej pečate,

- **Vykonávacie nariadenie Komisie (EÚ) 2025/1571 z 29. júla 2025**, ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014, pokiaľ ide o formáty a postupy v súvislosti s výročnými správami orgánov dohľadu,

- **Vykonávacie nariadenie Komisie (EÚ) 2025/1572 z 29. júla 2025**, ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014, pokiaľ ide o formát a postupy oznamovania zámeru a overovania v súvislosti so začatím poskytovania kvalifikovaných dôveryhodných služieb,

- **Vykonávacie nariadenie Komisie (EÚ) 2025/1929 z 29. septembra 2025**, ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014, pokiaľ ide o spájanie dátumu a času s údajmi a stanovovanie presnosti zdrojov času na poskytovanie kvalifikovaných elektronických časových pečiatok,

- **Vykonávacie nariadenie Komisie (EÚ) 2025/1942 z 29. septembra 2025**, ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014, pokiaľ ide o kvalifikované služby validácie kvalifikovaných elektronických podpisov a kvalifikované služby validácie kvalifikovaných elektronických pečatí,

- **Vykonávacie nariadenie Komisie (EÚ) 2025/1943 z 29. septembra 2025**, ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014, pokiaľ ide o referenčné normy pre kvalifikované certifikáty pre elektronické podpisy a kvalifikované certifikáty pre elektronické pečate,

- **Vykonávacie nariadenie Komisie (EÚ) 2025/1944 z 29. septembra 2025**, ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014, pokiaľ ide o referenčné normy pre procesy odosielania a doručovania údajov v kvalifikovaných elektronických doručovacích službách pre registrované zásielky a pokiaľ ide o interoperabilitu týchto služieb,

- **Vykonávacie nariadenie Komisie (EÚ) 2025/1945 z 29. septembra 2025**, ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014, pokiaľ ide o validáciu kvalifikovaných elektronických podpisov a kvalifikovaných elektronických pečatí a validáciu zdokonalených elektronických podpisov založených na kvalifikovaných certifikátoch a zdokonalených elektronických pečatí založených na kvalifikovaných certifikátoch,

- **Vykonávacie nariadenie Komisie (EÚ) 2025/1946 z 29. septembra 2025**, ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014, pokiaľ ide o kvalifikované služby uchovávania kvalifikovaných elektronických podpisov a kvalifikovaných elektronických pečatí,

- **Vykonávacie nariadenie Komisie (EÚ) 2025/2160 z 27. októbra 2025**, ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014, pokiaľ ide o referenčné normy, špecifikácie a postupy riadenia rizík poskytovania nekvalifikovaných dôveryhodných služieb,

- **Vykonávacie nariadenie Komisie (EÚ) 2025/2162 z 27. októbra 2025**, ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014, pokiaľ ide o akreditáciu orgánov posudzovania zhody vykonávajúcich posudzovanie kvalifikovaných poskytovateľov dôveryhodných služieb a kvalifikovaných dôveryhodných služieb, ktoré poskytujú, správu o posúdení zhody a schému posudzovania zhody,

- **Vykonávacie rozhodnutie Komisie (EÚ) 2025/2164 z 27. októbra 2025**, ktorým sa mení vykonávacie rozhodnutie (EÚ) 2015/1505, pokiaľ ide o verziu normy, z ktorej vychádza spoločný vzor pre dôveryhodné zoznamy,

- **Vykonávacie nariadenie Komisie (EÚ) 2025/2527 zo 16. decembra 2025**, ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014, pokiaľ ide o referenčné normy pre kvalifikované certifikáty pre autentifikáciu webových sídiel,

- **Vykonávacie nariadenie Komisie (EÚ) 2025/2530 zo 16. decembra 2025**, ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014, pokiaľ ide o požiadavky na kvalifikovaných poskytovateľov dôveryhodných služieb poskytujúcich kvalifikované dôveryhodné služby,

- **Vykonávacie nariadenie Komisie (EÚ) 2025/2531 zo 16. decembra 2025**, ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014, pokiaľ ide o referenčné normy a špecifikácie pre kvalifikované elektronické registre,

- **Vykonávacie nariadenie Komisie (EÚ) 2025/2532 zo 16. decembra 2025**, ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014, pokiaľ ide o referenčné normy a špecifikácie pre kvalifikované elektronické archivačné služby.

Dôveryhodný zoznam

Úrad vedie a na svojom webovom sídle zverejňuje dôveryhodný zoznam obsahujúci informácie o poskytovateľoch kvalifikovaných dôveryhodných služieb, ktorí sú pod dohľadom Slovenskej republiky a informácie o poskytovaných kvalifikovaných dôveryhodných službách.

V roku 2025 úrad publikoval dôveryhodné zoznamy č. 121 až 132.

Zoznam oprávnení

Zoznam oprávnení je informačným zdrojom pre kvalifikovaných poskytovateľov dôveryhodných služieb pre vydávanie mandátnych certifikátov, ktorý úrad aktualizuje a zverejňuje na svojom webovom sídle v strojovo spracovateľnej podobe. Úrad v roku 2025 prijal 22 žiadostí o aktualizáciu zoznamu oprávnení pričom zapísal 25 nových oprávnení, pri siedmich už evidovaných oprávneniach úrad aktualizoval údaje v zozname oprávnení, jedna žiadosť bola zamietnutá z dôvodu nesúladu s § 9 ods. 5 zákona o dôveryhodných službách a v jednom prípade bolo navrhnuté alternatívne riešenie žiadosti.

Nové dôveryhodné služby

Novelizáciou zákona č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách) v znení zákona č. 211/2019 Z. z. úrad (sekcia akreditácie a certifikácie) certifikáciu produktov pre elektronický podpis (najmä QSCD) od 1. januára 2025 nevykonáva.

V roku 2025 NBÚ posúdil osem žiadostí o udelenie kvalifikovaného štatútu pre kvalifikované dôveryhodné služby. Žiadosti neboli úplné (chýbal audit kybernetickej bezpečnosti), a preto boli žiadatelia vyzvaní, aby doplnili žiadosti. Žiadosti k 31. decembru 2025 nedoplnili, takže k tomuto dátumu nebol udelený žiaden kvalifikovaný štatút na kvalifikovanú dôveryhodnú službu.

NBÚ odňal štatút 19 kvalifikovaným dôveryhodným službám (ukončil činnosť kvalifikovaný poskytovateľ dôveryhodných služieb (Viasec, s.r.o.)) a boli zrušené kvalifikované dôveryhodné služby závislé na koreňovej certifikačnej autorite (KCA).

Posúdila tiež šesť správ z kontrolného auditu od kvalifikovaných poskytovateľov kvalifikovaných dôveryhodných služieb.

Tvorba medzinárodných noriem

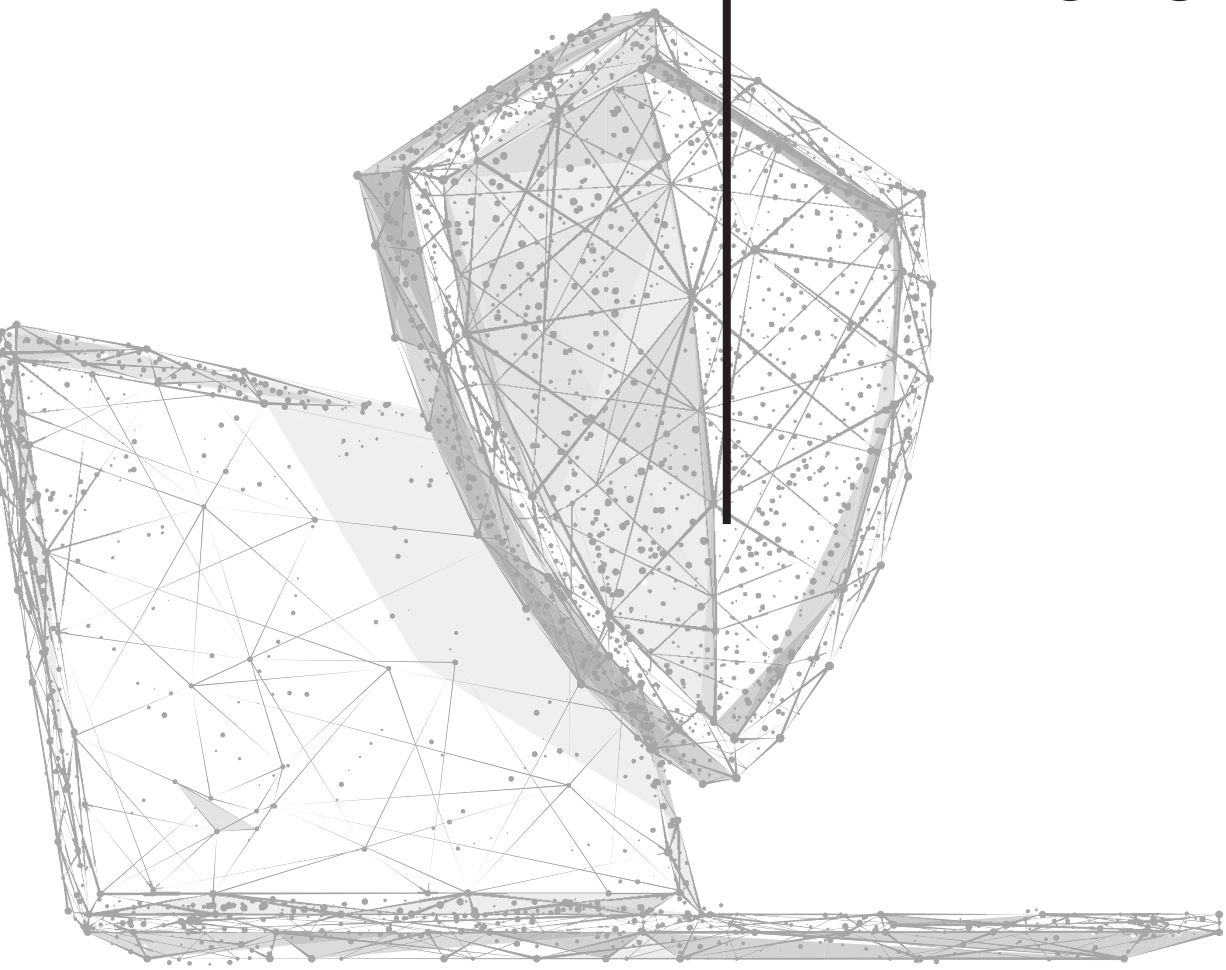
Pri tvorbe medzinárodných technických noriem použiteľných pre implementáciu nariadením (EÚ) č. 910/2014 v platnom znení je príslušník úradu súčasťou expertných skupín Európskej komisie, analyzujúcich riešenia, ktoré sú základom prípravy implementačných aktov k peňaženke digitálnej identity. Ako člen medzinárodných štandardizačných organizácií ISO a ETSI pripravoval štandardy na zahrnutie do implementačných aktov k nariadeniu (EÚ) č. 910/2014 v platnom znení.

Dôveryhodná infraštruktúra

V roku 2025 NBÚ v nadväznosti na novelu zákona č. 69/2018 o kybernetickej bezpečnosti ukončil prevádzku koreňovej certifikačnej autority Slovenskej republiky v dôvernej infraštruktúre. Táto autorita zabezpečovala vydávanie certifikátov verejných kľúčov a spravovala dlhodobú databázu vydaných kvalifikovaných certifikátov vrátane ich stavu platnosti, a to pre poskytovateľov, ktorým úrad priznal kvalifikovaný štatút.

07.

KYBERNETICKÁ BEZPEČNOSŤ



Národné centrum kybernetickej bezpečnosti

Národný bezpečnostný úrad prostredníctvom Národného centra kybernetickej bezpečnosti (NCKB) naďalej rozvíja svoje spôsobilosti pri zabezpečovaní otvoreného, bezpečného a chráneného národného kybernetického priestoru.

NCKB vykonáva bezpečnostný monitoring za účelom zberu informácií o kybernetických bezpečnostných incidentoch z rôznych zdrojov špecializovanými nástrojmi na dohľadovom centre. Úlohou tohto centra je bezpečnostný monitoring s cieľom zaistenia bezpečnosti dohľadovaných systémov.

Prijíma hlásenia o kybernetických bezpečnostných incidentoch, analyzuje ich, vyhodnocuje, vykonáva dohľad a koordinuje ich riešenie. Zdrojom údajov pri riešení a koordinácii kybernetických bezpečnostných incidentov je vlastná detekcia, povinné a dobrovoľné hlásenia prevádzkovateľov základných služieb a informácie od partnerov a partnerských organizácií. NCKB v oblasti monitoringu bezpečnostných hrozieb a zraniteľností zároveň distribuuje varovania a bezpečnostné bulletiny a zvyšuje tým úroveň prevencie.

NCKB kontinuálne rozvíjalo svoje interné nástroje a systémy slúžiace na detekciu kybernetických bezpečnostných incidentov a ich riešenie, analytické činnosti a schopnosti včasnej detekcie a šírenia situačného povedomia. Rovnako boli v rámci NCKB vytvárané kvartálne reporty o hrozbách v kybernetickom priestore a o činnosti APT skupín.

NBÚ evidoval v roku 2025 celkovo 1689 hlásení o kybernetických bezpečnostných incidentoch, o kybernetických bezpečnostných incidentoch, kybernetických hrozbách, udalostiach odvrátených v poslednej chvíli a o zraniteľnostiach:

- 1575 dobrovoľných hlásení o kybernetických bezpečnostných incidentoch
- 75 povinných hlásení o kybernetických bezpečnostných incidentoch
- 14 hlásení kybernetických hrozieb
- 9 hlásení udalostí odvrátených v poslednej chvíli
- 6 hlásení zraniteľností

Dominovali nasledujúce technické typy útokov: phishing a sociálne inžinierstvo (1067), podozrenie na úspešný prienik do systému vrátane APT (126), nedostupnosť vo forme DoS, DDoS útoku, sabotáže, výpadku služby (106) či škodlivý kód (62). Väčšina hlásení pochádzala z dobrovoľných hlásení, ktoré prevládali nad povinnými kategorizovanými hláseniami. Výrazný nepomer v počte dobrovoľných a povinných hlásení je spôsobený nedostatočným pochopením zákona a jednotlivých typov hlásení na strane PZS.

Technické typy útokov

Sociálne inžinierstvo	1067
Nevyžiadaná pošta (spam)	38
Škodlivý kód (vírus, malvér, ransomvér)	62
Skenovanie siete	17
Pokus o prienik do systému	34
Podozrenie na úspešný prienik do systému vrátane APT	126
Nedostupnosť (DoS, DDoS útok, sabotáž, výpadok služby)	106
Zraniteľnosť (ich existencia)	66
Obťažovanie	4
Vyhrážanie	42
Potláčanie práv a slobôd	0
Odpočúvanie	0
Neoprávnený prístup k informáciám, únik informácií, poškodenie informácií	32
Podvod (neautorizované využitie prostriedkov, porušenia autorských práv)	15
Iné	41
CELKOM KBI	**1650**
-	39
CELKOM HLÁSENÍ	**1689**

Najviac incidentov bolo nahlásených v sektore verejná správa (926), financie (72) a zdravotníctvo (44). Výrazné rozdiely v počte hlásení medzi sektormi sú spôsobené rôznou úrovňou detekčných schopností a taktiež uvedomenia subjektov. Uvedené čísla neznamenajú, že sektor verejná správa bol najčastejším cieľom útokov.

Sektory

Digitálna infraštruktúra	1067
Doprava	38
Energetika	62
Financie	17
Odpadové hospodárstvo	34
Poskytovatelia digitálnych služieb	126
Poštové a kuriérske služby	106
Riadenie služieb IKT (medzi podnikmi)	66
Verejná správa	4
Vesmír	42
Voda a atmosféra	0
Výroba a distribúcia chemických látok	0
Výroba, spracovanie a distribúcia potravín	32
Výroba	15
Výskum	41
Zdravotníctvo	1650
Iné	39
CELKOM	**1689**

Hlásenia kybernetických bezpečnostných incidentov a štatistické dáta potvrdzujú, že najrozšírenejšími a najúspešnejšími spôsobmi krádeže citlivých údajov a prieniku do systémov dlhodobo zostávajú útoky založené na zneužití princípov sociálneho inžinierstva, zraniteľností a nesprávnej konfigurácie verejne dostupných systémov prihlasovacích údajov a kryptografického materiálu, ktoré unikli buď z ľudskej nepozornosti, technickej chyby alebo následkom kybernetických útokov. Tento trend bolo možné pozorovať počas celého roka 2025 a útočníci sa zameriavali na zefektívnenie súvisiacich procesov, v ktorom nemalú úlohu zohrávala aj umelá inteligencia.

V roku 2025 sa charakter kybernetických incidentov na Slovensku niesol v znamení kombinácie cielených útokov na kľúčové inštitúcie, pokračujúcich phishingových kampaní a zneužívania technických zraniteľností. Dominovali najmä nasledujúce udalosti:

- Ransomvérový útok na Úrad geodézie, kartografie a katastra Slovenskej republiky, ktorý spôsobil výpadok katastrálneho informačného systému a ochromil viaceré služby verejnej správy aj súkromného sektora.

- Vlna výhražných e-mailov s tematikou bombových hrozieb, na ktorú bezpečnostné zložky reagovali metodikou vyhodnocovania rizika bombových hrozieb, NBÚ vydal výstrahu a varovanie pred kybernetickým bezpečnostným incidentom a prevádzkovateľom základnej služby uložil odmietanie e-mailov z anonymizačných služieb.

- Phishingové kampane šírené prostredníctvom kompromitovaných účtov v aplikácii WhatsApp s tematikou falošného hlasovania v súťaže cez aplikáciu WhatsApp.

- Phishing zneužívajúci kompromitované e-mailové kontá a cloudové úložiská.

- Kybernetický útok na spoločnosť Jaguar Land Rover, ktorý viedol k odstaveniu výroby a centrálnych IT systémov vo viacerých krajinách vrátane Slovenskej republiky.

- Výrazný nárast podvodov s tematikou výhodného investovania do kryptomien, pri ktorých sa útočníci vydávali za zástupcov investičných spoločností.

- Sofistikovaný útok štátom sponzorovanej skupiny na subjekt verejnej správy vedúci ku kompromitácii informačných systémov.

Dlhodobým systémovým rizikom zostávalo používanie neaktuálnych či zle nakonfigurovaných verzií softvéru, zariadení a služieb v infraštruktúre PZS aj neregulovaných subjektov, čo významne zvyšovalo pravdepodobnosť úspešnej kompromitácie prostredníctvom známych zraniteľností.

Národné centrum kybernetickej bezpečnosti na základe monitoringu otvorených zdrojov a kybernetických hrozieb, informácií od partnerov a vlastnej analytickej činnosti vydávalo bezpečnostné odporúčania a varovania pred zraniteľnosťami a hrozbami – 50 súhrnných bezpečnostných bulletinov a 596 bezpečnostných varovaní.

Národný bezpečnostný úrad každoročne vypracováva aj Správu o kybernetickej bezpečnosti v Slovenskej republike. Správa poskytuje detailnejšie informácie o stave kybernetickej bezpečnosti.

CYBERGAME

CyberGame patrí medzi najnáročnejšie kyberbezpečnostné hry v Európe, pričom úlohy pripravujú odborníci z Národného centra kybernetickej bezpečnosti NBÚ. V ročníku 2025 súťaž obsahovala vetvy zamerané na malvérovú, forenznú a OSINT analýzu, kryptografiu, procesy a riadenie bezpečnosti a ofenzívnu bezpečnosť, každú s viacerými scenármi.

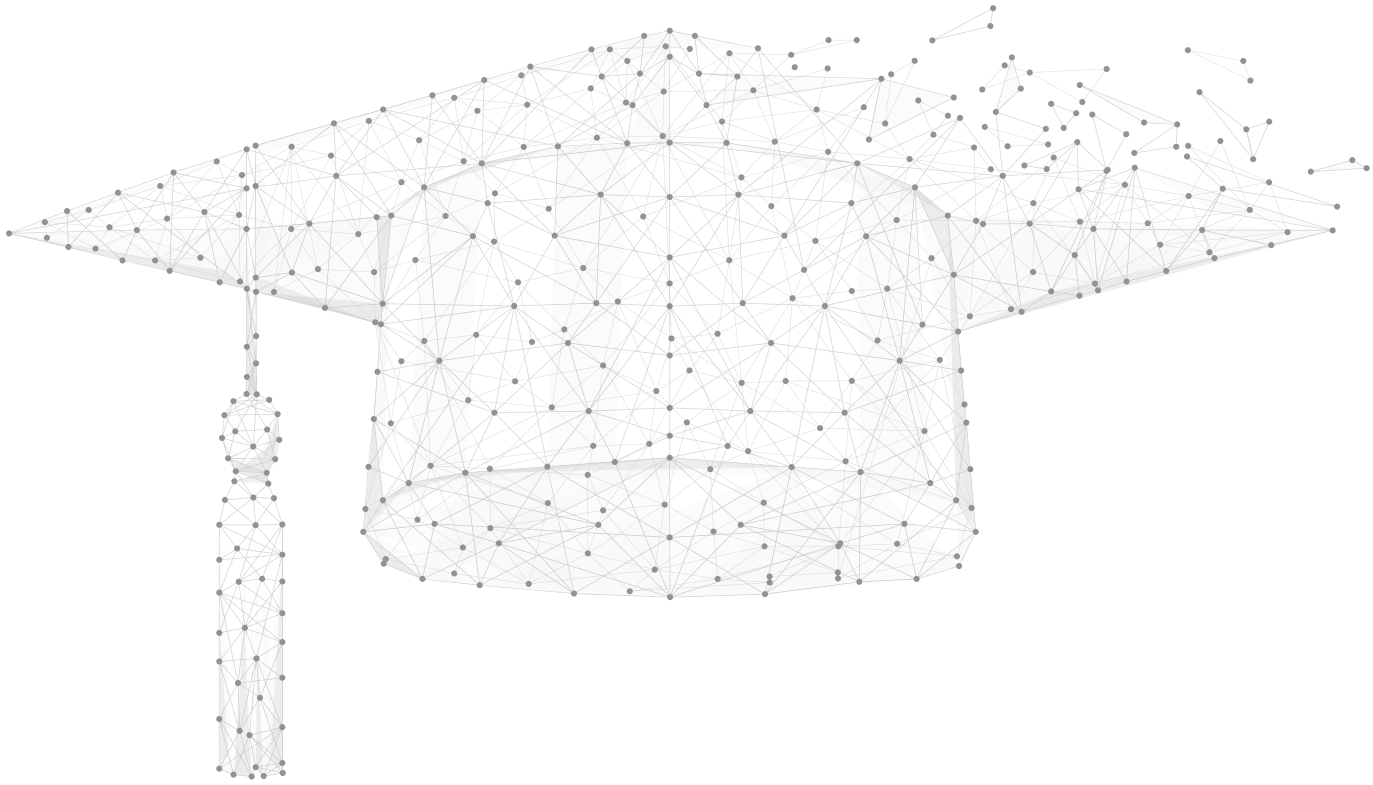
Scenáre pozostávali z úloh rôznej náročnosti, za ktorých splnenie hráči získavali vlajky a body podľa obtiažnosti. Za dokončenie celého scenára bola udelená bodová prémia. Hodnotenie prebiehalo automatizovane, úlohy na seba logicky nadväzovali a hráči si mohli zvoliť vetvy aj scenáre podľa vlastnej stratégie.

Profesionáli si vďaka CyberGame overujú svoje skúsenosti a študenti na nej počas vyučovania riešia úlohy z rôznych hracích vetiev. Z najlepších hráčov do 25 rokov, ktorí sa do CyberGame zapoja, vzniká každoročne slovenský reprezentačný tím na medzinárodné súťaže. Základným poslaním CyberGame je hľadanie talentov na kyberbezpečnosť.

Vo štvrtom ročníku súťaže sa registrovalo viac ako 5300 účastníkov – od žiakov základných škôl až po profesionálov z IT. Bodovala viac ako polovica z nich. Počas desiatich týždňov riešili úlohy rôzneho zamerania, ktoré pripravili kolegovia z Národného centra kybernetickej bezpečnosti.

V roku 2025 obsahovala súťaž tri analytické vetvy – malvérovú, forenznú a OSINT analýzu. Ďalšia hracia vetva bola venovaná kryptografii, a tá netechnická mala názov procesy a riadenie bezpečnosti. Hráči riešili aj úlohy zamerané na ofenzívnu bezpečnosť.

Ocenenia za úspechy v CyberGame boli udelené absolútnemu víťazovi, najlepšiemu študentovi, najlepšej juniorke, najlepšej hráčke a organizátori odmenili aj najmladšieho účastníka, expertov vo vetvách, najlepšieho hráča z verejnej správy a učiteľa.



VZDELÁVANIE V OBLASTI KYBERNETICKEJ BEZPEČNOSTI

Príslušníci a zamestnanci NCKB sa podieľali na výučbe viacerých predmetov na vysokých školách. V rámci Fakulty informatiky a informačných technológií STU zabezpečovali výučbu predmetov Bezpečnosť informačných technológií (zameraného na softvérové zraniteľnosti), Bezpečnosť operačných systémov a Forenzná analýza. Na Fakulte elektrotechniky a informatiky STU v Bratislave zabezpečovali výučbu predmetu Manažment bezpečnostných incidentov. Spolupodieľali sa na zabezpečení odborného obsahu pre vzdelávací program Bezpečnostné štúdia na Právnickej fakulte Univerzity Komenského. Odborníci z NBÚ sa v akademickom prostredí pohybovali pomerne často, o čom svedčí aj účasť odbornom seminári Kybernetické bezpečnostné incidenty, ransomvér a trestnoprávna zodpovednosť. NCKB ako partner podporovalo Slovak Cyber Team, národnú reprezentáciu mladých talentov, a podieľalo sa na realizácií tréningových bootcampov.

Úrad sa aktívne zapájal do vzdelávacích aktivít aj výučbou predmetu Bezpečnosť novinárov v online prostredí na Filozofickej fakulte Univerzity Komenského v Bratislave a realizoval aj prednášky na stredných školách.

V rámci oblasti kybernetickej bezpečnosti sa Slovensko snaží čoraz viac snaží zapojiť ženy o čom svedčí aj národná kapitola Women4Cyber, v rámci ktorej pôsobili odborníci z SK-CERT ako mentori v polročnom mentoringovom programe zameranom na prehlbovaní odborných znalostí.

Národný bezpečnostný úrad v spolupráci s partnermi pripravil dve konferencie zo série Kyber2025 na tému novej legislatívy a umelej inteligencie, ako aj ďalšie odborné podujatia. Prednáškami, workshopmi, ako aj aktívnou účasťou prispeli do odborného programu viacerých významných konferencií v oblasti kybernetickej bezpečnosti, ako sú ITAPA, EPI konferencia Kybernetická bezpečnosť, OpenCamp 2025, SlovakiaTech Fórum-Expo, Cyber Security Bratislava, Kybernetická bezpečnosť v doprave a nová smernica NIS2. Zástupcovia NCKB sa podieľali aj na tvorbe programu konferencie FIRSTCON25 v Kodani. Zúčastnili sa väčších ale aj menších odborných podujatí s cieľom zvýšiť povedomie o kybernetickej bezpečnosti u rôznych cieľových skupín

V roku 2025 Národný bezpečnostný úrad systematicky posilňoval povedomie o kybernetickej bezpečnosti aj prostredníctvom médií a vlastných komunikačných kanálov vrátane sociálnych sietí. Úrad zaznamenal nárast mediálnej prítomnosti a pravidelne vystupoval v tlačených, online aj audiovizuálnych médiách, čím prispel k širšiemu informovaniu verejnosti o aktuálnych kybernetických hrozbách a preventívnych opatreniach. Komunikačné aktivity sa zameriavali najmä na ochranu zariadení, riziká spojené s využívaním umelej inteligencie, phishingové útoky a ransomvér, ako aj na praktické odporúčania pre bezpečné správanie sa v online priestore, vrátane období dovoleniek a pobytu v zahraničí. Osobitná pozornosť bola venovaná rodičom a ochrane detí v digitálnom prostredí.

V komunikačnej oblasti sa venoval aj odborným a legislatívnym témam, najmä smernici NIS2, novele zákona o kybernetickej bezpečnosti a novým vyhláškam úradu, pričom informoval aj o možnostiach čerpania finančných prostriedkov z fondov Európskej únie v oblasti kybernetickej bezpečnosti. Úrad zároveň so štátnymi aj súkromnými spoločnosťami podpísal Deklaráciu o spolupráci pri ochrane seniorov pred podvodmi.

ORGÁN PRE POSUDZOVANIE ZHODY V OBLASTI KYBERNETICKEJ BEZPEČNOSTI

Ako súčasť implementácie opatrení vyplývajúcich z novely zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti, zameraných na znižovanie rizík spojených s dynamickým technologickým vývojom a digitalizáciou, zvyšovanie celkovej úrovne kybernetickej bezpečnosti v podmienkach Slovenskej republiky a podporu domácich výrobcov a dodávateľov IT riešení, zriadil Národný bezpečnostný úrad orgán pre posudzovanie zhody v oblasti kybernetickej bezpečnosti a začlenil ho do svojej organizačnej štruktúry.

Úrad ako prvý subjekt v Slovenskej republike preukázal spôsobilosť vykonávať akreditovanú činnosť splnením požiadaviek normy ISO/IEC 17065:2012 na certifikáciu produktov v oblasti hodnotenia kybernetickej bezpečnosti IKT podľa európskej certifikačnej schémy založenej na spoločných kritériách (EUCC).

Týmto krokom sa Slovenská republika ako siedma členská krajina Európskej únie (po Nemecku, Švédsku, Francúzsku, Španielsku, Holandsku a Taliansku) plnohodnotne zapojila do systému zabezpečujúceho automatické uznávanie certifikátov kybernetickej bezpečnosti vydaných certifikačnými orgánmi v rámci Európskej únie vo všetkých štátoch Európskeho hospodárskeho priestoru.

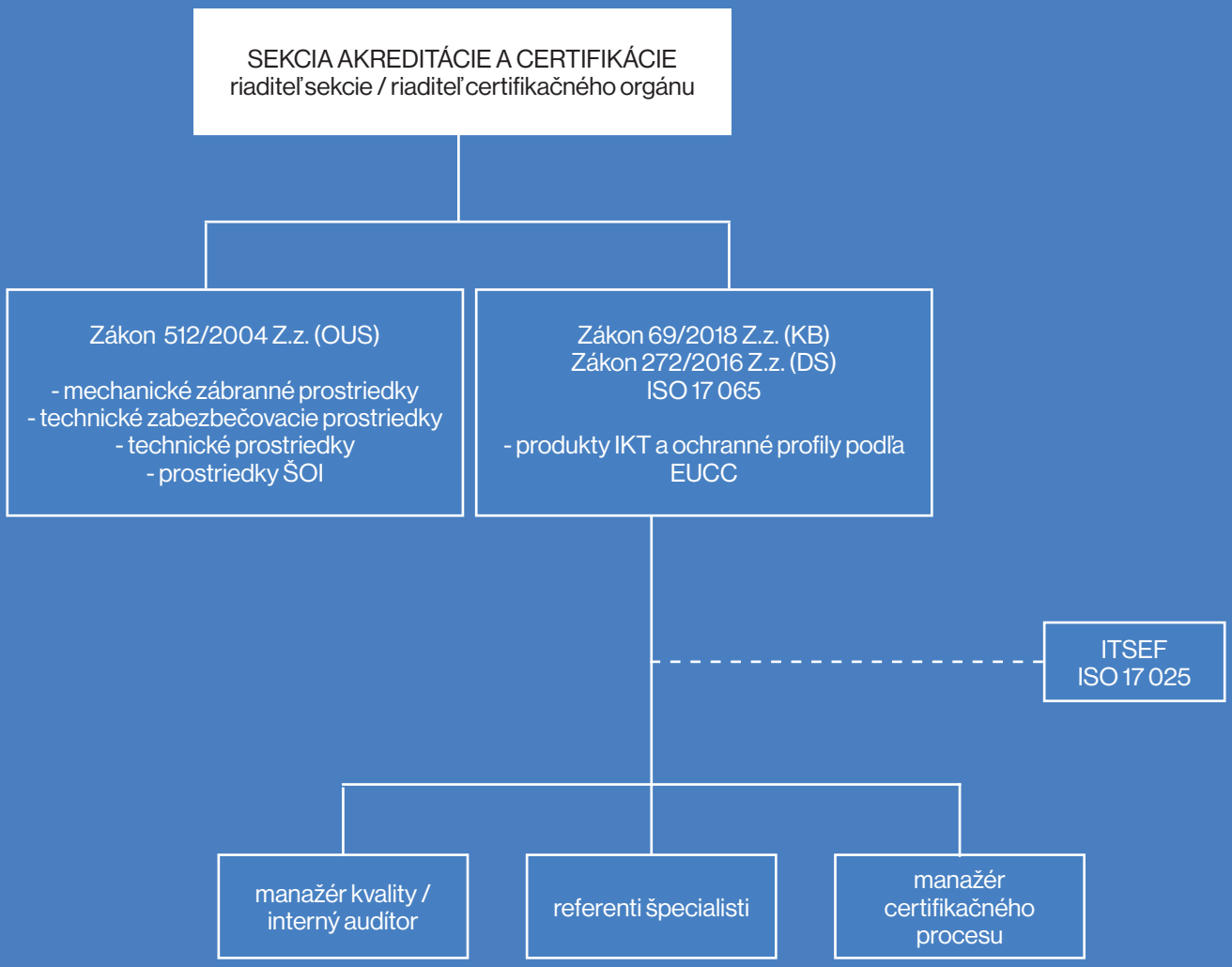
Certifikačný orgán je akreditovaný podľa požiadaviek normy ISO/IEC 17065: 2012 a notifikovaný v systéme NANDO (New Approach Notified and Designated Organisations) Európskej komisie na výkon certifikácie v oblasti hodnotenia kybernetickej bezpečnosti IKT produktov.

Certifikačný orgán podľa rozsahu akreditácie vykonáva činnosti posudzovania zhody na úrovni „Významná“ (Substantial) zodpovedajúcej AVA_VAN do úrovne 2 vrátane, respektíve EAL do úrovne 3 vrátane v súlade s:

- Nariadením Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013
- Vykonávacím nariadením Komisie (EÚ) 2024/482 z 31. januára 2024, ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881, pokiaľ ide o prijatie európskej schémy certifikácie kybernetickej bezpečnosti založenej na spoločných kritériách (EUCC)
- Spoločnými kritériami pre hodnotenie bezpečnosti informačných technológií, ako je stanovené v normách ISO/IEC 15408-1:2022, ISO/IEC 15408-2:2022, ISO/IEC 15408-3:2022, ISO/IEC 15408-4:2022, ISO/IEC 15408-5:2022
- Spoločnou metodikou pre hodnotenie bezpečnosti informačných technológií, ako je stanovené v norme ISO/IEC 18045:2022

Certifikačný orgán nenesie zodpovednosť voči žiadateľovi/držiteľovi certifikátu za škody spôsobené neudelením, odobratím, pozastavením alebo skončením platnosti certifikátu.

ORGANIZAČNÁ SCHÉMA CERTIFIKAČNÉHO ORGÁNU



NÁRODNÁ AUTORITA PRE CERTIFIKÁCIU KYBERNETICKEJ BEZPEČNOSTI

Európsky parlament a Rada (EÚ) v roku 2019 prijali a v roku 2025 novelizovali nariadenie 2019/881 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií (IKT), nazývaný Akt o kybernetickej bezpečnosti (**CSA**). V sledovanom období bol v dynamickom rozvoji aj celoeurópsky systém certifikácie kybernetickej bezpečnosti produktov IKT, služieb IKT, procesov IKT a riadených bezpečnostných služieb, ktorý má zvýšiť ich dôveryhodnosť.

V roku 2025 bolo preto potrebné reflektovať úlohy na úseku kybernetickej bezpečnosti vyplývajúce z členstva Slovenskej republiky v EÚ, a na to nadväzujúcimi európskymi legislatívnymi normatívnymi aktmi a národnými všeobecne záväznými právnymi predpismi.

Certifikácia podľa európskych schém certifikácie kybernetickej bezpečnosti v je v prostredí Slovenskej republiky riadená a koordinovaná Národným bezpečnostným úradom, ktorý v SR plní úlohy Národnej autority pre certifikáciu kybernetickej bezpečnosti (NCCA). NCCA je zriadená zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti a v rámci svojej činnosti v predmetných oblastiach priamo komunikuje s Európskou komisiou a agentúrou ENISA. Kompetencie NCCA priamo definuje Akt o kybernetickej bezpečnosti (**CSA**) vo svojom čl. 58.

V kontexte potrieb napĺňania odborných úloh v oblasti kybernetickej bezpečnosti nastala v roku 2025 zmena v organizačnej štruktúre NBÚ. Pre účely plnenia úloh a činnosť NCCA ustanovil riaditeľ NBÚ v zmysle organizačnej štruktúry NBÚ nezávislé postavenie dvom organizačným útvarom vo vecných otázkach, ktorými sú:

- Národný orgán pre kyberbezpečnostnú certifikáciu (NOKC), a
- Sekcia pre akreditáciu a certifikáciu (SAC).

NOKC a SAC sú navzájom nezávislé organizačné útvary a svoje úlohy a povinnosti plnia oddelene od seba, nezávisle, nestranne a v súlade s príslušnými právnymi predpismi a internými ustanoveniami NBÚ.

NOKC pre potreby zverejňovania informácií z úrovne NCCA vytvoril webovú stránku NCCA (https://ncca.nbu.gov.sk/), kde začal publikovať informácie súvisiace s certifikáciou podľa európskych schém kybernetickej bezpečnosti, EUDIW, dohľadu nad trhom, ako aj bežiacich projektov, výziev, vrátane budovania knižnice informácií.

NOKC zabezpečuje implementáciu kybernetických bezpečnostných cieľov EÚ do prostredia SR s úlohou reflektovať bezpečnostné záujmy a ciele SR. Medzi hlavné povinnosti NOKC sa radí zabezpečenie plnenia úloh vyplývajúcich z požiadaviek:

- CSA,
- Aktu o kybernetickej odolnosti (CRA) a s nimi súvisiaceho plnenia úloh orgánu dohľadu nad trhom,
- tvorba národných certifikačných schém,
- tvorba národnej certifikačnej schémy a koordinácia prípravy národného riešenia európskej peňaženky digitálnej identity (EUDIW),
- vzdelávanie a riadenie súvisiacich projektov v oblasti kybernetickej bezpečnosti.

EURÓPSKE SCHÉMY CERTIFIKÁCIE KYBERNETICKEJ BEZPEČNOSTI PODĽA CSA

a) Schéma EUCC

V roku 2025 bola v súlade s CSA novelizovaná európska schéma certifikácie kybernetickej bezpečnosti založenej na spoločných kritériách (EUCC). Schéma vychádza z celosvetovo uznávanej schémy a je použiteľná výhradne pre IKT produkty. Zahŕňa úroveň záruky „významná“ a „vysoká“ a nie je v nej možné aplikovať posúdenie zhody samohodnotením (conformity self-assessment). Platnosť certifikátu je stanovená na päť rokov a je ho možné obnoviť.

NOKC sa v roku 2025 sústredil najmä na implementáciu práve tejto EUCC do národného prostredia. Pre tento účel v roku 2025 spracoval a zverejnil šesť metodických usmernení a šesť pokynov riaditeľa NOKC súvisiacich s certifikáciou podľa EUCC. Dokumenty sú spracované v kontexte §5 ods. 1 písm. ab) zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov. Zároveň v tomto kontexte vznikol na NBÚ nezávislý Certifikačný orgán NBÚ.

b) Schéma EUCS

Ďalším návrhom európskej schémy certifikácie kybernetickej bezpečnosti je schéma pre certifikáciu cloudových služieb (EUCS). Na rozdiel od schémy EUCC pokrýva služby a zahŕňa všetky tri úrovne záruky – „základnú“, „významnú“ a „vysokú“. Poskytovateľom cloudových služieb však neumožňuje posúdenie zhody samohodnotením (conformity self-assessment). Schéma EUCS je tiež stále iba v procese návrhu.

c) Schéma EU5G

Ďalším návrhom európskej schémy certifikácie kybernetickej bezpečnosti je oblasť 5G sietí. Návrh stavia na súbore opatrení pre kybernetickú bezpečnosť sietí 5G, pričom sa očakáva, že schéma pomôže tlmiť ďalšie riziká spojené s týmto ekosystémom. Schéma EUCS je stále iba v procese návrhu.

d) Schéma EUDIW

Kandidátska schéma EUDI Wallet (Európska schéma pre peňaženku digitálnej identity) poskytne občanom a osobám s pobytom v EÚ bezpečný a interoperabilný nástroj na overenie ich totožnosti, ukladanie a zdieľanie digitálnych dokumentov a prístup k verejným a súkromným službám vo všetkých členských štátoch. Cieľom peňaženky je štandardizovať procesy digitálnej identifikácie a zároveň zabezpečiť súkromie a bezpečnosť. Schéma bude operovať s úrovňou záruky: „Vysoká“. Medzi jej prínosy sa bude radiť možnosť identifikovania sa v širokej škále verejných a súkromných online služieb a spolu s vysokou úrovňou ochrany súkromia. Táto schéma je v súčasnosti vo vývoji. Predpokladá sa účinnosť cca Q4/2026. NOKC začal v roku 2025 práce na príprave národnej certifikačnej schémy EUDIW a pripravuje textovú časť schémy v spolupráci s prípravou technického a technologického riešenia EUDIW Ministerstvom vnútra SR.

e) Kandidátska schéma EUAI

Kandidátska schéma EUAI (Európska schéma pre umelú inteligenciu) sa aktuálne pripravuje a bude sa vzťahovať na certifikáciu kybernetickej bezpečnosti produktov s umelou inteligenciou. Zahŕňa podporu budúceho vývoja a škálovateľnosti AI modelov a stanovuje harmonizované pravidlá o umelej inteligencii, poskytuje vývojárom a používateľom umelej inteligencie jasné požiadavky a povinnosti, týkajúce sa konkrétneho použitia umelej inteligencie. Samotné Nariadenie AI, ktorým sa ustanovujú harmonizované pravidlá v oblasti AI, reflektuje oblasť rýchlo sa rozvíjajúcej skupiny technológií, ktorá prispieva k širokému spektru hospodárskych, environmentálnych a spoločenských prínosov vo všetkých odvetviach a spoločenských činnostiach. Zlepšením predpovedí, optimalizáciou operácií a prideľovania zdrojov, ako aj personalizáciou digitálnych riešení, ktoré sú k dispozícii jednotlivcom a organizáciám, môže využívanie AI poskytnúť podnikom kľúčové konkurenčné výhody a podporiť sociálne a environmentálne priaznivé výsledky.

f) Kandidátska schéma EUMSS

Schéma EUMSS vzniká na základe CSA, konkrétne podľa dodatku, ktorý definuje riadené bezpečnostné služby (MSS - Managed Security Services) ako subjekt/alebo oblasť, pre ktorú sa požaduje vypracovanie kandidátskej schémy. MSS sú zamerané na poskytovanie bezpečnostných funkcií organizáciám (ako sú monitoring, detekcia, reakcia na incidenty, obnova, ďalšie prevádzkové bezpečnostné úlohy) prostredníctvom externých alebo interných poskytovateľov. Kritickým dôvodom pre zavedenie EUMSS je vysoká diverzita prístupov a požiadaviek naprieč členskými štátmi – rozdiely v technických normách, prevádzkových štandardoch, legislatíve či orgánoch vykonávajúcich dohľad nad týmito službami. Cieľom je ustáliť harmonizované požiadavky, ktoré zlepšia dôveru, kvalitu a interoperabilitu. Schéma bude postavená na horizontálnej vrstve (minimálne požiadavky, ktoré musí spĺňať každý poskytovateľ MSS, bez ohľadu na špecifiká služby) a na vertikálnej vrstve (Profiles – špecifické technické a prevádzkové požiadavky podľa typu služby (napr. služby reagovania na incident, detekcie, zotavenia, či iné komponenty MSS). Schéma je aktuálne v príprave, skúma sa realizovateľnosť, tvoria sa profily služieb, definujú sa technické a organizačné štandardy.

NÁRODNÁ CERTIFIKAČNÁ SCHÉMA - OVEROVANIE ODBORNEJ SPÔSOBILOSTI LEKTORA ODBORNEJ PRÍPRAVY Z KYBERNETICKEJ BEZPEČNOSTI V CIVILNOM LETECTVE

V roku 2025 NOKC spracoval a NBÚ ako vlastník vydal národnú certifikačnú schému - Overovanie odbornej spôsobilosti lektora odbornej prípravy z kybernetickej bezpečnosti v civilnom letectve. Táto certifikačná schéma umožní lektorom kybernetickej bezpečnosti preukázať splnenie požiadavky §34b odseku 6 zákona č. 143/1998 Z. z. o civilnom letectve (letecký zákon) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. Akreditačným orgánom poskytujúcim akreditáciu podľa požiadaviek normy ISO/IEC 17024/2012 Posudzovanie zhody - Všeobecné požiadavky na orgány vykonávajúce certifikáciu osôb je na území SR pre účely tejto certifikačnej schémy Slovenská národná akreditačná služba (SNAS), ktorá na svojich stránkach zverejňuje zoznam akreditovaných certifikačných orgánov.

DOHĽAD NAD TRHOM PODĽA CRA

Dohľad nad trhom (na nepotravinové výrobky, na ktoré sa vzťahuje široké spektrum harmonizačných právnych predpisov EÚ) sa v EÚ organizuje taktiež na národnej úrovni na základe spoločného rámca stanoveného v Akte o kybernetickej odolnosti (CRA) a nariadení Európskeho parlamentu a Rady (EÚ) 2019/1020 z 20. júna 2019 o dohľade nad trhom a súlade výrobkov č. 2019/1020. V uvedenom kontexte v SR úlohy orgánu dohľadu nad trhom plní NBÚ (ako orgán zodpovedný za kontrolu výrobkov vstupujúcich cez vonkajšie hranice EÚ). Cieľom dohľadu nad trhom je prijať na národnej úrovni primerané opatrenia tak, aby sa zamedzilo sprístupneniu a používaniu nevyhovujúcich produktov IKT, služieb IKT alebo procesov IKT na trhu, a zároveň zabezpečiť, aby výrobky spĺňali platné požiadavky zaisťujúce vysokú úroveň ochrany verejných záujmov ako zdravie a bezpečnosť vo všeobecnosti, zdravie a bezpečnosť na pracovisku, ochrany spotrebiteľov, životného prostredia a verejnej bezpečnosti a akýkoľvek iný verejný záujem chránený právnymi predpismi EÚ.

VÝZVY A PROJEKTY V KONTEXTE EURÓPSKEHO SYSTÉMU CERTIFIKÁCIE KYBERNETICKEJ BEZPEČNOSTI

V oblasti výziev zverejnil v roku 2025 NOKC:

a) výzvu na predkladanie žiadostí o NFP na podporu získania akreditácie na schému certifikácie podľa EUCC 19.12.2024),

b) výzvu na predkladanie žiadostí o nenávratný finančný príspevok (ďalej len „NFP“) na podporu vzdelávania a odbornej prípravy vývojárov riešení v oblasti kybernetickej bezpečnosti (31.03.2025),

c) výzvu na predkladanie žiadostí o nenávratný finančný príspevok (NFP) na podporu vzdelávania a odbornej prípravy vývojárov riešení v oblasti kybernetickej bezpečnosti (2) (07.07.2025)

d) výzvu na predkladanie žiadostí o NFP na podporu získania akreditácie na schému certifikácie podľa EUCC v rámci finančnej podpory tretím stranám (18.07.2025),

e) výzvu na predkladanie žiadostí o NFP na podporu auditov kybernetickej bezpečnosti (07.08.2025),

f) výzvu na predkladanie žiadostí o NFP na podporu vzdelávacích programov v oblasti certifikácie a hodnotenia podľa požiadaviek schémy certifikácie kybernetickej bezpečnosti podľa EUCC, v rámci finančnej podpory tretím stranám (25.11.2025).

NCCA je prostredníctvom NOKC súčasťou projektov:

a) TrustBoost (iniciatíva zameraná na zvýšenie kybernetickej bezpečnosti, odolnosti a dodržiavania predpisov v celej EÚ. Jej hlavným cieľom je posilniť úsilie o spoluprácu v oblasti dodržiavania kybernetickej bezpečnosti a certifikácie),

b) TestCert-SK (projekt je zameraný na podporu dobrovoľných akreditačných, certifikačných a testovacích činností, najmä v súvislosti s očakávanými európskymi schémami certifikácie kybernetickej bezpečnosti. V rámci implementácie a prínosov plánuje projekt využiť okrem iného aj finančnú podporu pre tretie strany ako nástroj na motiváciu kľúčových zainteresovaných strán s podporou certifikácie svojich produktov. Ako sekundárny cieľ projekt nasmeruje svoju podporu priamo pre kyberbezpečnostné audity infraštruktúry malých a stredných podnikov).

VZDELÁVANIE EXPERTOV NCCA

Nosnou témou NOKC v oblasti vzdelávania bolo v roku 2025 hľadanie a vzdelávanie expertov, ktorých NOKC zaraďoval do databázy expertov NCCA. V rámci toho sa do databázy expertov podarilo priebežne zaradiť desať expertov NCCA.

NOKC zabezpečuje vzdelávanie expertov NCCA prostredníctvom postupov a pravidiel uvedených v Metodickom usmernení NCCA č. MU-04 **Databáza expertov NCCA**, kde sú definované základné, kvalifikačné aj osobnostné požiadavky na expertov NCCA vrátane požiadaviek na ich zručnosti. NOKC v rámci tejto činnosti zabezpečuje vyhodnotenie odbornej spôsobilosti žiadateľov a plánovanie spolupráce s nimi, predovšetkým v oblasti poskytovania technických expertíz a činností vyplývajúcich z požiadaviek európskych schém certifikácie kybernetickej bezpečnosti. Získané informácie tvoria základ pre registráciu expertov v databáze NCCA spravovanej NOKC, následné vzdelávanie, distribúciu interných materiálov a monitorovanie expertov NCCA. Spôsob a forma vzdelávania odzrkadľuje požiadavky na špecifikáciu odborných kompetencií a požiadaviek kladených na expertov NCCA v súlade s európskym systémom kybernetickej bezpečnosti a schémami certifikácie kybernetickej bezpečnosti a reflektuje požiadavky Článku 58, ods. 7 CSA v oblasti povinností a úloh NCCA, ako aj požiadavky Článku 58, ods. 8 CSA, podľa ktorého má NCCA určené minimálne právomoci.

Zároveň v roku 2025 NOKC zorganizoval:

a) odborné školenie s účasťou medzinárodných lektorov pre desať expertov NCCA, ktorí získali kompetencie hodnotiteľa podľa EUCC, ako aj

b) webinár pre 135 záujemcov na tému Certifikácia kybernetickej bezpečnosti pre IKT produkty.

Paralelne bol NOKC prizvaný do pozície pozorovateľa počas akreditácie prvého certifikačného orgánu podľa EUCC (Certifikačný orgán NBÚ) a zúčastnil sa odborného sympózia českého Národného úradu pre kybernetickú a informačnú bezpečnosť (NÚKIB) na tému CRA. Zároveň sa zamestnanci NOKC aktívne zúčastňovali odborných konferencií NBÚ v pozícii lektorov v oblastiach CSA a CRA.

Priestor pre ďalšie zlepšenie v predmetnej oblasti sa ukazuje v činnostiach NOKC smerovaných ku zvýšenej miere oslovovania odborníkov na kybernetickú bezpečnosť, a to nielen v prostredí štátnej a verejnej správy, ale najmä v súkromnom sektore.

PLÁNY NA ĎALŠIE OBDOBIE

V ďalšom období bude NOKC realizovať svoje úlohy tak, aby sa stal aktívnym a kompetentným lídrom na poli zaručenia najvyššej úrovne kybernetickej bezpečnosti a zvýšenia kybernetickej odolnosti SR. A to prostredníctvom podpory aktivít budujúcich dôveru občanov SR s dôrazom na maximalizovanie príležitostí, ktoré IKT ponúkajú v záujme posilnenia inovácií, výskumu, vývoja, konkurencieschopnosti a rastu.

Aktivity NOKC budú smerovať k pripravenosti na efektívnu ochranu kybernetického priestoru SR pred hrozbami súčasnými i budúcimi v súvislosti s účinnou pomocou všetkým zainteresovaným stranám pri ich predchádzaní a riešení.

V súvislosti s uvedeným bude v roku 2026 NCCA preverená v rámci vzájomného preskúmania (Peer Review), rotačnej medzinárodnej aktivity zahraničných NCCA, v rámci ktorej sa vzájomne preskúmava pripravenosť, schopnosť plnenia úloh a realizované činnosti jednotlivých NCCA členských štátov EÚ. Táto aktivita je významným prvkom v stabilizácii činnosti NCCA a medzinárodnému potvrdeniu jej funkčnosti, odbornosti a odborných kvalít.

V roku 2026 sa zároveň z úrovne NBÚ plánuje vydanie novej národnej legislatívy súvisiacej s požiadavkami CRA v oblasti dohľadu nad trhom. Táto bude reflektovať požiadavky na produkty vyrábané a predávané v EÚ, ktoré obsahujú „digitálne prvky“, pričom tieto musia spĺňať základné požiadavky kybernetickej bezpečnosti ustanovené nariadením CRA. Legislatíva sa bude uplatňovať na produkty s digitálnymi prvkami sprístupnenými na trhu EÚ, ktorých zamýšľaný účel alebo odôvodnene predvídateľné použitie zahŕňa priame alebo nepriame logické alebo fyzické dátové pripojenie k zariadeniu alebo sieti (pôjde o hardvérové produkty, napr. smartfóny, notebooky, produkty pre inteligentné domácnosti, inteligentné hodinky, hračky pripojené k internetu, ďalej o mikroprocesory, firewally a brány inteligentných meracích systémov v rámci inteligentných meracích systémov, ako aj o softvérové produkty, napr. účtovný softvér, počítačové hry, mobilné aplikácie, a pod.. Zo špecifického pohľadu (uvedeného v CRA) sa pripravovaná legislatíva bude týkať aj správcov softvérových produktov s otvoreným zdrojovým kódom (open source).

KOMPETENČNÉ A CERTIFIKAČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI

Štátna príspevková organizácia Kompetenčné a certifikačné centrum kybernetickej bezpečnosti (KCCKB), ktorá spadá pod NBÚ, plní úlohu Národného koordinačného centra (NCC-SK) v sieti európskych koordinačných centier a Európskeho centra priemyselných, technologických a výskumných kompetencií v zmysle nariadenia (EÚ) č. 2021/887. Akreditácia od Európskej komisie potvrdzuje expertízu a kapacitu KCCKB manažovať európske finančné fondy pre kybernetickú bezpečnosť z priamo riadených programov EÚ.

V roku 2025 uzavrelo Kompetenčné a certifikačné centrum kybernetickej bezpečnosti prvý projekt NCC, ktorý bol poskytnutý na roky 2022 – 2024 a v auguste bol úspešne obhájený pred Európskou komisiou. Projekt bol venovaný zvyšovaniu povedomia o kybernetickej bezpečnosti, vytvoreniu kyberkomunity, organizácii odborných podujatí a podpore malých a stredných podnikov v budovaní kapacít. Zároveň od júna 2025 beží nový projekt NCC2.0 na roky 2025-2029. Kompetenčné centrum ako koordinátor je súčasťou projektu „NIS2" spolu s Národným bezpečnostným úradom a Ministerstvom dopravy Slovenskej republiky. V júli 2025 prebehlo úspešné obhájenie všetkých vykonaných aktivít pred expertami z Európskej komisie.

V rámci aktivít Národného koordinačného centra bola v roku 2025 ukončená a vyhodnotená výzva FSTP-Kaskádové financovanie ako súčasť projektu NCC, ktorej cieľom bolo významne prispieť k posilneniu kyberbezpečnostných kapacít zapojených subjektov. Predmetom výzvy bolo vypracovanie bezpečnostnej dokumentácie. Podporu získalo 44 subjektov so svojimi projektmi.

Súčasťou cieľov kompetenčného centra v roli Národného koordinačného centra v roku 2025 bolo aj intenzívne budovanie odbornej kyberkomunity. Toto úsilie viedlo k vytváraniu silných partnerstiev, zdieľaniu osvedčených postupov a zvýšeniu povedomia o dôležitosti kybernetickej bezpečnosti medzi podnikmi, akademickou sférou a verejným sektorom. Členmi európskej komunity kybernetickej bezpečnosti podľa Nariadenia (EÚ) č. 2021/887 sa prostredníctvom NCC-SK stalo 197 slovenských subjektov.

Kompetenčné centrum zorganizovalo k EÚ projektom viacero vzdelávacích a networkingových aktivít, ako boli: Cyberbrunch, Cyberbreakfast, séria online webinárov NIS2, stretnutia pracovných skupín audítorov a manažérov kybernetickej bezpečnosti, semináre s témou transpozície smernice NIS2, európske webináre zamerané na to, ako získať európske financovanie aj s medzinárodnou účasťou. Celkovo sa na uvedených aktivitách počas roku 2025 zúčastnilo vyše 3000 účastníkov.

Významným aspektom Národného koordinačného centra v medzinárodnom pôsobení bola účasť v riadiacich štruktúrach na európskej úrovni, najmä prostredníctvom participácie na zasadnutiach Správnej rady ECCC a stretnutiach siete NCC. Kompetenčné centrum sa v úlohe NCC aktívne zapájalo aj do činností pracovných skupín ECCC, v rámci ktorých prispievalo k výmene informácií, koordinácii aktivít a zdieľaniu skúseností v oblastiach relevantných pre rozvoj kybernetickej bezpečnosti na európskej úrovni. Osobitná pozornosť bola venovaná bilaterálnej spolupráci s českým národným koordinačným centrom NCC-CZ. V roku 2025 bola táto spolupráca formalizovaná podpisom memoranda o porozumení, ktoré vytvorilo rámec pre systematickú výmenu informácií, koordináciu aktivít a prípravu spoločných iniciatív.

V rámci expertných činností pre verejnú správu vykonalo kompetenčné centrum 39 auditov kybernetickej bezpečnosti a tri konzultačné projekty. V roku 2025 bolo u viac ako 50 subjektov realizované meranie zamerané na posudzovanie technických prostriedkov proti úniku utajovaných skutočností prostredníctvom nežiaduceho elektromagnetického vyžarovania (NEV). Znalecká organizácia vytvorila spolu 20 znaleckých posudkov.

Počet certifikovaných osôb sa prostredníctvom kompetenčného centra v roku 2025 navýšil o troch certifikovaných audítorov (celkový počet je 80) a 46 certifikovaných manažérov kybernetickej bezpečnosti (celkový počet je 100). Kompetenčné centrum v roku 2025 nepredĺžilo akreditáciu na certifikáciu manažérskych systémov.

KCCKB bolo úspešné aj v oblasti vzdelávania dospelých ako certifikovaná vzdelávacia inštitúcia. Vzhľadom na novely zákona č. 69/2018 o kybernetickej bezpečnosti a príslušných vyhlášok, boli aktualizované sylaby takmer pre všetky vzdelávacie produkty. Do portfólia vzdelávania pribudli nové špecializované kurzy a workshopy zamerané na riešenie incidentov a bezpečnosť AI.

Za rok 2025 bolo realizovaných celkovo 34 školení. Portfólio odborných školení zahŕňa kurzy Základy KB, Manažér KB 1 a 2, Audítor KB, sedem špecializačných kurzov a workshopov, Kurz manažérstva informačnej bezpečnosti podľa ISO/IEC 27001:2022 a webinár Prehľad kybernetickej bezpečnosti s účelom zvyšovania povedomia o kybernetickej bezpečnosti. Celkovo sa na uvedených vzdelávacích aktivitách počas roku 2025 zúčastnilo 438 účastníkov.

Kompetenčné centrum sa aktívne zúčastňovalo na konferenciách a podujatiach na Slovensku aj v zahraničí. Celkovo jeho zástupcovia v roku 2025 uskutočnili 50 odborných prednášok na konferenciách, workshopoch, seminároch ako aj na pôde vybraných vysokých škôl v SR.

V rámci publikačných aktivít vydávalo kompetenčné centrum odborné články, letáky na účely zvyšovania bezpečnostného povedomia. Počas adventu 2025 bola vydaná séria článkov pre občanov Slovenskej republiky v kooperácií so Slovenskou bankovou asociáciou na ochranu pred najčastejšími útokmi, ktoré cielia na financie obyvateľov:

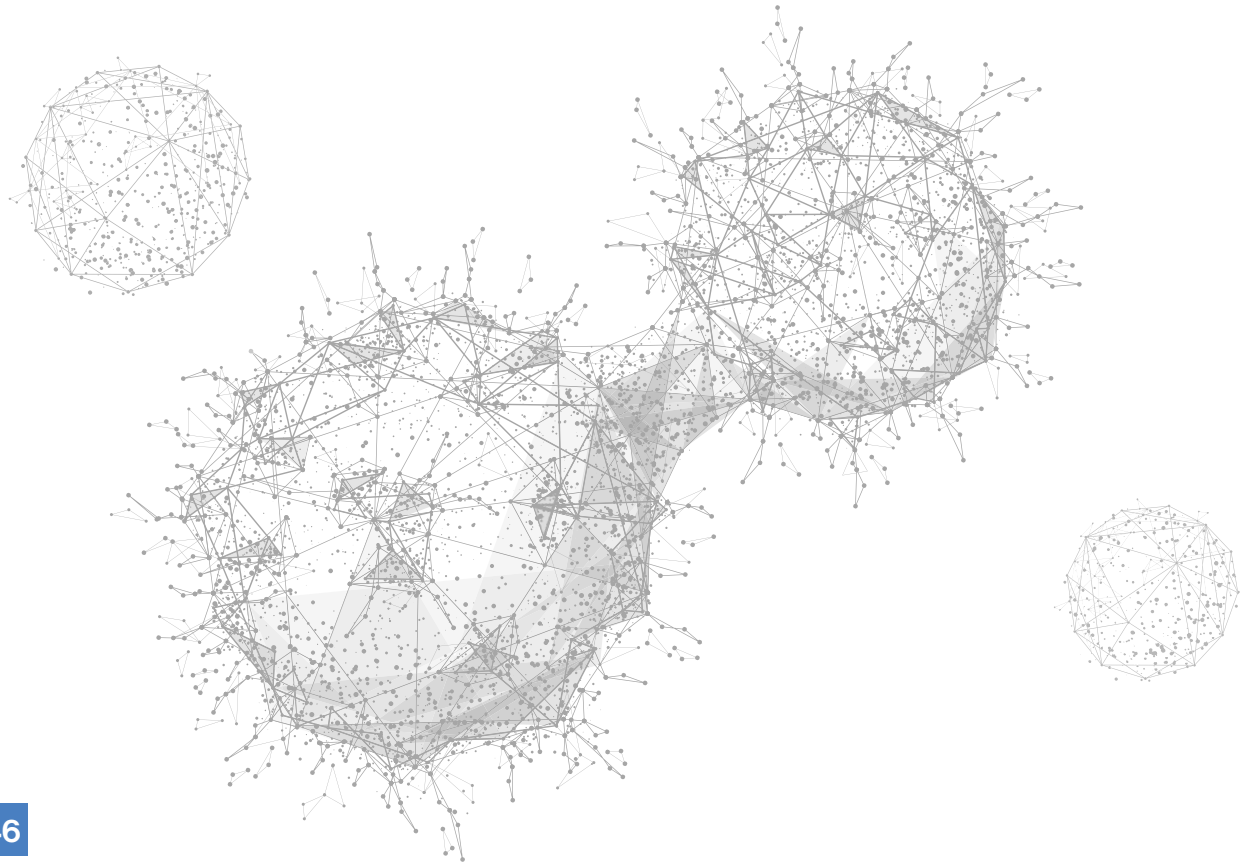
- Investičný podvod – lákavá ilúzia rýchleho zisku
- Phishing – ako funguje, ako ho rozpoznať a ako sa chrániť
- Whatsapp podvod – hlasujte za tanečnicu
- Útoky na online bazároch – aj predaj môže byť nebezpečný

Kompetenčné centrum vydalo v roku 2025 knihu Návrh vzdelávacích osnov pre II. St. ZŠ pre oblasť informačnej a kybernetickej bezpečnosti a odporúčané moderné didaktické metódy s príkladmi. Kniha nastavila základ vzdelávacích osnov pre druhý stupeň základných škôl. Svojou odbornou činnosťou prispelo k podpore NBÚ pri príprave a vypracovaní Metodiky analýzy rizík kybernetickej bezpečnosti a Odporúčaní pre kryptografické algoritmy.

Už každoročne sú na základe zadania kompetenčného centra spracované prieskumy stavu kybernetickej bezpečnosti, vydané následne aj vo forme verejného dokumentu. V roku 2025 bol uskutočnený prieskum verejnej mienky medzi verejnosťou na vzorke tisíc respondentov.

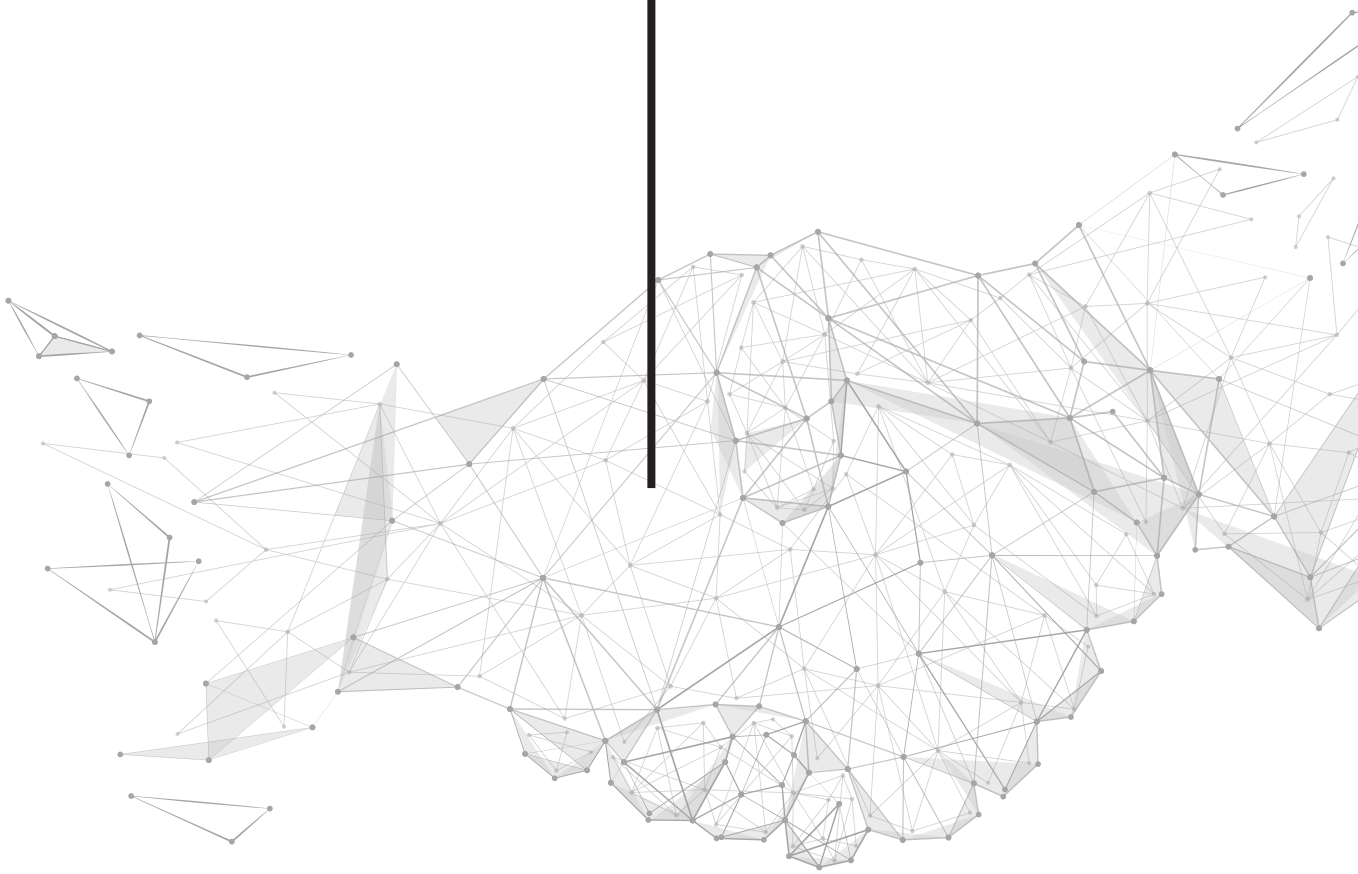
Aj v roku 2025 KCCKB rozširovalo okruh organizácií, s ktorými uzatvorilo spoluprácu formou podpisu memoranda.

Kompetenčné centrum s podporou NCKB rozširuje tím mladých talentovaných ľudí, ktorí Slovensko úspešne reprezentovali na viacerých prezenčných CTF turnajoch (Dublin Zerodays CTF 1.miesto, Bukurešť DCTF 4.miesto) a na množstve online CTF turnajov. Slovak Cyber Team v októbri 2025 na podujatí European CyberSecurity Challenge (ECSC) vo Varšave skončil na fantastickom 4.mieste, spomedzi 39 národných tímov. Aktivitu zastrešuje Európska agentúra pre kybernetickú bezpečnosť (ENISA) a ECCC. Slovak Cyber Team reprezentovalo desať mladých talentov – deväť chlapcov a jedno dievča. Na súťaž sa tím pripravoval niekoľko mesiacov. V júli sa zúčastnili medzinárodného bootcampu vo Viedni a následne šiestich tréningových bootcampov v Brunovciach. Tím sa aktívne pripravuje na účasť na ECSC v roku 2026.



08.

MEDZINÁRODNÁ SPOLUPRÁCA



Príslušníci úradu rozvíjajú vzťahy so zahraničnými partnermi na dennej báze naprieč desiatkami organizácií, platforiem aj formátov. NBÚ v roku 2025 potvrdil svoje smerovanie v budovaní bezpečnostného prostredia, ktoré zodpovedá princípom prijatým v Stratégii Európskej únie pre bezpečnostnú úniu na obdobie rokov 2020 až 2025 a v Stratégii kybernetickej bezpečnosti Európskej únie v digitálnej dekáde.

Prioritami naďalej zostávajú zvyšovanie odolnosti kybernetickej infraštruktúry, kybernetickej bezpečnosti a nastavovanie procesov na zaistenie bezpečnosti vo fyzickom i v digitálnom prostredí.

Európska únia

Pokiaľ ide oblasť ochrany utajovaných skutočností na úrovni EÚ sa príslušníci úradu v roku 2025 naďalej prezenčne zúčastňovali na pravidelných zasadnutiach najmä Bezpečnostného výboru Rady EÚ (ďalej len „CSC“), Bezpečnostného výboru Európskej služby pre vonkajšiu činnosť (ďalej len „Bezpečnostný výbor EEAS“), Expertnej skupiny pre personálnu bezpečnosť EEAS, Implementačnej pracovnej skupiny pre TEMPEST (ďalej len „ITTF“), Expertnej skupinu Rady EÚ pre technické bezpečnostné prehliadky (ďalej len „CSC-TSCM EG“), Skupiny expertov Európskej komisie pre bezpečnostnú politiku (ďalej len „ComSEG“), Bezpečnostného výboru Agentúry Európskej únie pre vesmírny program alebo Rady pre bezpečnostnú akreditáciu Agentúry Európskej únie pre vesmírny program

Na pôde Rady EÚ sa aj v roku 2025 rokovania CSC primárne zameriavali na dlho očakávané ukončenie rozsiahlej revízie bezpečnostných predpisov Rady na ochranu utajovaných skutočností EÚ [1] (EUCI) s cieľom odstrániť nedostatky identifikované v aplikačnej praxi a za účelom zvýšenia komfortu pre adresátov týchto predpisov. Úrad sa v danom pracovnom formáte aktívne podieľal na príprave bezpečnostných noriem s cieľom zvýšiť úroveň ochrany utajovaných skutočností a zároveň sa aktívne zapájal aj do procesu revízie bezpečnostných predpisov. Napriek tomu, že jednotlivé kapitoly revízie sa priebežne uzatvárali počas niekoľkých mesiacov (a rokov), pri predstavení už kompletného balíčka sa rokovania nezaobišli bez diskusií k už uzavretým kapitolám, čo proces ukončovania a schvaľovania predĺžilo až do konca roka 2025. Schválený text revízie bezpečnostných predpisov Rady na ochranu utajovaných skutočností EÚ (EUCI) na úrovni CSC bude začiatkom roka 2026 smerovať na lingvisticko-právne posúdenie, neskôr na schválenie COREPER a následne na prijatie a schválenie Radou EÚ. Rovnako ani minuloročná ambícia predsedajúceho CSC o ukončení pripomienkovania návrhu nariadenia Európskeho parlamentu a Rady EÚ o bezpečnosti informácií v inštitúciách, orgánoch, úradoch a agentúrach Únie (EUIBAs) sa nenaplnila a na poslednom rokovaní CSC v roku 2025 uviedol, že v ideálnom prípade, ak sa budú jednotlivé chýbajúce kapitoly prediskutovávať bez prieťahov, je možné očakávať jeho uzavretie až koncom roka 2026.

Bezpečnostný výbor EEAS v roku 2025 naďalej pokračoval v blízkej spolupráci a transparentnej informovanosti CSC, s ktorým zdieľal detaily aktuálnych aktivít a vývoja v oblasti ochrany utajovaných skutočností. Zasadnutia Bezpečnostného výboru EEAS sa v roku 2025 venovali najmä novému programu zvyšovania bezpečnostného povedomia do vnútra organizácie, rozvíjaniu spolupráce s tretími krajinami a medzinárodnými organizáciami, ako aj zlepšovaniu zabezpečenia informačných systémov využívaných civilnými aj vojenskými štruktúrami EEAS. Bezpečnostný výbor EEAS v roku 2025 aktualizoval niekoľko regulačných rámcov zameraných na vyššie personálno-bezpečnostné štandardy a zároveň zavádzajúcich vylepšené procesy a osvedčené postupy, pri čom sa inšpiroval modelom NATO.

V roku 2025 bol počas zasadnutia ITTF predstavený projekt novej budovy Európskej obrannej agentúry (EDA) “The Muse”, s cieľom implementácie požiadaviek a princípov TEMPEST ochrany už v počiatočných štádiách realizácie projektu, a to najmä s ohľadom na veľké množstvo spracovávaných utajovaných informácií do stupňa utajenia SECRET UE/EU SECRET. V nadväznosti na revíziu bezpečnostných predpisov Rady EÚ na ochranu utajovaných skutočností EÚ (EUCI) sa začal proces pripomienkovania bezpečnostnej politiky EÚ pre TEMPEST ochranu (“TEMPEST Information Assurance Security Policy“) a nadväzujúcich príručiek.

Bezpečnostná politika EÚ pre TEMPEST ochranu je jedným z východiskových dokumentov pre Bezpečnostný štandard Národného bezpečnostného úradu pre ochranu pred nežiaducim elektromagnetickým vyžarovaním.

CSC-TSCM EG bola navrhnutá a následne CSC schválená metodika pre vykonávanie technických bezpečnostných prehliadok pre ochranu utajovaných informácií EÚ “Guidelines for minimum Technical Surveillance Counter Measures for the protection of EU classified information (R-UE/EU-R)“.

Vzhľadom k neexistencii národnej metodiky v Slovenskej republike pre vykonávanie technických bezpečnostných prehliadok ide o podstatný dokument pre vykonávanie technických bezpečnostných prehliadok v rámci SR.

[1] Rozhodnutie Rady 2013/488/EÚ o bezpečnostných predpisoch na ochranu utajovaných skutočností EÚ.

20. februára 2025 sa uskutočnilo 17. **Bezpečnostné sympózium**, ktoré organizuje Európska komisia (ďalej aj „Komisia“) s názvom „Bezpečnosť EÚ v časoch permanentnej krízy - Inovatívne riešenia pre bezprecedentné výzvy“. Sympózium spojilo bezpečnostných expertov, tvorcov politík a odborníkov z praxe v Bruseli, aby sa zaoberali vyvíjajúcou sa situáciou v oblasti hrozieb a identifikovali potenciálne zraniteľnosti. Podporilo spoluprácu medzi rôznymi bezpečnostnými komunitami vrátane zástupcov inštitúcií EÚ, členských štátov, medzinárodných organizácií a akademickej obce. Zainteresované strany sa tak venovali problematike pripravenosti EÚ na neustále sa vyvíjajúcu panorámu hrozieb a úlohu ľudského faktora v predkrízovej fáze a v oblasti informačnej bezpečnosti.

Rokovania **ComSEG** boli v roku 2025 zamerané na zdieľanie informácií o aktuálnej panoráme hrozieb – o interných a externých hrozbách, ktorým čelia inštitúcie EÚ. Taktiež boli prezentované nové bezpečnostné pravidlá, ktoré nastavila Komisia pre outsourcované služby/firmy, ako aj princípy ochrany neutajovaných informácií Komisie citlivého charakteru v systémoch umelej inteligencie. Najdlhšiu diskusiu si vyžiadala problematika vykonávania bezpečnostných previerok osôb dlhodobo žijúcich mimo pôsobnosti bezpečnostného úradu krajiny, ktorej je daná osoba občanom, ktorý však aj napriek tomuto faktu musí previerku vykonať. Zložitejší proces pre Komisiu predstavuje, ak osoba dlhodobo žije v krajine mimo členského štátu EÚ. Táto problematika bola predmetom diskusie aj na stretnutí expertov členských štátov EÚ zameranom na personálnu bezpečnosť, ktoré sa koncom roka uskutočnilo v priestoroch Európskeho parlamentu a na ktorého príprave sa aktívne podieľali EEAS, Európska komisia, Rada EÚ a Európsky parlament. Európsky parlament a EEAS predstavili svoje virtuálne programy na budovanie a posilnenie bezpečnostného povedomia, ktoré by mohli byť využité aj na národných úrovniach a nielen pre zamestnancov spomínaných inštitúcií.

Úrad sa zúčastňoval aj pravidelných zasadaní bezpečnostných akreditačných výborov a pracovných skupín EÚ zameraných predovšetkým na bezpečnosť utajovaných informácií, s ktorými sa manipuluje v rámci utajovaných systémov v súlade s bezpečnostnými politikami cudzej moci. Zároveň sa tieto rokovania týkali aj adaptácie súboru nových pravidiel, požiadaviek a ich aplikovania v reakcii na vyvíjajúce sa technológie a bezpečnostnú situáciu vo svete.

V oblasti kybernetickej bezpečnosti sa rok 2025 niesol najmä v znamení implementácie už prijatej legislatívy v národnom prostredí ako je kľúčová **horizontálna smernica o zabezpečení vysokej úrovne kybernetickej bezpečnosti v Únii** (smernica **NIS2**), ktorá sa zameriava na zvyšovanie kybernetickej bezpečnosti v organizáciách a kritických sektoroch a ktorá upravuje povinnosti pre regulované sektory. Jej cieľom je, aby tieto subjekty mali jasne stanovené procesy riadenia rizík, zaviedli primerané bezpečnostné opatrenia a včas hlásili významné kybernetické bezpečnostné incidenty.

Implementácia sa ďalej týkala **aktu o kybernetickej odolnosti (nariadenie CRA)**, ktorý sa sústreďuje na produkty s digitálnym prvkom – softvér, hardvér, internet vecí a iné. Stanovuje pre výrobcov povinnosť navrhovať produkty bezpečne „secure by design“, pravidelne ich aktualizovať, riešiť zraniteľnosti počas celého životného cyklu a transparentne informovať o rizikách. Na národnej úrovni sa preto tvoril systém, ktorý má umožniť požadovanú certifikáciu a následný dohľad nad certifikovanými produktami.

Aktívna a najmä komplexná práca sa týkala okrem iného aj implementácie **nariadenia o stanovení rámca pre európsku digitálnu identitu (nariadenie eIDAS 2)**, ktorým sa zavádza európska peňaženka digitálnej identity. Národné riešenie peňaženky musí spĺňať spoločne dohodnuté technické špecifikácie, aby bolo vzájomne interoperabilné s ostatnými členskými štátmi EÚ, čomu bude predchádzať náležitá certifikácia riešenia a jeho partnerské preskúmanie. V priebehu roka 2025 sa konali technické výbory na úrovni Komisie, ktorých výsledkom bolo vydanie implementačných nariadení Komisie vo vestníku EÚ. Zavedením aktualizovaných pravidiel elektronickej identifikácie vrátane európskej peňaženky digitálnej identity sa vytvoril pevný a právne nespochybniteľný základ spoločného chráneného digitálneho priestoru v Európskej únii. Slovenská republika, prostredníctvom príslušníkov úradu, počas celého roka 2025 aktívne zasielala množstvo pripomienok a komentárov, ktoré boli pozitívne prijaté a slúžili na zefektívnenie a racionalizáciu prerokovávaných právnych noriem.

Na nariadenie eIDAS 2 koncom novembra 2025 nadviazal **nový akt o európskej peňaženke podnikateľa (nariadenie EBW)**, ktorého cieľom je umožniť firmám a iným právnym subjektom jednoduchú, rýchlu a bezpečnú komunikáciu, výmenu dokumentov a overovanie totožnosti naprieč EÚ. Jeho riadne prerokovanie sa uskutoční až počas cyperského predsedníctva v roku 2026.

Vo februári 2025 z dôvodu administratívneho korigenda po výmene Európskeho parlamentu vstúpilo do účinnosti **nariadenie o kybernetickej solidarite (nariadenie CySOLa)**, ktoré sa sústredilo na spoločnú ochranu a reakciu EÚ pri kybernetických bezpečnostných incidentoch väčšieho rozsahu. Zavádza celoeurópsky systém detekcie kybernetických hrozieb, sieť cezhraničných „cyber hubov“, mechanizmy koordinovanej reakcie a tzv. európsku kybernetickú rezervu – skupinu odborníkov a kapacít, ktoré môžu byť nasadené pri útokoch. Jeho cieľom je zlepšiť pripravenosť štátov a umožniť rýchlu, koordinovanú reakciu na incidenty presahujúce hranice jedného štátu. Záverom roka 2025 Moldavsko požiadalo o pomoc z rezervy na účely kybernetickej bezpečnosti. Komisia po posúdení žiadosti predložila Rade EÚ návrh na prijatie vykonávacieho aktu, ktorým by sa povoľovalo poskytnutie podpory Moldavsku.

Rada EÚ prijala v júni 2025 aktualizované odporúčanie, ktoré definuje, ako má EÚ a členské štáty EÚ reagovať na rozsiahle kybernetické bezpečnostné incidenty alebo kybernetické krízy. Tzv. **blueprint** stanovuje jednotný postup v rámci celej EÚ od detekcie, analýzy, eskalácie, reakcie až po zotavenie po incidente. Zároveň zdôrazňuje potrebu koordinácie medzi jednotlivými aktérmi. Na jeseň 2025 sa tiež v Rade EÚ na úrovni pracovnej skupiny uskutočnilo praktické cvičenie, ktoré premostilo navrhované procesy do praxe.

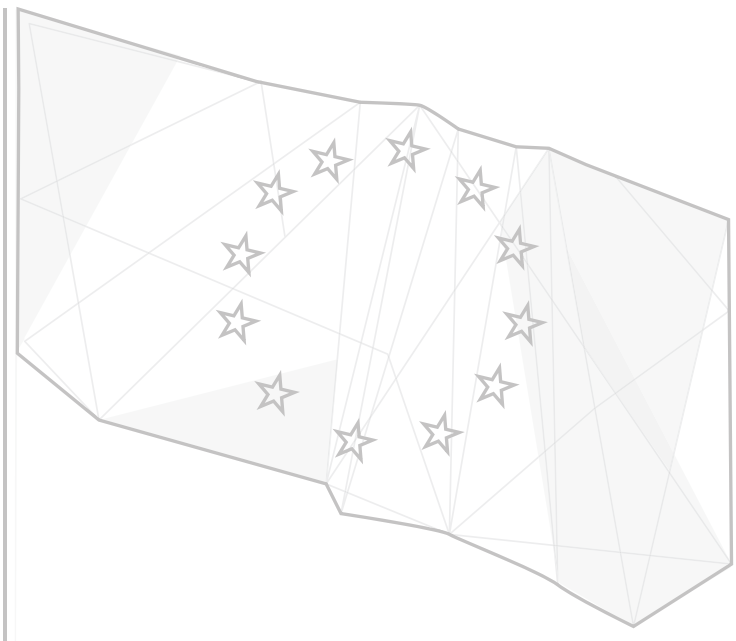
Komisia predstavila **simplifikačný omnibus** pre digitálnu agendu, ktorého súčasťou je aj harmonizácia notifikácií kybernetických bezpečnostných incidentov už prijatej rôznej legislatívy, ako je nariadenie GDPR, nariadenie CRA, smernica NIS2, smernica CER, nariadenie DORA. V lete 2025 zároveň Komisia publikovala návrh **nariadenia o bezpečnosti, odolnosti a udržateľnosti vesmírnych (Vesmírny akt, EUSA)**, ktorý obsahuje aj kyberbezpečnostné prvky a najmä sa definuje ako lex specialis vo vzťahu k smernici NIS2, čo prekáža väčšine členských štátov EÚ vrátane Slovenskej republiky.

V roku 2025 sa napriek očakávaniam neobjavil zverejnený návrh revízie nariadenia pre kybernetickú bezpečnosť (nariadenie CSA), ktorý rieši otázku mandátu agentúry ENISA a systém certifikácie v EÚ. Mal by byť publikovaný až v januári 2026. Slovenská republika sa však spolu s ostatnými členskými štátmi EÚ vyjadrila k jeho očakávaným prvkom v neformálnom dokumente.

V oblasti **kybernetickej diplomacie**, ktorá obsahovo presahuje do domén spoločnej zahraničnej a bezpečnostnej politiky EÚ a spoločnej bezpečnostnej a obrannej politiky EÚ, sa aktivity Slovenskej republika a ostatných členských štátov EÚ v prvej polovici roka sústredili prevažne na koordináciu spoločných pozícií EÚ pre rokovania Pracovnej skupiny s otvoreným koncom (OEWG) pre bezpečnosť a využívanie informačných a komunikačných technológií (IKT) pri OSN, kde vrcholili diskusie o založení permanentného mechanizmu, ktorý by pokrýval globálnu koordináciu aspektov kybernetickej bezpečnosti. Tzv. **Globálny mechanizmus OSN** v tomto ohľade začne fungovať od marca 2026. Slovenská republika sa tiež zapojila do kybernetických dialógov s tretími partnerskými krajinami a zúčastnilo sa cvičenia aplikácie „Súboru nástrojov kybernetickej diplomacie v praxi“. V kontexte vyhodnocovania neustálych kybernetických hrozieb Slovenská republika spolupracovala s ostatnými členskými štátmi EÚ, svojimi strategickými partnermi, EEAS (INTCEN), Európskou komisiou, agentúrou ENISA, Európskym kompetenčným centrom (ECCC), ECSO, EUROPOL, či CERT-EU a zúčastňovala sa prípravy ďalších **sankčných kyberbezpečnostných zoznamov** pre dotknuté fyzické osoby na žiadosť Estónska, či nášho strategického partnera Veľkej Británie. Slovenská republika sa tiež zapojila do procesu prípravy strategického materiálu k zaujatiu pozície EÚ voči škodlivým aktivitám pochádzajúcich z tretej krajiny.

Slovenská republika v rámci svojich medzinárodných aktivít usporiadala začiatkom júla 2025 konferenciu na pôde Stáleho zastúpenia v Bruseli venovanú digitálnym a kyberbezpečnostným zručnostiam, či získavaniu nových talentov. Určená bola pre odbornú verejnosť, priemysel a zástupcov inštitúcií EÚ a členské štáty EÚ.

Poradným orgánom Komisie je formát Európskej skupiny pre certifikáciu kybernetickej bezpečnosti (EU Cybersecurity Certification Group - **ECCG**) a jeho pracovné skupiny, na zasadnutiach ktorých pravidelne participujú i zástupcovia úradu. V uplynulom roku sa uskutočnilo celkom päť zasadnutí ECCG. Cieľom tohto formátu je poskytovať odborné stanoviská k predloženým otázkam, ktoré sa v roku 2025 týkali najmä novelizácie nariadenia CSA, implementácie nariadenia CRA, vzájomného vzťahu medzi nariadením CRA a EUCC. V roku 2025 bol dokončený návrh kandidátskej schémy EU5G a začali sa prípravy na schému EU MSS. Ďalšími témami bola príprava schémy európskej peňaženky digitálnej identity a činností pracovných skupín. Tieto pracovné skupiny sa zameriavajú na vytvorenie rámca pre jednotné uplatňovanie požiadaviek nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881 ako aj požiadaviek vyplývajúcich z príslušných európskych certifikačných schém. Výsledkom práce skupiny Peer Review bolo **vydanie vykonávacieho nariadenia Komisie (EÚ) 2025/2540**, ktorým sa ustanovil jednotný rámec pre výkon peer review. Pracovná skupina Maintenance and Review sa okrem iného zameriava na aktualizáciu existujúcich a tvorbu nových State of the Art dokumentov vydaných k certifikačnej schéme EUCC.



Na účely zjednotenia implementácie nariadenia CRA Komisia zriadila štyri pracovné skupiny. Príslušníci úradu sú zastúpení v každej z týchto pracovných skupín, na zasadnutiach ktorých sa aktívne zúčastňovali aj v roku 2025. Skupina expertov (Expert Group) je neformálna skupina expertov, ktorá poskytuje poradenstvo Komisii a je konzultovaná v súvislosti s návrhmi delegovaných aktov. Témy diskusie sú rôzne oblasti implementácie nariadenia CRA, vrátane usmernení. Výbor pre bezpečnosť výrobkov (Product Security Comittee) má formálnu úlohu, ktorou je poskytovanie stanovísk k návrhom vykonávacích aktov (komitologický postup). Skupina notifikujúcich orgánov (Notifying Authorities Group) je stála skupina, ktorej cieľom je zabezpečiť jednotné uplatňovanie kapitoly IV nariadenia CRA v celej EÚ. Skupina pre administratívnu spoluprácu (ADCO) je zriadená podľa článku 52 ods. 15 nariadenia CRA na účely jednotného uplatňovania činností orgánov trhového dohľadu.

Významnú úlohu zohrávala aj účasť na zasadaniach skupiny pre digitálnu identitu (**EUDICG**). Skupina sa zaoberala koordináciou príprav tvorby národných schém pre peňaženky digitálnej identity.

Okrem toho sa v roku 2025 úrad aktívne zúčastňoval aj na zasadnutiach **Skupiny pre spoluprácu – k transpozícii smernice NIS (NIS Cooperation Group)** a na jej platformách **Work Stream on Post-Quantum Cryptography** (PQC), **Work Stream on Elections** (volebné procesy), **Work Stream on Health** (zdravotníctvo), **Working Group on Aviation** (letecká doprava) a **Work Stream on Risk Assessments and Supply Chain Security** (hodnotenie rizík a bezpečnosť dodávateľského reťazca).

Zasadnutia na úrovni **skupiny pre spoluprácu** (NIS Cooperation Group) sú organizované na základe smernice NIS, ktorá stanovuje opatrenia na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Európskej únii a zavádza rámec pre spoluprácu medzi členskými štátmi v oblasti kybernetickej bezpečnosti. Cieľom skupiny pre spoluprácu je dosahovať vysokú spoločnú úroveň bezpečnosti pre sieťové a informačné systémy v EÚ, podporovať a uľahčovať strategickú spoluprácu a výmenu informácií medzi členskými štátmi najmä pokiaľ ide o zdieľanie poznatkov aplikačnej praxe a najlepších postupov. Práce v skupine boli počas roka zamerané na aktualizáciu procesov súvisiacich s implementáciu smernice NIS2, prípravou príručiek, usmernení a ďalších dokumentov súvisiacich s týmito procesmi. Slovenská republika proces transpozície smernice NIS2 zavŕšila 28. novembra 2024, kedy Národná rada Slovenskej republiky schválila zákon č. 366/2024 Z. z., ktorým sa mení a dopĺňa **zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti.** Zákon o kybernetickej bezpečnosti nadobudol účinnosť 1. januára 2025. Slovenská republika sa tak stala piatou krajinou, ktorá si splnila transpozičnú povinnosť a len treťou krajinou s úplnou transpozíciu smernice NIS2. Celý rok 2025 sa tak niesol v znamení aplikácie zákona o kybernetickej bezpečnosti na podklade transponovanej smernice NIS2. Úrad zastúpený svojimi príslušníkmi v skupine a jej pracovných formátoch (**Work Streamoch - WS**) aktívne vystupoval, vznášal pripomienky k podporným strategickým dokumentom a zúčastňoval sa modelovaných cvičení a workshopov.

Jedeným z najaktívnejších pracovných formátov (WS) v rámci Skupiny pre spoluprácu v roku 2025 bol **WS on Peer review** (Vzájomné preskúmavanie a hodnotenie národných kapacít). Svoje činnosti zastúpení experti členských krajín smerovali na témy ako aktualizácia mapy národných stratégií kybernetickej bezpečnosti (NCSS), aktualizáciu rámca pre hodnotenia národných kapacít (NCAF v.2.0) a vykonávanie pilotných projektov NCAF. Pokiaľ ide o tému vzájomného preskúmavania a hodnotenia, skupine sa podarilo pripraviť strategický dokument a finalizáciu procesu schválenia dokumentácie vzájomného hodnotenia. Dokončenie pilotného vzájomného hodnotenia a podpora jeho realizácie s asistenciou zo strany Európskej komisie a ENISA prinesú členským štátom nový nástroj, ktorý im na základe výmeny skúseností a spolupráce s minimálne dvoma ďalšími členskými štátmi umožní objektívne porovnať a vyhodnotiť úroveň ich kybernetickej bezpečnosti. Na rok 2026 plánuje ENISA na základe návrhov vyplývajúcich z ročných dialógov pokračovať v poskytovaní prispôsobenej podpory troch oblastiach: tvorba poznatkov (hlbšie preskúmanie správy podľa smernice NIS2, usmernenia k národnej implementácii hlásenia incidentov a správa o stave kybernetickej bezpečnosti v Únii); prenos poznatkov (aktualizácia mapy NCSS a usporiadanie tematického zasadnutia o ACP); a podpora hodnotení (hodnotenia NCSS a pokračovanie peer review). Súčasne zámerom úradu je v roku 2026 byť prvou krajinou, ktorá sa na vzájomnom preskúmavaní zúčastní (pilotné preskúmavanie bolo vykonané Cyprom).

Hlavnými témami **WS on PQC zasadaní** boli prijatie a implementácia nových post-kvantových štandardov do národnej a medzinárodnej bezpečnostnej infraštruktúry i legislatívy a koordinácia medzi členskými štátmi EÚ a ďalšími partnerskými krajinami v oblasti výskumu a implementácie týchto technológií. Diskusie boli zamerané na implementáciu post-kvantových kryptografických algoritmov, ktoré sú odolné voči hrozbám vyplývajúcim z kvantových počítačov. Naďalej je potrebné monitorovanie pokroku v oblasti post-kvantovej kryptografie, uľahčovanie výmeny informácií medzi odborníkmi a koordinácia realizovaných krokov prostredníctvom špecializovanej platformy. Zároveň je nevyhnutná spolupráca na príprave nadväzujúcich dokumentov a technických odporúčaní, ktoré budú vychádzať z „Plánu koordinovanej implementácie post-kvantovej kryptografie“. Vzhľadom na

to, že kvantové technológie a post-kvantová kryptografia sa stávajú strategickou prioritou pre všetky členské štáty EÚ, a teda aj pre Slovenskú republiku, v roku 2025 sa uskutočnila v rámci dánskeho predsedníctva Rady EÚ Európska kvantová technologická konferencia (European Quantum Technologies Conference - EQTC) v Kodani, ktorej sa zúčastnili aj zástupcovia úradu. Podujatie sa konalo v kľúčovom období medzi prijatím Európskej kvantovej stratégie a pripravovaným Európskym kvantovým aktom. Konferencia EQTC tvorí významnú platformu na prepojenie výskumu, priemyslu a verejnej správy prostredníctvom odborných vedeckých zasadnutí, politických diskusií a prezentácií technologických riešení, čím prispieva k výmene poznatkov, posilneniu spolupráce a formovaniu ďalšieho smerovania kvantových technológií v Európe.

Počas roka 2025 sa **Workstream on Supervision** (WS pre otázky dohľadu a určenia právomoci) intenzívne venoval výkladu a aplikačným otázkam smernice NIS2, najmä v oblasti určenia jurisdikcie a mechanizmov vzájomnej pomoci medzi členskými štátmi. Kľúčovou témou diskusií bolo určenie hlavného usadenia (main establishment) a otázka, či má byť posudzované na úrovni jednotlivého právneho subjektu alebo na úrovni celej skupiny podnikov. Táto diskusia mala zásadný vplyv na ďalšie prvky dohľadu, vrátane určenia kontrolného podniku a rozlíšenia medzi samostatnou dcérskou spoločnosťou a skupinou podnikov. WS sa podrobne zaoberal aj výkladom pojmu „rozhodnutia prevažne prijímané“ podľa článku 26 ods. 1 smernice NIS2, vrátane otázok, akú úlohu zohráva faktická kontrola, ako aj miera zapojenia holdingu do riadenia dcérskych spoločností. Významná pozornosť bola venovaná aj praktickým dôkazným otázkam, najmä tomu, aké kritériá a dôkazy sú potrebné na určenie miesta, kde sa rozhodnutia prevažne prijímajú, ako aj možnostiam ich získania v prípadoch, keď nie sú verejne dostupné. Ako východisko sa zvažovalo aj sebahodnotenie subjektov, pričom WS diskutoval o tzv. „red line“ scenároch, ktoré by odôvodňovali jeho spochybnenie zo strany orgánov dohľadu. Ďalšou významnou témou bola úloha zástupcu v Únii a jeho postavenie v kaskádovom systéme podľa článku 26 smernice NIS2, vrátane otázky, či ide o poslednú možnosť alebo alternatívny prístup k určeniu jurisdikcie. WS sa zároveň venoval potrebe zavedenia jasného mechanizmu riešenia sporov medzi členskými štátmi pri rozdielnych výkladoch smernice NIS2. V oblasti vzájomnej pomoci (mutual assistance) sa WS zameral na otvorené otázky financovania, najmä na určenie členského štátu, ktorý by niesol náklady, s dôrazom na flexibilné, prípadovo posudzované riešenia. Diskutovala sa aj potreba vytvorenia technickej platformy na výmenu informácií a poskytovanie vzájomnej pomoci, pričom ako možný koordinátor bola identifikovaná ENISA a zvažovalo sa využitie existujúcich nástrojov, ako je platforma IMI, s cieľom predložiť túto otázku na schválenie NIS Cooperation Group.

V rámci pracovnej skupiny WS on Elections na zasadnutiach venovaných bezpečnosti a dôveryhodnosti volebných procesov, najmä v kontexte digitálnych volieb a elektronického hlasovania, dominovali témy ochrany pred kybernetickými útokmi počas volieb, ochrany osobných údajov voličov, zabezpečenia integrity volebného procesu vrátane prevencie manipulácie a podvodov, ako aj výmeny skúseností medzi členskými štátmi a medzinárodnými organizáciami v oblasti volebnej bezpečnosti.

V rámci rastúcej digitalizácie zdravotnej starostlivosti sa skupina **WS on Health** sústreďovala na jednu z hlavných priorít EÚ, ktorou je posilnenie kybernetickej bezpečnosti v sektore zdravotníctva a zabezpečenie vysoko bezpečnej digitálnej infraštruktúry, ktorá je nevyhnutná pre ochranu citlivých údajov a pre efektívne fungovanie zdravotných systémov. Na zasadnutiach sa členovia skupiny, z pohľadu dôležitých tém pre úrad, venovali transpozícii smernice NIS2 do národnej legislatívy v sektore zdravotníctva, ktorá je zameraná na zlepšenie ochrany kritickej digitálnej infraštruktúry v oblasti zdravotnej starostlivosti a **Európskemu akčnému plánu ku kybernetickej bezpečnosti nemocníc a zdravotníckych zariadení**. Zástupcovia úradu tak aktívne mohli prispievať informáciami ohľadom napredovania legislatívneho procesu novelizácie zákona o kybernetickej bezpečnosti s dopadom na sektor zdravotníctva.

Cieľom **WG on Aviation** počas roka 2025 bolo zabezpečenie spolupráce a koordinácie medzi Európskou komisiou, členskými štátmi a zainteresovanými stranami v otázkach týkajúcich sa implementácie legislatívy EÚ, programov a politík v oblasti kybernetickej bezpečnosti v civilnom letectve. Prioritou skupiny tak boli koordinácia pri dodržiavaní príslušných legislatívnych požiadaviek v oblasti kybernetickej bezpečnosti, ako sú smernica NIS2, vykonávacie nariadenie Komisie (EÚ) 2019/1583 o opatreniach na vykonávanie spoločných základných noriem bezpečnostnej ochrany letectva, pokiaľ ide o opatrenia kybernetickej bezpečnosti (AVSEC) a vykonávacie nariadenie Komisie (EÚ) 2023/203, ktorým sa stanovujú pravidlá uplatňovania nariadenia na požiadavky na riadenie rizík v oblasti informačnej bezpečnosti s potenciálnym vplyvom na bezpečnosť letectva pre organizácie (PART IS) a zdieľanie skúseností členských štátov v zmysle osvedčených postupov v oblasti kybernetickej bezpečnosti civilného letectva. Aj v tomto prípade zástupcovia úradu zdieľali informácie napredovania legislatívneho procesu transpozície smernice NIS2 s dopadom na sektor leteckej dopravy.

V rámci **WS on Risk Assessments and Supply Chain Security** bola v roku 2025 nosnou témou aktualizácia nástroja pre bezpečnosť dodávateľského reťazca (ICT Supply Chain Security Tool Box), ktorého hlavnou úlohou je poskytnúť členským štátom EÚ spoločný, štruktúrovaný a nezáväzný prístup k zabezpečeniu ich dodávateľských reťazcov IKT. Tento nástrojový súbor podporuje členské štáty tým, že identifikuje vybrané riziká spojené s ich dodávateľskými reťazcami IKT a poskytuje odporúčania, ako posilniť kybernetickú bezpečnosť a odolnosť ich dodávateľských reťazcov IKT.

Zástupcovia Národného centra kybernetickej bezpečnosti boli na úrovni EÚ súčasťou viacerých pracovných skupín a iniciatív zameraných na budovanie spoločného rámca kybernetickej bezpečnosti. Medzi najvýznamnejšie aktivity patrí účasť v **Európskej sieti styčných organizácií pre kybernetické krízy CyCLONe**, sieti zástupcov členských štátov na zvládanie kybernetických kríz. V rámci stretnutí prebiehala strategická diskusia zameraná na efektívne zdieľanie informácií o kybernetickej bezpečnosti. Spolupráca podporuje výmenu dôležitých informácií v kybernetickom priestore. Stretnutia CyCLONe mali v roku 2025 za cieľ vylepšovanie a overovanie postupov pri riešení závažných kybernetických bezpečnostných incidentov s cezhraničným presahom.

V roku 2025 sa uskutočnilo cvičenie **BlueOLEX**, ktoré sa zameralo na simuláciu eskalácie rozsiahleho kybernetického bezpečnostného incidentu na dopravný sektor. Cieľom cvičenia bolo zabezpečenie primeranosti a zlepšenia procesov operačných postupov, internej spolupráce, určenie jasného interného komunikačného kanálu, zlepšenie reakcie na vzťahy s verejnosťou počas kríz v oblasti kybernetickej bezpečnosti a preverenie schopností riešiť tieto krízy. V roku 2025 sa tiež uskutočnilo cvičenie CySOPex 2025, ktorého sa zúčastnili zástupcovia väčšiny členských štátov EÚ. Cvičenie bolo zamerané na dopravný sektor a kritickú infraštruktúru. Cvičenie bolo zamerané na precvičenie rýchlosti reakcie, pripravenosť na rozsiahle kybernetické bezpečnostné incidenty a efektívnosť výmeny informácií na národnej a medzinárodnej úrovni.

SK-CERT – národná jednotka CSIRT, ktorý patrí pod Národné centrum kybernetickej bezpečnosti NBÚ, aktívne pôsobilo aj v rámci medzinárodných organizácií združujúcich jednotky CSIRT. V rámci CSIRT Network, ktorý združuje národné jednotky CSIRT členských štátov EÚ, si SK-CERT s ostatnými členskými štátmi vymieňal operatívne informácie o kybernetických hrozbách a kybernetických bezpečnostných incidentoch. Keďže vojenská situácia na východe Európy sa nezmenila, jednotlivé štáty si vymieňali informácie a skúsenosti s incidentami a útokmi, ktoré súviseli s vojnou na Ukrajine a poskytovali si vzájomnú pomoc podľa potreby. SK-CERT si v rámci CSIRT Network v roku 2025 udržal najvyšší status vyspelosti CSIRT jednotky „Advanced“, ktorý sa udeľuje po tzv. peer-review procese, v ktorom jedna CSIRT jednotka hodnotí vyspelosť inej CSIRT jednotky podľa nastavenej objektívnej metodiky.

V roku 2025 sa medzinárodná spolupráca Kompetenčného certifikačného centra kybernetickej bezpečnosti (KCCKB) v roli Národného kompetenčného centra (NCC) zameriavala predovšetkým na systematickú interakciu s partnerskými organizáciami na európskej úrovni, najmä s **Európskym kompetenčným centrom kybernetickej bezpečnosti (ECCC)** a so sieťou národných koordinačných centier.

NCC sa v priebehu roka aktívne zapájalo do spoločných aktivít v rámci siete NCC, pričom významnou súčasťou boli viaceré medzinárodné webináre organizované v spolupráci s partnerskými organizáciami z Fínska, Nemecka, Česka, Rakúska. Tieto podujatia slúžili ako platforma na výmenu odborných skúseností, prezentáciu aktuálnych iniciatív a šírenie osvedčených postupov medzi členskými štátmi. Zároveň prispeli k posilneniu odborných kapacít a prehĺbeniu spolupráce naprieč európskym ekosystémom.

Významným aspektom medzinárodného pôsobenia NCC bola účasť na riadiacich štruktúrach na európskej úrovni. Zástupcovia KCCKB sa v roku 2025 zúčastnili štyroch zasadnutí Správnej rady ECCC a zasadnutí siete NCC, ktoré sa konali v apríli, júli, októbri a decembri. Popri účasti na zasadnutiach Správnej rady sa KCCKB v úlohe NCC zapájalo aj do práce v pracovných skupinách ECCC. Prostredníctvom týchto skupín sa KCCKB podieľalo na výmene informácií, koordinácii aktivít a zdieľaní skúseností v oblastiach relevantných pre rozvoj kybernetickej bezpečnosti na európskej úrovni.

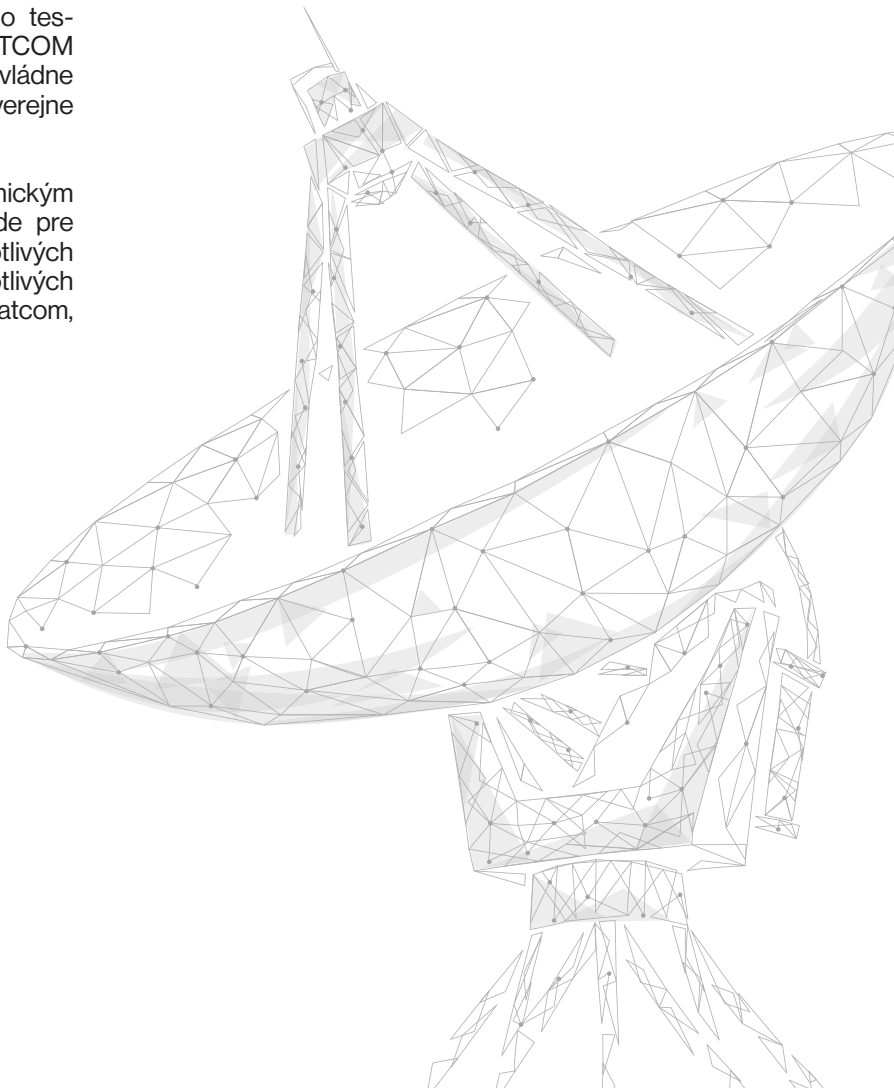
Medzinárodná spolupráca v roku 2025 podporila zapojenie NCC do európskych aktivít a prispela k lepšej výmene informácií v rámci siete NCC. Spolupráca s ECCC a ostatnými národnými koordinačnými centrami vytvorila predpoklady pre pokračovanie spolupráce a zapájanie sa do ďalších spoločných aktivít a projektov.

Agentúra Európskej únie pre vesmírny program (EUSPA)

V roku 2025 sa príslušníci úradu zúčastňovali na pravidelných zasadaniach **Bezpečnostného výboru pre Vesmírne programy EÚ** v rámci **Agentúry Európskej únie pre vesmírny program (EUSPA)**. Hlavnými bodmi diskusie boli: revízia základných bezpečnostných požiadaviek (GSR) a bezpečnostných pokynov programu (PSI) EU SST a EGNOS a taktiež stanovenie rámca pre určovanie stupňov utajenia pre jednotlivé komponenty Vesmírnych programov EÚ. Tieto rozsiahle dokumenty boli pripravované v jednotlivých podporných pracovných skupinách, či už ide o **Pracovnú skupinu pre bezpečnosť programu Galileo, GOVSATCOM, Copernicus** alebo **EGNOS**. V súvislosti s programom GOVSATCOM a IRIS2 zasadala pracovná skupina Bezpečnosť pre **EuroQCI** (Quantum Communication Infrastructure), ktorá sa podieľa na diskusii o prierezovej téme kvantovej komunikačnej infraštruktúry. Tá má byť využitá v súvislosti s programom GOVSATCOM a IRIS2 a má zabezpečiť vysokú mieru šifrovania, odolnosti a v konečnom dôsledku aj bezpečnosti, keďže táto sieť má byť prispôsobená aj na prenos utajovaných skutočností.

V rámci EUSPA, za účasti príslušníkov úradu, okrem pravidelných zasadnutí **Rady pre bezpečnostnú akreditáciu**, prebehol v roku 2025 operatívy audit v riadiacom centre programu Galileo (GCC-I) v Talianskom Fuccine. Z hľadiska zhoršujúcej sa geopolitickej situácie bolo v roku 2025 prioritou urýchliť finalizáciu bezpečnostných prvkov jednotlivých systémov. Do testovacej prevádzky bol uvedený systém IS-GOVSATCOM (zabezpečený satelitný komunikačný systém pre vládne inštitúcie) a Galileo PRS (satelitný systém pre verejne regulovateľnú službu).

Jednotlivé pracovné skupiny, tzv. panely, sú technickým poradným orgánom, ktorý dáva odporúčania Rade pre bezpečnostnú akreditáciu k plneniu jednotlivých projektových míľnikov a akreditácií jednotlivých systémových komponentov programu Galileo, Govsatcom, EGNOS a IRIS2 (G2G).



Organizácia pre bezpečnosť a spoluprácu v Európe (OBSE)

Zorganizované stretnutia účastníckych štátov **Organizácie pre bezpečnosť a spoluprácu v Európe (OBSE)**, na ktorých mal v roku 2025 aktívne zastúpenie aj úrad, podčiarkli dôležitosť medzinárodnej spolupráce v oblasti kybernetickej bezpečnosti a zdieľania informácií o existujúcich a potenciálnych hrozbách. Činnosti a fungovanie OBSE v roku 2025 boli aj naďalej ovplyvnené nestabilnou geopolitickou situáciou, najmä prebiehajúcou vojnou Ruskej federácie proti Ukrajine, čo sa následne premietlo aj na priebehu rokovaní o prevažne nesenzitívnych a expertných témach, akými sú kybernetická bezpečnosť a bezpečnosť IKT.

V uplynulom roku sa uskutočnili celkom štyri zasadnutia **neformálnej pracovnej skupiny OBSE pre oblasť kybernetickej bezpečnosti a informačných a komunikačných technológií (IWG). Stretnutie kontaktných bodov OBSE pre oblasť IKT** (opatrenia na budovanie dôvery - CBM) sa konalo súbežne s druhým zasadnutím IWG v júni 2025. Obsah zasadnutí tvorili diskusie o prebiehajúcej implementácii existujúcich iniciatív v zmysle CBM zúčastnených štátov OBSE, pričom vývoj CBM v rámci OBSE prebiehal paralelne s aktivitami Prvého výboru OSN s dôrazom na význam regionálnych organizácií pri implementácii záväzkov v oblasti kybernetickej bezpečnosti, ďalej to boli diskusie o národných iniciatívach (pripravované národné stratégie kybernetickej bezpečnosti a príslušné akčné plány ich realizácie) a vnútroštátnom vývoji v oblasti kybernetickej/IKT bezpečnosti. Krajiny tiež upriamili pozornosť na národné procesy venujúce sa novým a vznikajúcim technológiám, viedli odborné diskusie o nových naliehavých kybernetických výzvach, ako napríklad vývoj umelej inteligencie, dopady kvantových technológií a o iných relevantných kybernetických a IKT hrozbách.

Výročná konferencia OBSE, ktorá sa konala súbežne s tretím zasadnutím IWG v októbri 2025, opätovne potvrdila kľúčovú úlohu OBSE ako fóra pre inkluzívny dialóg o kybernetickej bezpečnosti a bezpečnosti IKT. Jednotlivé diskusné panely poukázali na potrebu zosúladenia politických záväzkov s praktickými opatreniami a na význam koordinovanej spolupráce medzi štátmi, súkromným sektorom a medzinárodnými partnermi.

Sekretariát OBSE sa dlhodobo venuje činnostiam, ktoré uľahčujú či podporujú činnosti pracovných skupín na úrovni OSN. Jednou z najdôležitejších aktivít Sekretariátu OBSE a Oddelenia pre nadnárodné hrozby (TNTD) v roku 2025 bola podpora aktivít OEWG (pracovnej skupiny s otvoreným koncom), a to najmä príspevky k tvorbe Dohovoru OSN proti počítačovej kriminalite (formálne „Dohovor OSN o posilnení medzinárodnej spolupráce pri boji proti určitým trestným činom spáchaným prostredníctvom informačných a komunikačných technológií“) a podpora transformácie OEWG na permanentný mechanizmus kybernetickej bezpečnosti, tzv. Global Mechanism (Globálny mechanizmus).

Prostredníctvom zasadnutí IWG úrad zdieľal informácie o implementačných procesoch transpozície smernice NIS2 do národnej legislatívy, o stave kybernetickej bezpečnosti, ako aj o aktuálnych aktivitách a pokrokoch pri implementácii CBM.

Úrad vníma prínos zasadnutí OBSE v bezpečnom zdieľaní informácií na regionálnej úrovni, posilňovaní medzinárodnej spolupráce, upevňovaní svojho postavenia ako spoľahlivého medzinárodného hráča a v rozširovaní svojej siete kontaktných bodov (PoC) v kybernetickej oblasti a IKT oblasti i mimo členských štátov EÚ. V spojitosti s ativitami OBSE, úrad veľmi pozitívne hodnotí i koordinovanie spolupráce na národnej úrovni so zástupcami MZVEZ SR.

Z perspektívy úradu boli kľúčové najmä témy týkajúce sa vzájomného informovania účastníckych štátov OBSE a budovania dôvery, medziregionálnej spolupráce OBSE s inými regionálnymi organizáciami (UAS, ECOWAS) a medzinárodnými organizáciami (OSN), stratégií boja proti aktuálnym kybernetickým a hybridným hrozbám (ich prevencia, reakcia na takéto hrozby a nástroje stabilizácie kybernetického priestoru) a zamedzenia zneužívania nových a vznikajúcich technológií, a to hlavne v kontexte podvratných aktivít vykonávaných nielen štátnymi, ale aj neštátnymi aktérmi.

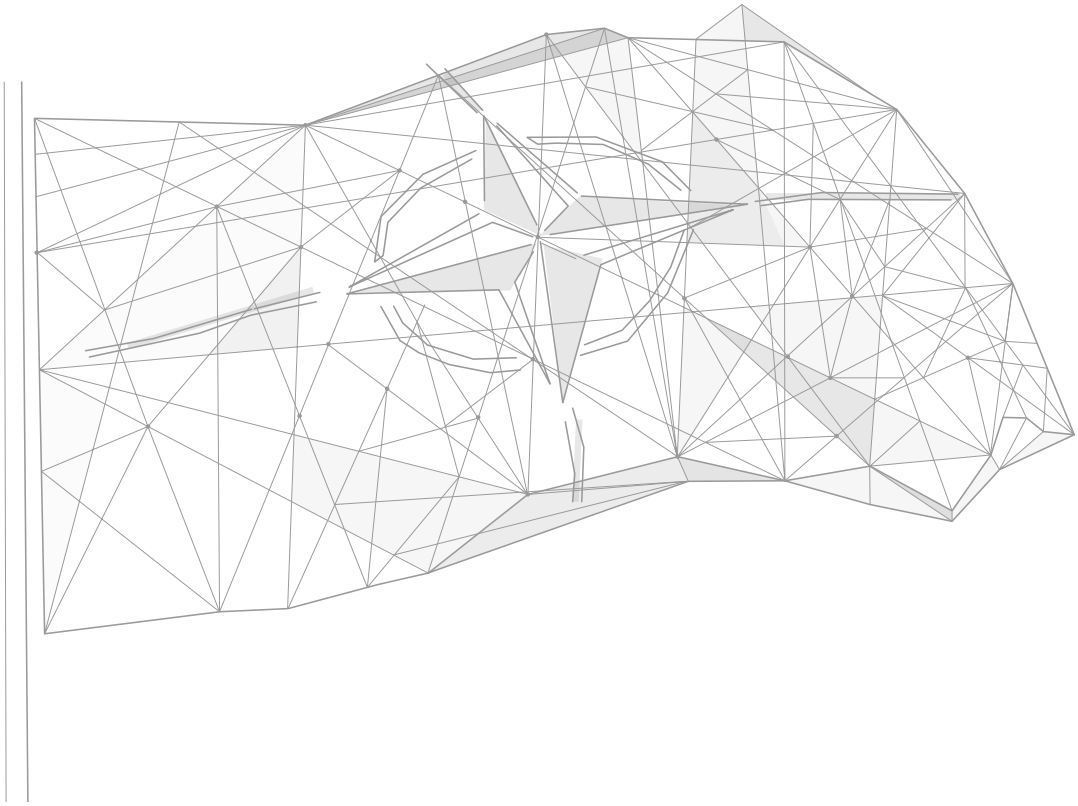
Medzinárodné aktivity

V septembri 2025 sa uskutočnilo v prezenčnej forme 38. plenárne zasadanie Multinational Industrial Security Working Group (MISWG). Pracovná skupina MISWG je uznávaným orgánom pre spoluprácu v oblasti najlepších postupov v oblasti medzinárodnej priemyselnej bezpečnosti, kde je zastúpených takmer 40 krajín sveta vrátane Slovenskej republiky. Hlavnou témou stretnutia bolo podporovať, zlepšovať a harmonizovať spoločné medzinárodné osvedčené postupy na ochranu utajovaných skutočností (v oblasti priemyselnej bezpečnosti) a určitých iných foriem vládou kontrolovaných informácií, ktoré čelia súčasným a novým bezpečnostným hrozbám a výzvam v tejto oblasti. Počas plenárneho zasadnutia bolo zdôraznených viacero významných rozhodnutí aj podstatný pokrok, ktorý bol v jeho priebehu dosiahnutý. V rámci MISWG uskutočnili zástupcovia úradu viacero bilaterálnych rozhovorov so zámerom prehĺbiť spoluprácu s partnermi v oblastiach ochrany utajovaných skutočností a kybernetickej bezpečnosti, zároveň aktívnou účasťou prispeli, keď odprezentovali tému „Aktuálny stav ochrany utajovaných skutočností na Slovensku“.

O nadviazaní bližšej spolupráce sa viedli rozhovory rovnako so zástupcami Južnej Kórey, Japonska, Austrálie a Nového Zélandu. Pokračovala komunikácia s Českou republikou, Švajčiarskom a zástupcami Rakúskej republiky. Témami boli ochrana utajovaných skutočností v segmente obranná spolupráca a obranný priemysel.

V novembri 2025 sa v priestoroch Eurojustu v Haagu konala 24. výročná medzinárodná konferencia a valné zhromaždenie Európskych partnerov proti korupcii (EPAC) a Európskej siete kontaktných bodov proti korupcii (EACN), ktorej sa zúčastnili príslušníci sekcie kontroly a bezpečnosti. Stretnutie inšpekčných služieb a protikorupčných zložiek bolo zamerané na tematiku „Udržiavanie integrity: Naliehavé výzvy v meniacom sa svete“. Medzinárodná sieť EPAC - European Partners Against Corruption (Európski partneri proti korupcii) - vznikla ako neformálna sieť protikorupčných a inšpekčných zložiek členských štátov Európskej únie, ktorých predstavitelia sa každoročne zúčastňujú na medzinárodnej konferencii a valnom zhromaždení za účelom prijímania zásadných politík, stanovenia hodnotového rámca a vymedzenia strategických priorít v oblasti integrity, prevencie a boja proti korupcii. Medzinárodná sieť EACN poskytuje aktuálne informácie pre vzájomnú spoluprácu a výmenu informácií s inšpekčnými a protikorupčnými zložkami členských krajín Európskej únie. Konferencia prebiehala v dvoch paneloch, ktoré boli tematicky zamerané na strategické prístupy v oblasti korupcie a integrity a medzinárodnú spoluprácu v boji proti korupcii. Hlavným zámerom konferencie bolo prehĺbenie vzájomnej spolupráce a posilnenie partnerských vzťahov útvarov, ktoré sa podieľajú na prevencii korupcie a na boji s trestnou činnosťou v členských krajinách Európskej únie.

V rámci svojich úloh príspevková organizácia NBÚ, KCCKB, vybudovala tím mladých expertov na informačnú bezpečnosť, ktorý zastupuje Slovenskú republiku na medzinárodných súťažiach. V roku 2025 na súťaži mladých kybertalentov European Cybersecurity Challenge (ECSC) získali významné prvenstvá: účasť na CTF súťaži v Dubline (Írsko), marec 2025 - 1. miesto, ECSC Finals súťaže vo Varšave (Poľsko), apríl 2025 - 4. miesto spomedzi 39 štátov. Zúčastnili sa aj ďalších aktivít, kde významným spôsobom dokázali svoju kvalitu: ECSC Steering committee a Initial Planning Meeting vo Varšave (Poľsko), apríl 2025, Medzinárodný bootcamp vo Viedni (Rakúsko), júl 2025 - 10 štátov Medzinárodný bootcamp v Brunovciach (Slovensko), august 2025 - 10 štátov, ECSC Steering committee a Planning Meeting v Poľsku.



Organizácia Severoatlantickej zmluvy (NATO)

Počas roka 2025 sa uskutočnili rokovania **Bezpečnostného výboru NATO (SC)**, ktoré prebehli vo všetkých svojich formátoch – vo formáte bezpečnostných politík, bezpečnosti komunikačných a informačných systémov (CISS) a na najvyššej úrovni – úroveň riaditeľov bezpečnostných úradov členských štátov. Predsedajúcim výboru bol riaditeľ Bezpečnostného úradu NATO (NOS) Galen Nace, ktorý diskutoval s predstaviteľmi bezpečnostných autorít o rôznych bezpečnostných témach, a to nielen v kontexte súčasnej geopolitickej situácie.

Za **hlavný míľnik úradu** v oblasti medzinárodných vzťahov v roku 2025 možno zaručene označiť **zasadnutie Bezpečnostného výboru NATO s non-NATO entitami** (nečlenské štáty, spolupracujúce medzinárodné organizácie a inštitúcie), ktoré sa uskutočnilo 17.-19. septembra 2025 v Bratislave. Úrad sa podujal túto významnú udalosť hostiť po pozitívnej odozve z minuloročnej návštevy riaditeľa NOS a zástupcu generálneho tajomníka NATO pre bezpečnosť Galena J. Nacea, ktorý v rámci pracovnej cesty navštívil svojich bezpečnostných partnerov.

Išlo o historicky druhé rozšírené zasadnutie Bezpečnostného výboru NATO (prvé sa uskutočnilo v máji 2019 vo Varšave), na ktorom sa stretlo viac ako 130 zástupcov národných bezpečnostných úradov členských štátov a partnerov NATO z viac než 60 krajín a medzinárodných organizácií. Podujatie, ktoré spoločne zorganizoval NBÚ a NOS, potvrdilo nielen významnú úlohu Slovenskej republiky v Aliancii, ale aj jeho rešpektované postavenie medzi partnermi. Slovenská republika sa opäť ukázala ako spoľahlivý spojenec, ktorý vie vytvárať priestor na odbornú diskusiu a hľadať riešenia pre spoločnú bezpečnosť. Rokovanie otvoril aj štátny tajomník Ministerstva zahraničných vecí a európskych záležitostí Slovenskej republiky Marek Eštok, čím zdôraznil politický rozmer podujatia a podporu vlády Slovenskej republiky pre spoluprácu v oblasti bezpečnostnej politiky.

Hlavným zámerom stretnutia bola výmena a zdieľanie osvedčených postupov pri ochrane utajovaných skutočností a hľadanie riešení pre nové bezpečnostné hrozby najmä v kontexte partnerstiev. Ako uviedol riaditeľ NOS, partnerstvá posilňujú Alianciu, ktorá sa zaviazala spolupracovať s našimi partnermi na presadzovaní osvedčených postupov v oblasti bezpečnosti s cieľom chrániť našich ľudí, informácie, systémy a zariadenia. Rovnako potvrdil, že sme hrdí na to, že sme zlepšili bezpečnostné nastavenia medzi NATO a partnermi. Riaditeľ úradu zdôraznil, že zasadnutie ukázalo, že NATO a jeho partneri vedia spoločne reagovať na komplexné výzvy a premietať princíp kolektívnej bezpečnosti do praktických riešení. Taktiež vyjadril presvedčenie, že výsledky rokovaní prispejú k posilneniu pozície NATO ako garanta stability a bezpečnosti, k upevneniu partnerstiev a k rozšíreniu priestoru vzájomnej dôvery.

Na pôde NATO zároveň pokračovala príprava podporných dokumentov k hlavnej bezpečnostnej politike NATO C-M(2002)49-REV1, najmä usmernení v oblasti personálnej, fyzickej a objektovej, administratívnej bezpečnosti a bezpečnostnej ochrany informácií stupňa NATO Restricted. V rámci rokovaní výrazne rezonovala otázka nedostatočnej úrovne zabezpečenia akreditácie utajovaných komunikačných a informačných systémov NATO, ktoré sú prepojené aj s národnými systémami. Delegácie v tejto súvislosti vyjadrili nespokojnosť a požiadali, aby NOS o danom stave informoval Severoatlantická rada.

Koncom roka 2025 sa uskutočnilo posledné spoločné rokovanie pracovnej skupiny pozostávajúcej z členov Archívneho výboru a SC, ktorej úlohou bolo riešiť problematiku hromadného odtajovania utajovaných skutočností NATO. Výsledok ich práce bude postúpený na jednotlivé formáty s cieľom ich následného prediskutovania a schválenia.

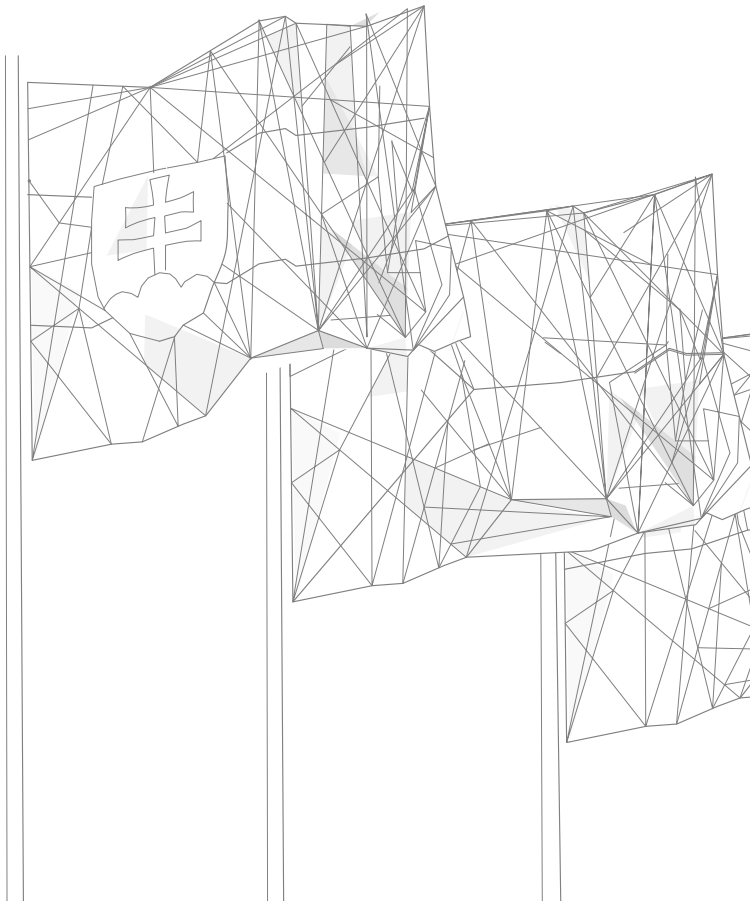
V decembri 2025 sa uskutočnilo aj samostatné zasadanie **Archívneho výboru (NATO AC)**, ktorého leitmotívom bola pokračujúca diskusia o procesoch odtajovania informácií označených ako „NATO Restricted" a ich následnému uvoľňovaniu verejnosti. Konkrétne príklady z praxe na národnej úrovni by tak mali napomôcť k lepšiemu uchopeniu a zarámcovaniu problematiky aj na úrovni Aliancie. Niektoré krajiny počas rokovaní taktiež prezentovali systém vedenia záznamov (ich manipulácie a archivácie) z vojenských operácií, ako aj záznamov o zmenách v procesoch automatického odtajovania utajovaných skutočností v Nemecku a Grécku.

Čo sa kybernetickej bezpečnosti týka, udalosťou roka 2025 bola pre NATO **konferencia Cyber Defence Pledge**, ktorá sa uskutočnila v máji vo Varšave. Účastníci tak prvýkrát po rozsiahlej úprave dotazníka (2023) reflektujúceho na rýchlo sa meniaci kyberpriestor mohli zhodnotiť dosiahnutý pokrok v oblasti kybernetickej bezpečnosti/obrany Aliancie v konkrétnej téme – kybernetická obrana v oblasti kritickej infraštruktúry, bezpečnosti dodávateľského reťazca a vesmírnych systémov. Na vypracovaní dotazníka spolupracoval úrad s Vojenským spravodajstvom a Ministerstvom vnútra Slovenskej republiky. Slovenská republika umožnila spojencom zdieľanie svojho samohodnotenia rovnako, ako to spravili takmer všetky členské štáty.

Tretia výročná konferencia o kybernetickej obrane NATO bola ďalšou dôležitou udalosťou roka, a to nielen v oblasti kybernetickej obrany. Konferencia sa uskutočnila v októbri v Tirane a prepojila všetky zainteresované strany na všetkých troch úrovniach (politickej, technickej a vojenskej) nielen v rámci štruktúr NATO, ale aj u 32 spojencov.

Úrad sa zúčastňoval aj pravidelných zasadaní bezpečnostných akreditačných výborov a pracovných skupín NATO, zameraných predovšetkým na bezpečnosť utajovaných informácií, s ktorými sa manipuluje v rámci utajovaných systémov v súlade s bezpečnostnými politikami cudzej moci. Zároveň sa tieto rokovania týkali aj adaptácie súboru nových pravidiel, požiadaviek a ich aplikovania v reakcii na vyvíjajúce sa technológie a bezpečnostnú situáciu vo svete.

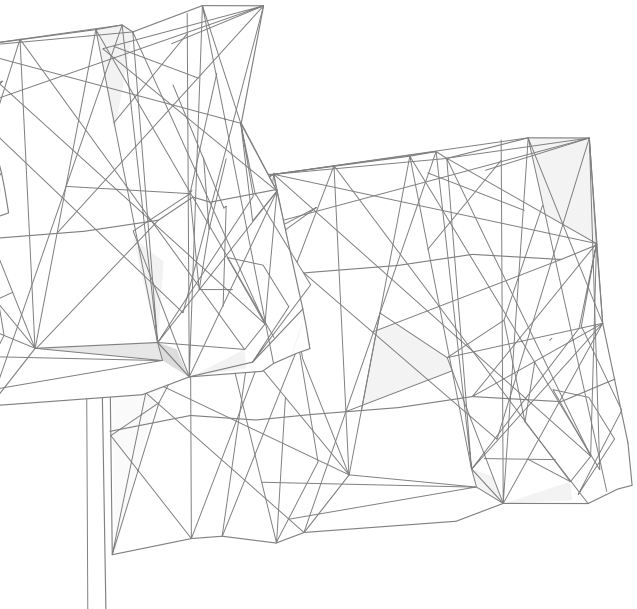
V roku 2025 úrad participoval aj na spoločnom aliančnom cvičení **NATO Able Staff 2025**, ktoré sa uskutočnilo v novembri 2025 a malo preveriť komunikačné procedúry súvisiace s jadrovým plánovaním, precvičiť použiteľné opatrenia systému krízovej odozvy aliancie, priniesť zdokonalenie v konzultačnej oblasti, realizovať praktický výcvik personálu v centrále NATO, v Hlavnom veliteľstve spojeneckých síl v Európe (SHAPE) a v národných ústrediach. Úrad sa na cvičení zúčastňoval na distribučnej úrovni, prostredníctvom pracoviska centrálneho registra zabezpečil prijímanie a postupovanie utajovaných skutočností. Komunikácia počas cvičenia prebiehala prostredníctvom informačného systému NS WAN a NNCCRS (NATO Nuclear Command Control Response System), ktorým prúdil tok informácií medzi zainteresovanými rezortmi, úradom a centrálou NATO.



Regionálna spolupráca

Na základe rotácie predsedníctva krajín, ktoré sú členmi **Stredoeurópskej platformy pre kybernetickú bezpečnosť (CECSP), Národné centrum kybernetickej bezpečnosti Maďarska** v roku 2025 predsedalo tejto platforme. Zástupcovia úradu sa aktívne zúčastnili na rokovaniach platformy spolu s ďalšími kolegami zastúpenými krajinami **Vyšehradskej štvorky** (Česká republika, Maďarsko, Poľsko), **Rakúska a Slovinska**, ktoré sa stalo regulárnym členom platformy. Predmetom samotných rokovaní boli aktuálne témy, ktoré na úrovni EÚ rezonovali počas celého roka 2025 a súčasne sa partneri v rámci týchto tém snažili nájsť spoločné prieniky a vzájomnú podporu. Zároveň maďarské predsedníctvo nadviazalo na rakúske a pokračovalo s updatom zakladajúcich dokumentov „Central European Cyber Security Platform – Declaration" a „Working program for European Central Security Platform". Medzi tie najdôležitejšie témy stretnutia patrili: „Aktuálny stav procesu transpozície **smernice NIS 2** v jednotlivých členských štátoch a informácie o významných kybernetických bezpečnostných incidentoch z posledného obdobia"; **„Kybernetická bezpečnosť a činnosť Národných kompetenčných centier", „Umelá inteligencia v kontexte kybernetickej bezpečnosti" a „Využívanie umelej inteligencie v súvislosti so systémom „Honeypot"**. Experti sa zhodli, že pri aproximácii sa vyžaduje adaptívny, koordinovaný a inovatívny prístup, ktorým sa dosiahne najširšia harmonizáciou naprieč celou EÚ. Slovinsko sa zúčastnilo rokovaní už tretí krát a práve zmenou statusových dokumentov nastúpi cestu riadneho člena voči čomu nemajú zakladajúce krajiny žiadne výhrady a na princípe rozvoja spolupráce krajín strednej Európy v oblasti kybernetickej bezpečnosti schválili členstvo Slovinska.

Rok 2025 sa niesol v duchu stretnutí s najbližším partnerom – **Českou republikou**. Česká republika organizovala už šiesty ročník Prague Cyber Security Conference, ktorá sa uskutočnila v marci 2025. Témou konferencie boli **„Invisible frontlines"** (Neviditeľné hranice) – kybernetický priestor nie je len prostredím pre každodenný život, ale rovnako miestom, kde dochádza k stretom medzi členskými štátmi alebo medzi štátnymi aktérmi. Konflikty si zo začiatku často neviditeľné, ale ich dopady sú skôr, či neskôr viac než reálne (narušenie kritickej infraštruktúry, ekonomické škody až po destabilizáciu demokratickej spoločnosti). Okrem zástupcov úradu sa konferencie zúčastnilo 46 krajín sveta.



V apríli 2025 sa uskutočnilo stretnutie so zástupcami **Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB)** k otázkam transpozície smernice NIS 2. Predmetom diskusie boli aj nasledovné témy: pôsobnosť zákona o kybernetickej bezpečnosti vo vzťahu k teritorialite, samoidentifikácia subjektu ako prevádzkovateľa základnej služby, uplatňovanie nariadenia DORA, analytické činnosti na úseku kybernetickej bezpečnosti, implementácia nariadenia CRA, certifikácia kybernetickej bezpečnosti alebo vývoj stavu súladu kybernetickej bezpečnosti podľa anonymizovaných auditných správ. Českých partnerov zaujímali skúsenosti s reguláciou cloud computingu v Slovenskej republike, s bezpečnosťou dodávateľského reťazca a otázky k regulácii verejnej správy, obcí alebo výskumu.

V rámci prehĺbenia a rozšírenia vzájomnej spolupráce sa v novembri 2025 uskutočnilo dvojdňové stretnutie s **Národním bezpečnostním úřadem Českej republiky**. Boli prezentované spoločné témy so zameraním na aktuálne trendy a vývoj v oblasti ochrany utajovaných skutočností. Hlavnou oblasťou stretnutia bola elektronizácia služieb v oblasti bezpečnostných previerok pre fyzické osoby a podnikateľov. Rokovania boli vedené vo forme tematických pracovných skupín podľa oblastí ich odborného pôsobenia, prebehli v konštruktívnom a profesionálnom duchu a boli prínosom najmä v týchto oblastiach: výmena praktických skúseností a overených postupov z aplikačnej praxe, komparácia legislatívnych rámcov a administratívnych procesov, digitalizácia procesov bezpečnostných previerok, identifikácia aktuálnych výziev, prehĺbenie vzájomnej dôvery, rozvoj existujúcej spolupráce a hľadanie nových foriem praktickej spolupráce.

Bilaterálne vzťahy

Zo strany príslušníkov úradu boli bilaterálne vzťahy aktívne rozvíjané naprieč všetkými pracovnými platformami a formátmi, či už pri osobnom kontakte počas zasadnutia pracovných skupín, alebo pri ad hoc plnení úloh práve na bilaterálnej úrovni.

Zástupcovia úradu tiež participovali na uzavretí zmluvy medzi **vládou Slovenskej republiky a Organizáciou pre spoluprácu v spoločnom vyzbrojovaní** (OCCAR), ktorá bola podpísaná vo februári 2025. Predmetná zmluva umožní slovenským subjektom účasť na európskych projektoch v oblasti zbrojného priemyslu.

V záujme ďalšieho rozvíjania a prehlbovania spolupráce v oblasti kybernetickej bezpečnosti s **Kenskou republikou** sa v roku 2025 uskutočnila prvá iterácia Cyber Game v Kenskej republike aj vďaka podpore NCKB.

V rámci bilaterálnych vzťahov príslušníci úradu a zástupcovia NCKB pravidelne komunikovali a vymieňali si informácie o aktuálnych právnych predpisoch na národnej úrovni, zraniteľnostiach, kybernetických hrozbách a kybernetických bezpečnostných incidentoch a vymieňali si informácie o osvedčených postupoch a o dobrej praxi so svojimi zahraničnými partnermi aj mimo EÚ a zúčastňovali sa rôznych medzinárodných cvičení kybernetickej bezpečnosti. Takisto sa po vecnej stránke zástupcovia úradu a zástupcovia NCKB zúčastňovali bilaterálnych rokovaní a zahraničných prijatí zastrešovaných práve odborom medzinárodných vzťahov sekcie regulácie a dohľadu.

O nadviazanie spolupráce v oblasti kybernetickej bezpečnosti prejavila záujem **Brazílska federatívna republika**. Rokovania vyústili do podpísania Memoranda o spolupráci v oblasti kybernetickej bezpečnosti medzi úradom a Kabinetom pre inštitucionálnu bezpečnosť Kancelárie prezidenta Brazílskej federatívnej republiky v máji 2025. Na memorandum nadviazalo pracovné stretnutie v decembri s predstaviteľom Ministerstva zahraničných vecí Brazílskej federatívnej republiky, na ktorom sa prediskutovalo aktuálne nastavenie kompetencií úradov a orgánov štátnej správy pri riešení kybernetických záležitostí. Implementácia memoranda ostáva významným mementom pri budovaní vzájomnej úzkej spolupráce a je dôležité v nastolenom trende pokračovať.

V októbri 2025 bolo podpísané Memorandum o porozumení medzi úradom a Národným úradom pre kybernetickú bezpečnosť **Rwandskej republiky** o posilnení spolupráce v oblasti kybernetickej bezpečnosti. Návšteva bola finančne podporená rozvojovým nástrojom SlovakAid – Sharing Slovak Expertise. Rwandská delegácia ocenila stav opatrení a kybernetickú bezpečnosť v Slovenskej republike. Identifikovala viacero oblastí, v ktorých vidí perspektívu vzájomnej spolupráce, ako napríklad zriadenie Národného bezpečnostného úradu Rwandy, podpora budovania kyberkomunity, podpora vzdelávania, proces certifikácie audítorov a manažérov kybernetickej bezpečnosti, proces vykonávania auditov - auditing scheme, založenie Rady audítorov, riadenie kybernetického útoku alebo účasť na Cyber Game.

Pokiaľ išlo o bilaterálnu spoluprácu na úrovni KCCKB osobitná pozornosť bola venovaná bilaterálnej spolupráci s **českým národným koordinačným centrom** (NCC-CZ). V roku 2025 bola táto spolupráca formalizovaná podpisom memoranda o porozumení, ktoré vytvorilo rámec pre systematickú výmenu informácií, koordináciu aktivít a prípravu spoločných iniciatív.

Výmena zahraničných informácií

Elektronizácia registrov zahraničných utajovaných skutočností prostredníctvom online prepojenia s registrami utajovaných skutočností orgánov verejnej moci umožňuje bezpečnú, rýchlejšiu a flexibilnejšiu evidenciu a elektronickú distribúciu utajovaných skutočností. V roku 2025 úrad jednotlivým registrom utajovaných skutočností, zriadenými orgánmi verejnej moci, naďalej poskytoval metodickú pomoc pri elektronickej evidencii utajovaných skutočností. Pracovisko centrálneho registra spracovalo 2760 utajovaných skutočností NATO a 3135 utajovaných skutočností EÚ. Úrad sprostredkoval aj výmenu 90 utajovaných skutočností cudzej moci. Na úrade od roku 2010 pôsobí register utajovaných skutočností NATO ATOMAL. V roku 2025 v ňom neboli zaevidované žiadne ATOMAL utajované písomnosti.

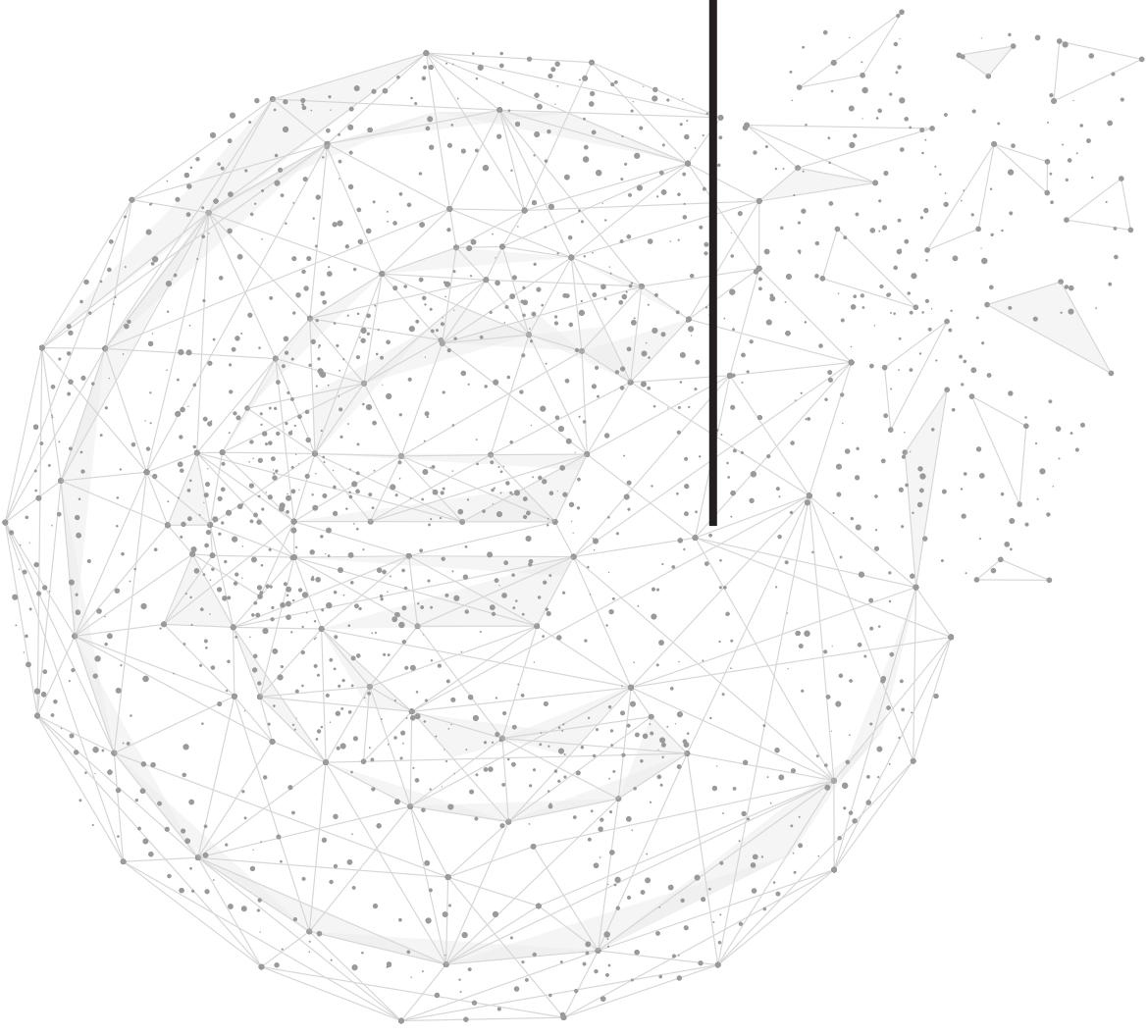
STUPEŇ UTAJENIA	2024	2025
NATO RESTRICTED	1198	1398
EU RESTRICTED	1232	1040
CUDZIA MOC VYHRADENÉ	484	63
NATO CONFIDENTIAL	413	414
EU CONFIDENTIAL	939	1039
CUDZIA MOC DÔVERNÉ	41	23
NATO SECRET	819	948
EU SECRET	882	1056
CUDZIA MOC TAJNÉ	22	4
NATO TOP SECRET	0	0
EU TOP SECRET	0	0
CUDZIA MOC PRÍSNE TAJNÉ	0	0
NATO SPOLU	2430	2760
EU SPOLU	3053	3135
CUDZIA MOC SPOLU	547	90

Národný bezpečnostný úrad má od roku 2021 zriadené centrálne úložisko utajovaných skutočností pre dočasné uloženie utajovaných skutočností, ktoré majú trvalú dokumentárnu hodnotu. Centrálne úložisko utajovaných skutočností je zriadené na detašovanom pracovisku v Topoľčiankach.

V roku 2025 bola spustená do prevádzky zaručená konverzia, ktorú úrad vykonáva podľa vyhlášky Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. 70/2021 Z. z. o zaručenej konverzii.

09.

HOSPODÁRENIE



Rozpis záväzných ukazovateľov rozpočtu kapitoly 41 – Národný bezpečnostný úrad na rok 2025, vplyv rozpočtových opatrení na výšku upraveného rozpočtu, skutočné čerpanie rozpočtových prostriedkov k 31. decembru 2025 a percentuálne vyhodnotenie plnenia k upravenému rozpočtu je uvedený v tabuľke č. 1.

Záväzné ukazovatele rozpočtu úradu pre rok 2025 schválené zákonom 345/2024 o štátnom rozpočte na rok 2025 zo dňa 3. decembra 2024 v znení neskorších predpisov boli úradom dodržané. Pri hospodárení s finančnými prostriedkami úrad postupoval podľa zásad hospodárnosti, efektívnosti a účelnosti pri dodržiavaní legislatívnych predpisov, najmä zákona č. 523/2004 o rozpočtových pravidlách verejnej správy, zákona č. 357/2015 o finančnej kontrole a audite, zákona č. 343/2015 o verejnom obstarávaní, uznesení vlády Slovenskej republiky a metodických pokynov a usmernení Ministerstva financií Slovenskej republiky.

Tabuľka č. 1: Rozpis záväzných ukazovateľov pre kapitolu 41 – Národný bezpečnostný úrad (v eurách)

Ukazovatele	Schválený rozpočet	Upravený rozpočet	Skutočnosť	Plnenie k upr. rozpočtu
I. Príjmy kapitoly celkom	**22 000, 00**	**22 000, 00**	**25 642, 58**	**116, 56 %**
A. Záväzný ukazovateľ (zdroj 111)	20 000, 00	20 000, 00	23 613, 35	118, 07 %
kód zdroja 72e	2 000, 00	2 000, 00	2 029, 23	101, 46 %
II. Výdavky kapitoly celkom (A + B+ C + C.1)	**17 984 619, 00**	**19 284 490, 69**	**19 126 268, 63**	**99, 18 %**
A. Výdavky spolu bez prostriedkov podľa § 17 ods. 4 zákona č. 523/2004 Z. z. a prostriedkov Európskej únie a prostriedkov z Plánu obnovy a odolnosti	**17 982 619, 00**	**19 223 601, 76**	**19 065 380 ,01**	**99, 18 %**
z toho:				
A.1. rozpočtové prostriedky kapitoly (kód zdroja 111 + 11H + 11UA)	17 982 619, 00	19 218 669, 23	19 060 447, 48	99, 18 %
A.2. prostriedky na spolufinancovanie	0, 00	0, 00	0, 00	0, 00 %
A.3. mzdy, platy, služ. príj. a ost. os. vyrovnania (610),kód zdroja 111+11H+11UA)	8 273 100, 00	8 449 300, 00	8 309 484, 50 *	98, 35%
z toho:				
mzdy, platy, služ. príjmy a ost. os. vyrovnania aparátu ústred. orgánu (kód zdroja 111 + 11H + 11UA)	8 273 100, 00	8 449 300, 00	8 309 484, 50 *	98, 35 %
Počet zamestnancov RO podľa prílohy č. 1 k uzneseniu vlády SR č. 606/2024	259 osôb	259 osôb	234 osôb **	90, 35 %
z toho: aparát ústredného orgánu	259 osôb	259 osôb	234 osôb **	90, 35 %
A.4. kapitálové výdavky (700) (bez prostriedkov na spolufinancovanie)	1 470 513, 00	1 470 513, 00	1 470 081, 71	99 97 %
z toho: kód zdroja 111	1 470 513, 00	1 470 513, 00	1 470 081, 71	99, 97 %
A.5. Plán obnovy a odolnosti – prostriedky na úhradu DPH	0, 00	4 932, 53	4 932, 53	100, 00 %
z toho: kód zdroja 1P02	0, 00	4 932, 53	4 932, 53	100, 00 %
B. Prostriedky podľa § 17 ods. 4 zákona č. 523/2004 Z. z. (Podľa § 17 ods. 4 z. č. 523/2004 Z. z. je RO oprávnená čerpať tento limit do výšky rozpočt. príjmov skut. prijatých a je oprávnená prekročiť limit výdavkov z dôvodu dosiahnutia vyšších ako rozpočt. príjmov.)	**2 000, 00**	**2 000, 00**	**2 000, 00**	**100, 00 %**
C. Prostriedky z rozpočtu Európskej únie a prostriedky z Plánu obnovy a odolnosti spolu	**0, 00**	**58 888, 93**	**58 888, 62**	**99, 99 %**
z toho:				
C.1 prostriedky z rozpočtu Európskej únie	0, 00	0, 00	0, 00	0, 00 %
C.2 prostriedky z Plánu obnovy a odolnosti	0, 00	58 888, 93	58 888, 62	99, 99 %
z toho: kód zdroja 3P02	0, 00	58 888, 93	58 888, 62	99, 99 %
D. Výdavky štátneho rozpočtu na realizáciu programov vlády SR a častí programov vlády SR	**17 984 619, 00**	**19 284 490, 69**	**19 126 268, 63**	**99, 18 %**
0D9 Bezpečnosť informácií	17 919 173, 00	19 000 633, 21	18 842 802, 95	99, 17 %
0EK0U Informačné technológie financované zo štátneho rozpočtu – NBÚ	65 446, 00	283 857,48	283 465,68	99, 86%
E. Systemizácia policajtov v štátnej službe	**236 osôb** **7 468 014, 00**	**236 osôb** **7 630 214, 00**	**211 osôb **** **7 554 305, 67 *****	**89, 41 %** **99, 01 %**

* plus 81 926,91 eur financovaných z ostatných samostatných účtov (projekty NIS2, TestCertSK a TrustBoost)
** počet zamestnancov k 31.12.2025 (vrátane 7 obsadených tabuľkových miest na materskej a rodičovskej dovolenke)
*** plus 62 682,66 eur financovaných z ostatných samostatných účtov (projekty NIS2, TestCertSK a TrustBoost)

Rozpočet na rok 2026

Zákonom č. 303/2025 o štátnom rozpočte na rok 2026 zo dňa 21. októbra 2025 boli schválené záväzné ukazovatele štátneho rozpočtu jednotlivých kapitol na rok 2026. V nadväznosti na bod C.1. uznesenia vlády SR č. 492 zo dňa 10. októbra 2025 k návrhu rozpočtu verejnej správy na roky 2026 až 2028 a ustanovenie § 6 ods. 3 zákona č. 523/2004 o rozpočtových pravidlách verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov boli úradu oznámené záväzné ukazovatele štátneho rozpočtu na rok 2026.

Výdavky úradu pre rok 2026 sú rozpočtované v rámci programu 0D9 – Bezpečnosť informácií a medzirezortného podprogramu 0EK0U – Informačné technológie financované zo štátneho rozpočtu – NBÚ v celkovej sume 18 024 126,00 eur. Príjmy úradu ako záväzný ukazovateľ sú rozpočtované v sume 20 000,00 eur, príjmy pod kódom zdroja 72e sú rozpočtované v sume 2 000,00 eur.

Rozpočtované prostriedky úradu použije pri plnení úloh, ktoré mu vyplývajú z jeho postavenia ústredného orgánu štátnej správy pre ochranu utajovaných skutočností, šifrovú službu, kybernetickú bezpečnosť a dôveryhodné služby. Ďalšie úlohy úradu súvisia s plnením úloh z uznesení vlády Slovenskej republiky a vyplývajú zo záväzkov SR voči EÚ a NATO.

Verejné obstarávanie

Portál Transparex.sk aj v roku 2025 zverejnil hodnotenie verejných obstarávateľov v rámci rebríčka „Zodpovední verejní obstarávatelia“, v ktorom analyzoval subjekty z verejného sektora. Hodnotenie zahŕňalo ústredné orgány štátnej správy, samosprávy, školy, zdravotnícke zariadenia, ako aj ďalšie štátne inštitúcie a podniky.

Národný bezpečnostný úrad dosiahol v tomto hodnotení opätovne veľmi dobrý výsledok a získal známku A+, čím potvrdil vysokú úroveň procesov verejného obstarávania. S celkovým bodovým ziskom 80,37 bodu sa úrad umiestnil na 20. mieste medzi ústrednými orgánmi štátnej správy, čo predstavuje posun oproti predchádzajúcemu roku.

Výsledky hodnotenia poukazujú na systematický a odborný prístup k verejnému obstarávaniu, orientovaný na efektívne využívanie verejných prostriedkov, transparentnosť postupov a vytváranie rovných podmienok hospodárskej súťaže.

Nová fyzická a objektová bezpečnosť úradu

V súvislosti s vybudovaním novej fyzickej a objektovej bezpečnosti úradu bolo zrealizovaná hlasová signalizácia požiaru, elektrická požiarna signalizácia, elektrický zabezpečovací systém, systém kontroly vstupu a nadstavbový systém C4.

Rekonštrukcia jedálne

V priebehu roka úrad zároveň efektívne využil existujúce priestorové kapacity rekonštrukciou dlhodobo nevyužívanej časti budovy, ktorá v minulosti slúžila ako skladový priestor. Jej prestavbou vznikla funkčná a účelová jedáleň, ktorá dnes slúži všetkým zamestnancom a príslušníkom úradu. Nová jedáleň vytvára príjemné zázemie na obed a krátku prestávku, čo má pozitívny vplyv na pohodu a sústredenie počas pracovného dňa.

Úprava priestoru vychádzala z potreby zlepšiť každodenné pracovné podmienky a zároveň zodpovedne využívať existujúce kapacity úradu. Súčasťou priestoru sú aj automaty na občerstvenie a teplé nápoje, ktoré vytvorili možnosť stravovania priamo na pracovisku.

Národná kultúrna pamiatka – kaštieľ Brunovce

Národný bezpečnostný úrad má vo svojej správe renesančný kaštieľ z druhej polovice 17. storočia nachádzajúci sa v obci Brunovce, okres Nové Mesto nad Váhom. Kaštieľ je zapísaný v Ústrednom zozname pamiatkového fondu, v registri nehnuteľných národných kultúrnych pamiatok. Okolo kaštieľa je anglický park z konca 18. storočia.

Po minulé roky bol kaštieľ v obmedzenej miere prístupný verejnosti a zároveň bol využívaný predovšetkým na služobné účely ako školiace stredisko, alebo priestor na rokovania či konferencie úradu. Kaštieľ, vrátane záhrady a kaplnky, sa dal využiť aj na súkromné akcie pracovníkov úradu a ostatných občanov, napríklad svadby, oslavy výročia obce, sväté omše v priestoroch kaplnky a podobne.

Vzhľadom na nevyhovujúci technický stav tejto národnej kultúrnej pamiatky, úrad už v roku 2022 pristúpil k zámeru jej kompletnej obnovy. Cieľom je realizácia rekonštrukcie z finančných prostriedkov z priorít Plánu obnovy a odolnosti Slovenskej republiky pri obnove verejných historických a pamiatkovo chránených budov.

V roku 2023 boli zrealizované reštaurátorský a architektonicko-historický výskum kaštieľa. Na základe vypracovaných správ bolo vydané rozhodnutie, v ktorom Krajský pamiatkový úrad (KPÚ) v Trenčíne schválil návrh na reštaurovanie. V roku 2024 bola vypracovaná Projektová dokumentácia pre vydanie stavebného povolenia, ktorá bola doručená Krajskému pamiatkovému úradu v Trenčíne za účelom vydania Záväzného stanoviska. Po zapracovaní všetkých pripomienok do projektovej dokumentácie bolo dňa 19.12.2024 vydané záväzné stanovisko. Následne bude projektová dokumentácia postúpená príslušnému stavebnému úradu MV SR za účelom vydania stavebného povolenia.

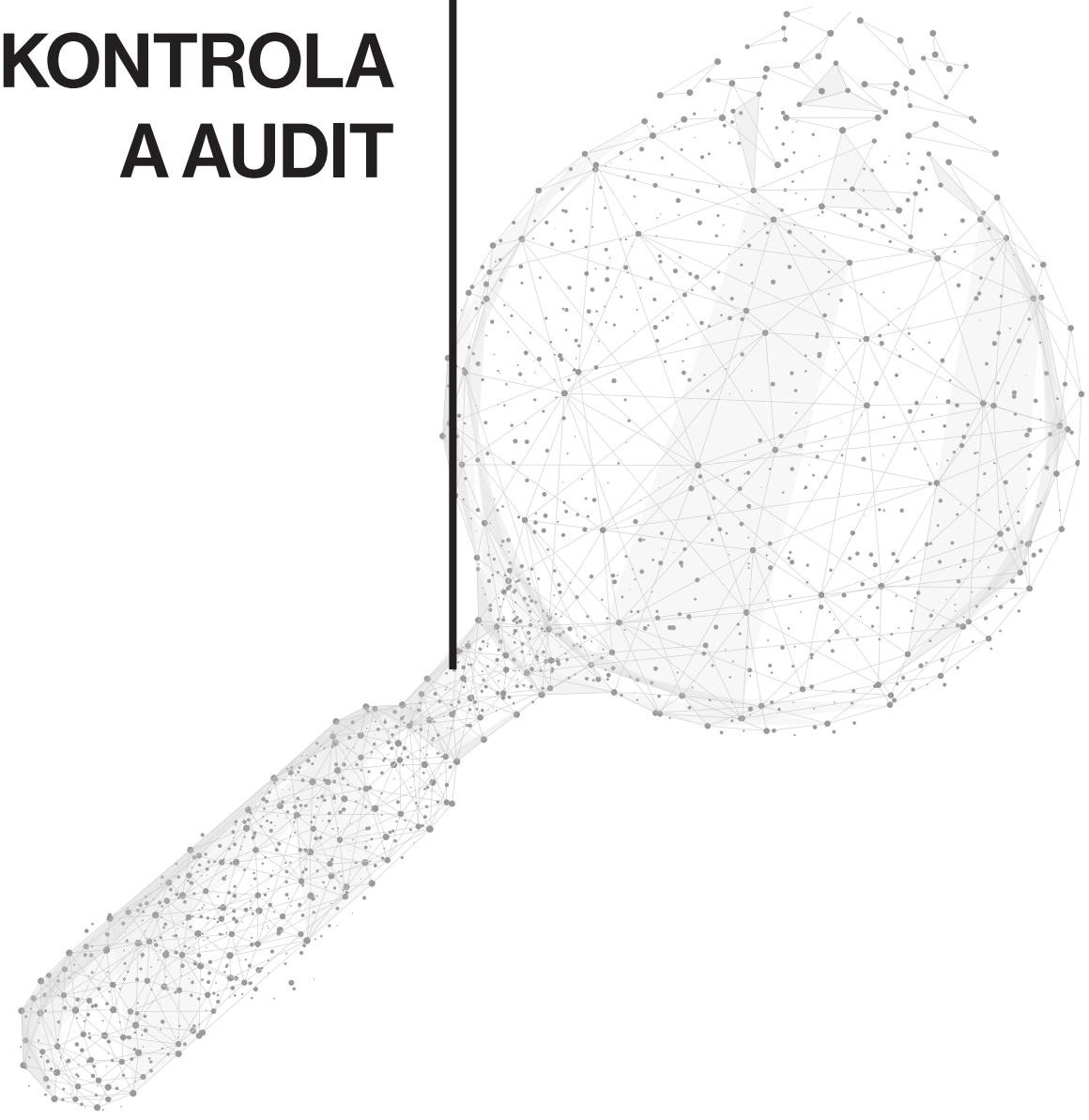
Z dôvodu hygienickej závadnosti vody zo studne, ktorá podľa opakovaných rozborov nespĺňala podmienky na pitnú vodu, bol objekt kaštieľa v roku 2024 napojený na verejný vodovod.

V anglickom parku, ktorý je súčasťou NKP, boli v zmysle povolení KPÚ Trenčín vykonané sanačné výruby, ozdravné orezy a následná výsadba nových drevín.

Dňa 23.04.2025 nadobudlo právoplatnosť Stavebné povolenie vydané príslušným stavebným úradom. Na základe všetkých potrebných povolení v druhej polovici roka 2025 prebiehalo spracovanie súťažných podkladov k vyhláseniu zákazky na „Obnovu NKP účelové zariadenie kaštieľ Brunovce“, pričom samotné vyhlásenie zákazky na predkladanie ponúk uchádzačmi je naplánované v roku 2026.

10.

KONTROLA A AUDIT



Kontrola a audit kontrolná činnosť

Úrad vykonal kontrolu naprieč všetkými úsekmi pôsobnosti zverenej zákonmi v 37 subjektoch:

- kontroly na úseku ochrany utajovaných skutočností – 18 subjektov (10 štátnych orgánov a 8 držiteľov potvrdenia o priemyselnej bezpečnosti)
- dohľad a inšpekcia v rozsahu plnenia záväzkov vyplývajúcich z členstva v NATO – 1 subjekt
- kontroly na úseku kybernetickej bezpečnosti 19 subjektov (prevádzkovateľov základných služieb – 6 orgánov verejnej moci a 13 subjektov súkromného sektora).

Kontrolné skupiny sa zamerali najmä na komplexnosť prijatých opatrení a ich koordináciu naprieč jednotlivými úsekmi. Celkovo bolo v kontrolovaných subjektoch zaznamenaných 63 kontrolných zistení:

- 46 na úseku ochrany utajovaných skutočností,
- 17 na úseku kybernetickej bezpečnosti (údaj k 05.02.2026).

Dohľadová činnosť

Úrad v roku 2025 vykonával ex ante a ex post dohľad s cieľom preveriť, či kvalifikovaní poskytovatelia dôveryhodných služieb a nimi poskytované kvalifikované dôveryhodné služby spĺňajú požiadavky stanovené v nariadení (EÚ) č. 910/2014 v platnom znení.

V priebehu roka 2025 bolo úradu doručených **osem žiadostí o udelenie kvalifikovaného štatútu** pre kvalifikované dôveryhodné služby – vyhotovovanie kvalifikovaných elektronických pečiatok, uchovávanie kvalifikovaných elektronických podpisov, uchovávanie kvalifikovaných elektronických pečatí. Vzhľadom na skutočnosť, že žiadosti neboli kompletné a žiadatelia ani na výzvu úradu žiadosti nedoplnili, k 31.12.2025 nebol udelený žiaden kvalifikovaný štatút na požadovanú kvalifikovanú dôveryhodnú službu.

K 31.12.2025 bol **odňatý kvalifikovaný štatút 19 kvalifikovaným dôveryhodným službám**, pričom jednému kvalifikovanému poskytovateľovi dôveryhodných služieb bol odobratý kvalifikovaný štatút (ukončenie činnosti a odobraté kvalifikované štatúty boli aj jeho 10 kvalifikovanými dôveryhodným službám) a bolo zrušených deväť kvalifikovaných dôveryhodných služieb, ktoré boli závislé na Koreňovej certifikačnej autorite.

V hodnotenom období úrad posúdil **šesť správ z kontrolného auditu** od kvalifikovaných poskytovateľov kvalifikovaných dôveryhodných služieb.

Metodická činnosť

Na úseku **regulácie a metodiky** úrad vydáva odborné stanoviská a metodické usmernenia k všeobecne záväzným právnym predpisom, ktoré poskytuje štátnym orgánom, fyzickým osobám a právnickým osobám vo všetkých oblastiach jeho pôsobnosti. Vybrané úrad následne anonymizuje a zverejňuje na svojom webovom sídle. Celkovo úrad v roku 2025 vydal **402 metodických usmernení a odborných stanovísk**:

na úseku ochrany utajovaných skutočností	**36**
personálna bezpečnosť	11
administratívna bezpečnosť	1
priemyselná bezpečnosť	13
fyzická bezpečnosť a objektová bezpečnosť	0
bezpečnosť technických prostriedkov	5
bezpečnostní zamestnanci	1
cudzia moc	5
v oblasti šifrovej ochrany informácií	**0**
na úseku kybernetickej bezpečnosti	**304**
na úseku dôveryhodných služieb	**16**
prierezové stanoviská	**44**
nezaradené	**2**

Vnútorná kontrola

V roku 2025 sekcia kontroly a bezpečnosti vykonala šesť kontrol v zmysle zákona č. 10/1996 Z. z. o kontrole v štátnej správe v znení neskorších predpisov, kde tri kontroly boli ukončené protokolom a tri kontroly prebiehajú. Predmetom uvedených kontrol bola kontrola dodržiavania základného času služby v týždni a služby vykonávanej nad základný čas služby v týždni a služobnej pohotovosti u príslušníkov Národného bezpečnostného úradu a dodržiavania pracovného času u zamestnancov vo verejnom záujme, kontrola fyzickej a objektovej bezpečnosti Národného bezpečnostného úradu, mimoriadna kontrola udeľovania a čerpania služobného voľna príslušníkov Národného bezpečnostného úradu v zmysle zákona č. 73/1998 Z. z. o štátnej službe príslušníkov Policajného zboru, Slovenskej informačnej služby, Zboru väzenskej a justičnej stráže Slovenskej republiky a Železničnej polície v znení neskorších predpisov, kontrola tuzemských a zahraničných služobných ciest, kontrola správnosti vyplácania mzdových prostriedkov a dávok výsluhového zabezpečenia, kontrola splnenia opatrení prijatých na odstránenie zistených nedostatkov a ich účinnosť, ako aj jedna operatívna kontrola liečebného režimu.

Vnútorný audit

V roku 2025 boli útvarom vnútorného auditu vykonané štyri plánované vnútorné audity a jeden mimoriadny vnútorný audit, ktorých cieľom bolo overiť a hodnotiť:

- dodržiavanie Nariadenia riaditeľa NBÚ č. 2/2024 o finančnom riadení a finančnej kontrole za obdobie od 01.03.2024 do 31.12.2024 v povinnej osobe NBÚ,
- dodržiavanie zákona č. 278/1993 Z. z. o správe majetku štátu za rok 2024 v povinnej osobe NBÚ,
- hospodárnosť, efektívnosť, účinnosť a účelnosť pri hospodárení s verejnými financiami – prostriedky ŠR - za rok 2024 v povinnej osobe KCCKB,
- hospodárnosť, efektívnosť, účinnosť a účelnosť pri hospodárení s verejnými financiami – prostriedky ŠR - za obdobie od 01.07.2024 do 30.06.2025 v povinnej osobe NBÚ,
- oprávnenosť nákladov použitých na základe Dohody o grante – za obdobie od 01.11.2022 do 24.07.2025 v povinnej osobe KCCKB.

Vykonanými vnútornými auditmi boli zistené štyri nedostatky. Dva nedostatky boli strednej závažnosti, systémové – finančne nevyčísliteľné a dva nedostatky boli nízkej závažnosti, nesystémové – finančne nevyčísliteľné.

Povinnej osobe boli v zmysle zákona č. 357/2015 o finančnej kontrole a audite stanovené lehoty na prijatie opatrení na nápravu nedostatkov a na odstránenie príčin ich vzniku, zaslanie zoznamu prijatých opatrení a splnenie prijatých opatrení.

Bezpečnostné riziká

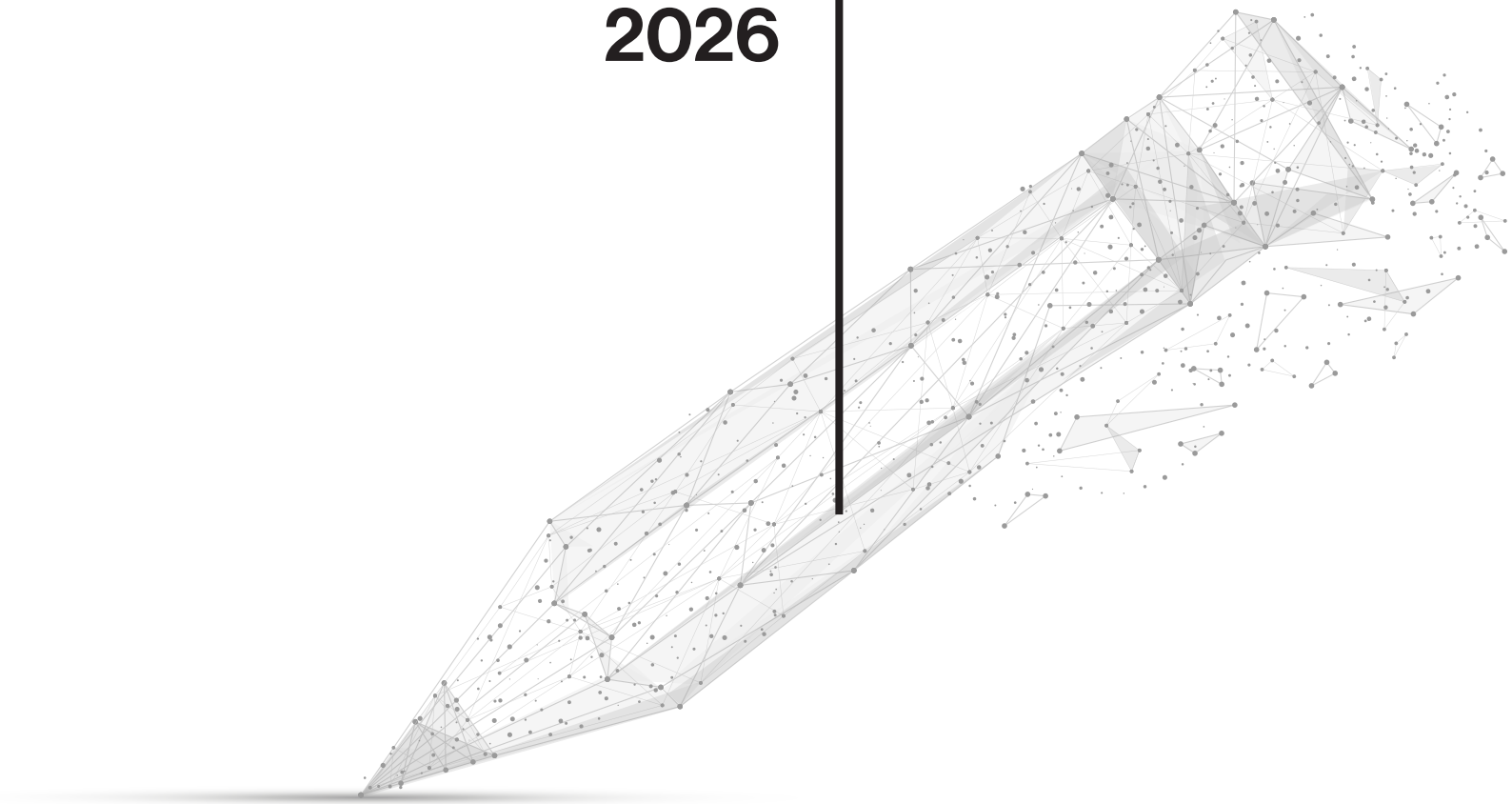
NBÚ vykonával svoju pôsobnosť na úseku vnútornej ochrany, získaval, sústreďoval, analyzoval a preveroval informácie o bezpečnostných rizikách týkajúcich sa pôsobnosti úradu a jeho príslušníkov a zamestnancov. kvalifikovaných dôveryhodných služieb, ktoré boli závislé na Koreňovej certifikačnej autorite.

Sťažnosti a petície

Sekcia kontroly a bezpečnosti NBÚ prijala tri sťažnosti, z toho jedna sťažnosť bola vyhodnotená ako neopodstatnená a dve sťažnosti boli postúpené na vecné útvary úradu.

11.

PRIORITY NA ROK 2026



PRIORITY NA ROK 2026

Úrad bude naďalej:

podporovať vzdelávanie a výcvik špecialistov na odborných kurzoch, seminároch a školeniach doma i v zahraničí s cieľom nadobúdať nové zručnosti a prehlbovať ich kvalifikáciu. Prehlbovanie kvalifikácie je dôležité najmä z pohľadu požiadaviek na prevádzkovanie certifikačného orgánu pre produkty hodnotené v zmysle európskej horizontálnej schémy založenej na Common Criteria.

rozvíjať spôsobilosti certifikovať IKT produkty s dôrazom na rozšírenie akreditácie CO NBÚ podľa aktualizovaných resp. pripravovaných európskych a národných certifikačných schém (eIDAS 2.0, EUDIW – peňaženka elektronickej identyty, EU5G – 5G služby, EUAI – umelá inteligencia, EUCS - cloudové služby, EUMSS – riadené bezpečnostné služby).

rozvíjať spôsobilosti v oblasti certifikácie mechanických zabezpečovacích, technických zabezpečovacích a technických prostriedkoch, či prostriedkoch šifrovej ochrany informácií.

K prioritám pre rok 2026 patrí aj realizácia projektov výskumu a vývoja financovaných z prostriedkov EÚ ako napríklad „Výskum a vývoj post kvantových šifrovacích algoritmov“, alebo „Quantum-Resistant Cryptography in Practice (QARC)“. Na projektoch sa okrem príslušníkov sekcie akreditácie a certifikácie bude podieľať aj akademická obec a partnerské národné bezpečnostné úrady zo štátov Európskej únie. Projekty sú primárne zamerané na praktickú aplikáciu novej generácie šifrovacích algoritmov do knižníc programovacích jazykov a vývojových prostredí a zároveň aj prípravy stratégií a postupov na celospoločenský prechod na nové kryptografické štandardy.

Medzi priority úradu na rok 2025 sa radí aj obmena mechanických zábranných prostriedkov na úrade, nastavenie riadneho fungovania nového systému evidencie návštev a zabezpečenie implementácie Národnej protikorupčnej stratégie Slovenskej republiky na roky 2026 – 2029.

© 2026 NÁRODNÝ BEZPEČNOSTNÝ ÚRAD