NÁRODNÝ
BEZPEČNOSTNÝ
ÚRAD

KONSOLIDOVANÁ VÝROČNÁ SPRÁVA

NÁRODNÝ
BEZPEČNOSTNÝ
ÚRAD

KONSOLIDOVANÁ VÝROČNÁ SPRÁVA

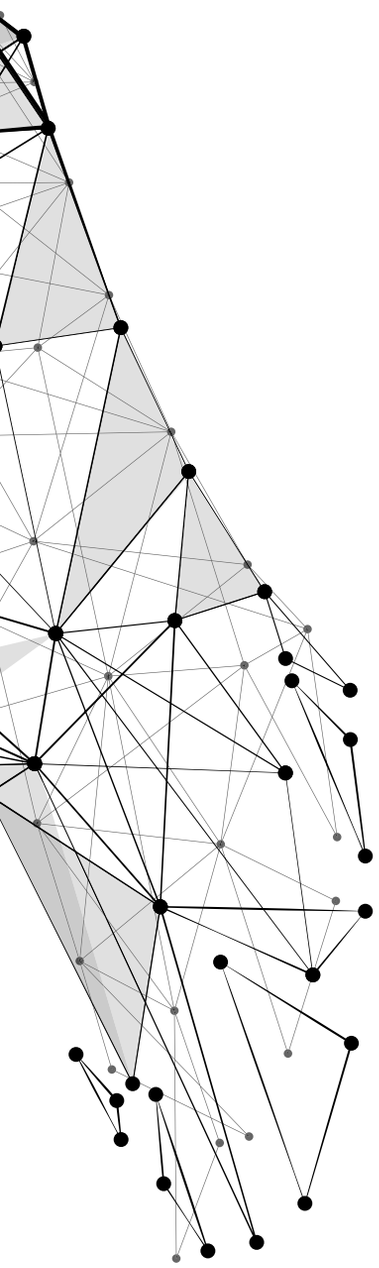
OBSAH

IDENTIFIKÁCIA ORGANIZÁCIE

Národný bezpečnostný úrad 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 o ochrane utajovaných skutočností a súvisiace všeobecne záväzné právne predpisy a platné štandardy

Zákon č. 272/2016 o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a súvisiace všeobecne záväzné právne predpisy a právne predpisy Európskej únie

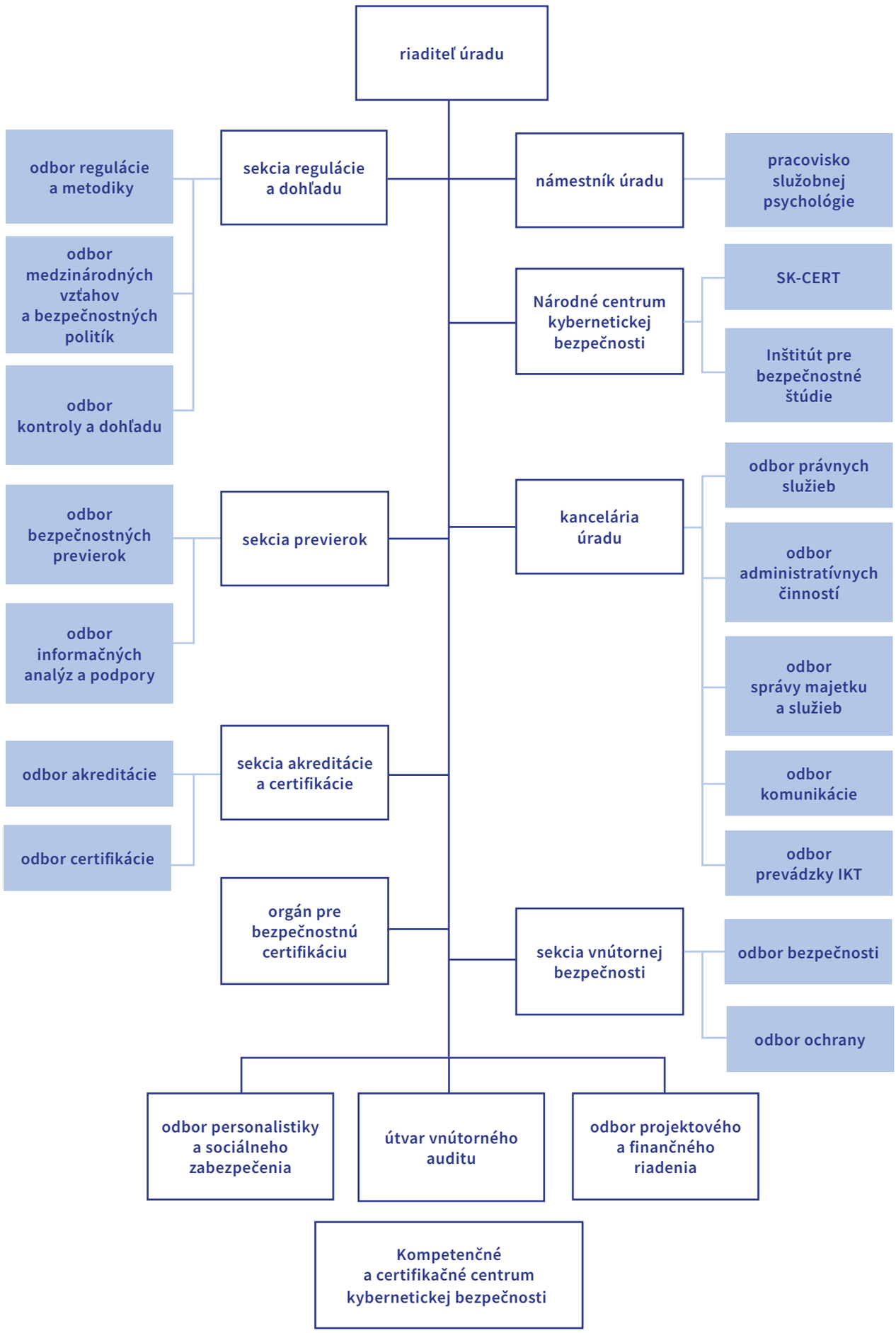
Zákon č. 69/2018 o kybernetickej bezpečnosti a súvisiace všeobecne záväzné právne predpisy, medzinárodné právne predpisy a právne predpisy Európskej únie

VEDENIE ÚRADU

Na čele 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



KÚ

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, buduje a rozvíja externé vzťahy a spoluprácu, zabezpečuje komunikáciu smerom k verejnosti.

SP

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.

SRD

Sekcia regulácie a dohľadu

Je vecným útvarom úradu v oblasti ochrany utajovaných skutočností, šifrovej ochrany informácií, kybernetickej bezpečnosti, dôveryhodných služieb a verejnej regulovanej služby, ktorú poskytuje globálny satelitný navigačný systém zriadený v programe Galileo.

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

Vydáva stanoviská a metodiky, vytvára koncepčné a strategické materiály, vypracováva bezpečnostné a znalostné štandardy, ktorých ustálené postupy zavádza do medzinárodných štandardov cez pracovné skupiny ISO alebo európske štandardizačné inštitúcie, vydáva certifikačné a podpisové politiky.

Organizačne pripravuje a realizuje skúšky bezpečnostných zamestnancov a školenia na úseku ochrany utajovaných skutočností. Na medzinárodnej úrovni zastupuje úrad a koordinuje zahraničné aktivity úradu. Pripomienkuje návrhy legislatívnych materiálov v medzirezortnom pripomienkovom konaní a vykonáva legislatívny proces materiálov so zahraničným prvkom.

Jej styční dôstojníci v EÚ, NATO a USA plnia úlohy pri rozvíjaní a budovaní medzinárodných vzťahov a spolupráce úradu v zahraničí. Zabezpečujú komunikáciu medzi úradom a zahraničnými partnermi a zastupujú záujmy Slovenskej republiky.

SVB

Sekcia vnútornej bezpečnosti

Sekcia vnútornej 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.

SAC

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.

NCKB

Národné centrum kybernetickej bezpečnosti

Plní úlohy národnej jednotky CSIRT. Zabezpečuje služby spojené s riadením bezpečnostných incidentov, odstraňovaním ich následkov a následnou obnovou činnosti informačných systémov v spolupráci s ich vlastníkmi a prevádzkovateľmi. Zabezpečuje aj výkon analytických činností, výskumu, rozširovania bezpečnostného povedomia a vzdelávania v oblasti kybernetickej bezpečnosti a ďalšie úlohy na úseku kybernetickej bezpečnosti.

V rámci Národného centra kybernetickej bezpečnosti (NCKB) pôsobí Inštitút pre bezpečnostné štúdie, ktorý plní úlohy na úseku všeobecnej analytiky, posudzovania bezpečnostných rizík, vyhodnocovania politík, tvorby prognóz, stratégií a implementačných plánov úradu.

OPSZ

Odbor personalistiky a sociálneho zabezpečenia

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

OPFR

Odbor projektového a finančného riadenia

Zabezpečuje projektové a programové riadenie v podmienkach úradu.

ÚVA

Útvar vnútorného auditu

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

OBC

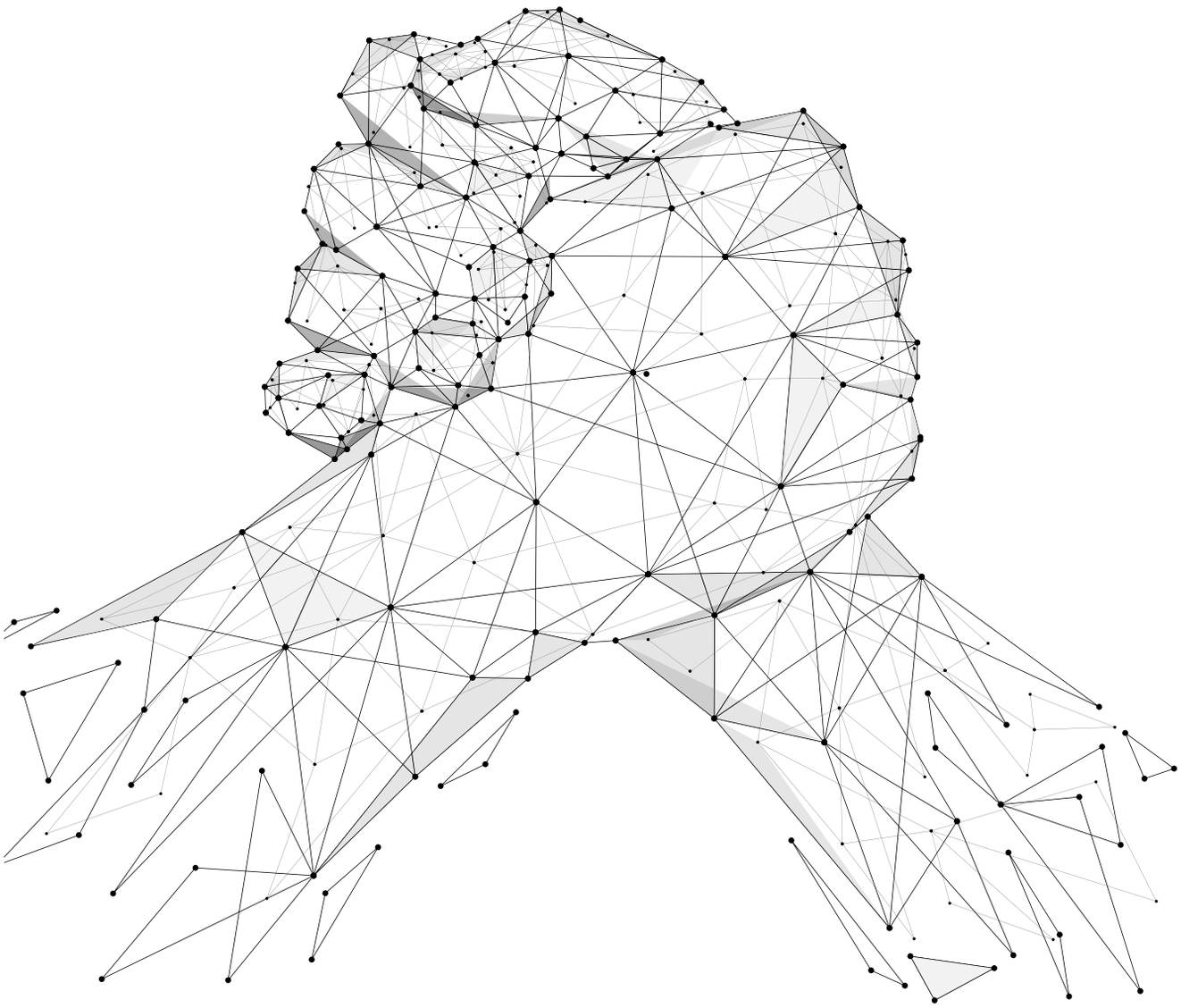
Orgán pre bezpečnostnú certifikáciu

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

KCCKB

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.



ĽUDSKÉ ZDROJE

Prehľad o počte a štruktúre príslušníkov a zamestnancov

	Štátna služba		Zamestnanci		Príslušníci a zamestnanci	
Prípravná štátna služba	**36**	16,98 %				
Stála štátna služba	**168**	79,25 %				
Dočasná štátna služba	**8**	3,77 %				
Spolu	**212**	90,6 %	**22**	9,4 %	**234**	100 %

Veková štruktúra príslušníkov a zamestnancov

	Príslušníci		Zamestnanci		Príslušníci a zamestnanci	
do 34 rokov	42	19,81 %	8	36,36 %	50	21,37 %
35 — 49 rokov	115	54,25 %	7	31,82 %	122	52,14 %
50 — 59 rokov	43	20,28 %	3	13,64 %	46	19,66 %
60 a viac rokov	12	5,66 %	4	18,18 %	16	6,84 %
Spolu	212	90,6 %	22	9,4 %	234	100 %

Ženy a muži v NBÚ

	Príslušníci		Zamestnanci		Príslušníci a zamestnanci	
Ženy	105	94,59 %	6	5,41 %	111	47,43 %
Muži	107	86,99 %	16	13,01 %	123	52,56 %
Spolu	212	92,8 %	22	7,2 %	234	100 %

Vzdelanostná štruktúra príslušníkov a zamestnancov

Príslušníci			Zamestnanci	
0	0 %	Základné vzdelanie	0	0 %
34	16,04 %	Úplné stredné vzdelanie	8	36,36 %
6	2,83 %	Vysokoškolské vzdelanie I.st.	2	9,09 %
158	74,53 %	Vysokoškolské vzdelanie II.st.	12	54,55 %
14	6,6 %	Vysokoškolské vzdelanie III.st.	0	0 %
212	100 %	Spolu	22	100 %

SLUŽOBNÁ PRÍPRAVA

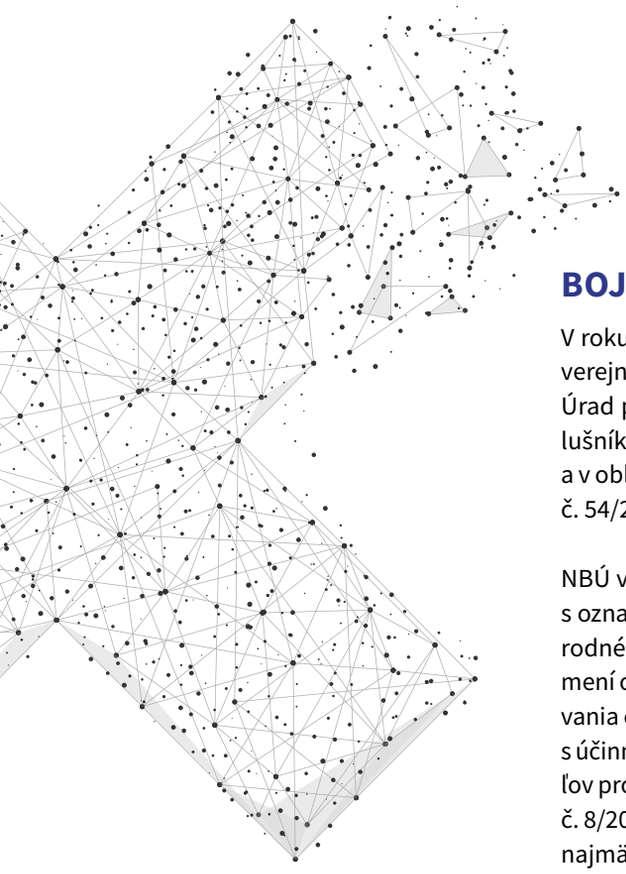
Príslušníci sekcie vnútornej bezpečnosti plnili úlohy v rámci služobnej prípravy cvičeniami v oblasti telesnej prípravy, streleckej prípravy, špeciálnej prípravy a zdravotníckej prípravy. Na strelecký a špeciálnu prípravu využívali zariadenia ozbrojených bezpečnostných zborov, ozbrojených zborov, Slovenskej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

PRACOVISKO SLUŽOBNEJ PSYCHOLÓGIE

Služobný psychológ počas roka 2024 realizoval 35 psychologických vyšetrení žiadateľov o prijatie do služobného pomeru príslušníka NBÚ, z toho 34 z nich bolo ku koncu roka uzavretých, pričom úspešnosť žiadateľov bola 79 %. Vykonalo sa aj sedem dopravno–psychologických vyšetrení, dve analýzy s cieľom zmapovať aktuálnu situáciu na vybraných útvaroch a bolo poskytnutých viac ako 180 hodín psychologického poradenstva. Pracovisko tiež pre niektoré útvary na základe ich požiadavky pripravilo odborné prednášky.

PREHLBOVANIE KVALIFIKÁCIE A ZVYŠOVANIE ZRUČNOSTÍ

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



BOJ PROTI KORUPCII

V roku 2024 sme aktualizovali protikorupčný program NBÚ. Jeho cieľom je ochrana verejného záujmu prostredníctvom zmenšovania priestoru a príležitostí pre korupciu. Úrad prijal protikorupčné systémové opatrenia, ktoré spočívajú vo vzdelávaní príslušníkov a zamestnancov úradu v oblasti zvyšovania protikorupčného povedomia a v oblasti oznamovania protispoločenskej činnosti, v súvislosti s novelizáciou zákona č. 54/2019 o ochrane oznamovateľov protispoločenskej činnosti.

NBÚ vydal na zabezpečenie jednotného postupu pri vybavovaní hlásení súvisiacich s oznamovaním protispoločenskej činnosti interný predpis – Nariadenie riaditeľa Národného bezpečnostného úradu č. 8/2024 o vnútornom systéme vybavovania oznámení o protispoločenskej činnosti, z dôvodu zosúladenia vnútorného systému vybavovania oznámení o protispoločenskej činnosti na úrade so zákonom č. 189/2023, ktorý s účinnosťou od 1. septembra 2023 novelizoval zákon č. 54/2019 o ochrane oznamovateľov protispoločenskej činnosti. Nariadenie riaditeľa Národného bezpečnostného úradu č. 8/2024 stanovuje 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 sekcie vnútornej bezpečnosti sa aktívne zúčastnili podujatí Úradu vlády Slovenskej republiky a Úradu na ochranu oznamovateľov. Jeden z príslušníkov sekcie sa stal členom Rady protikorupčných koordinátorov na Úrade vlády Slovenskej republiky.

Podľa interného predpisu – Nariadenie riaditeľa Národného bezpečnostného úradu č. 8/2020 o opatreniach v oblasti prevencie korupcie posudzovanie dôveryhodnosti partnerov vecného vzťahu – posudzujú pracovníci sekcie kontroly a bezpečnostiriziKovosť partnerov kvôli možnému korupčnému riziku.

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

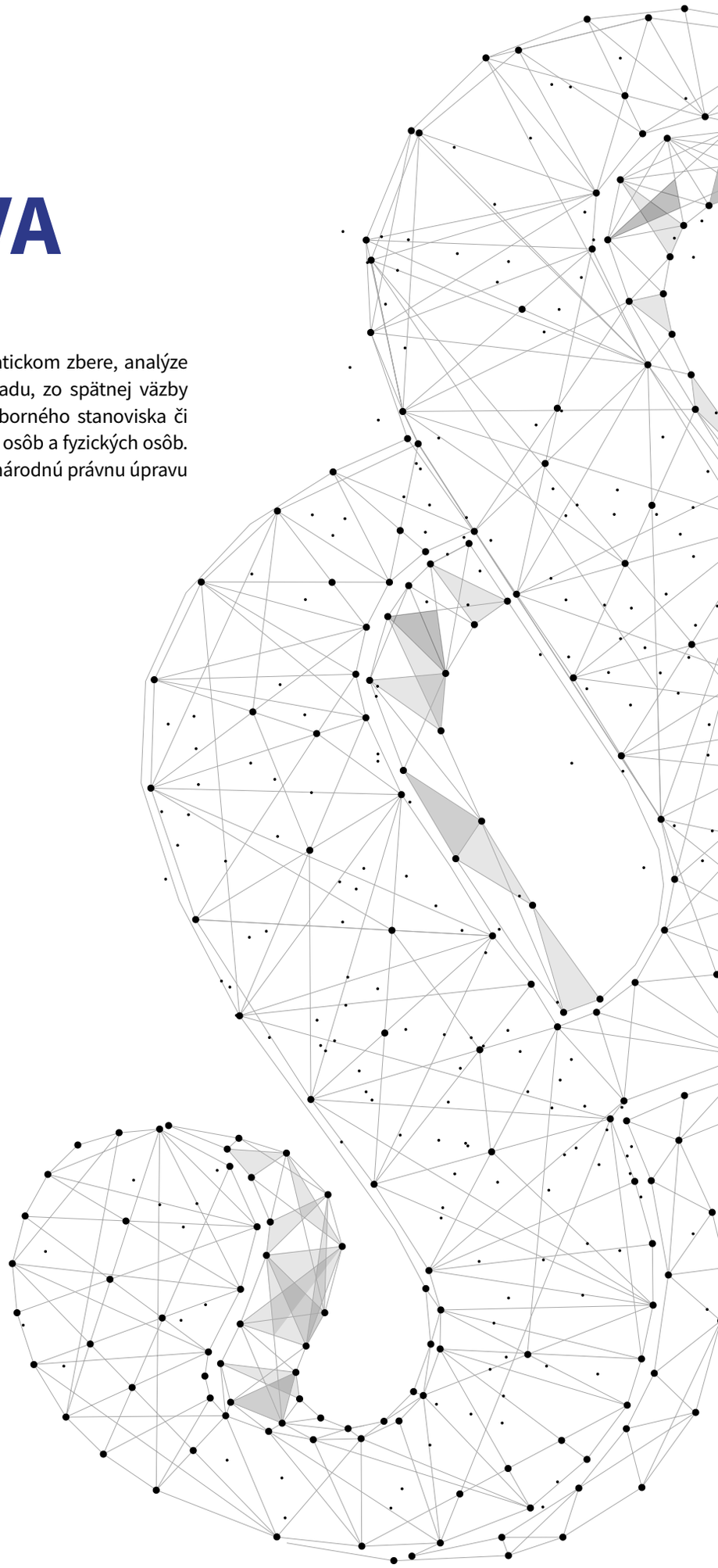
Školenia v oblasti podávania oznámení a boja proti korupcii boli zaradené aj do špecializovaného štúdia príslušníkov úradu a formou e-learningu boli preškolení všetci príslušníci úradu.

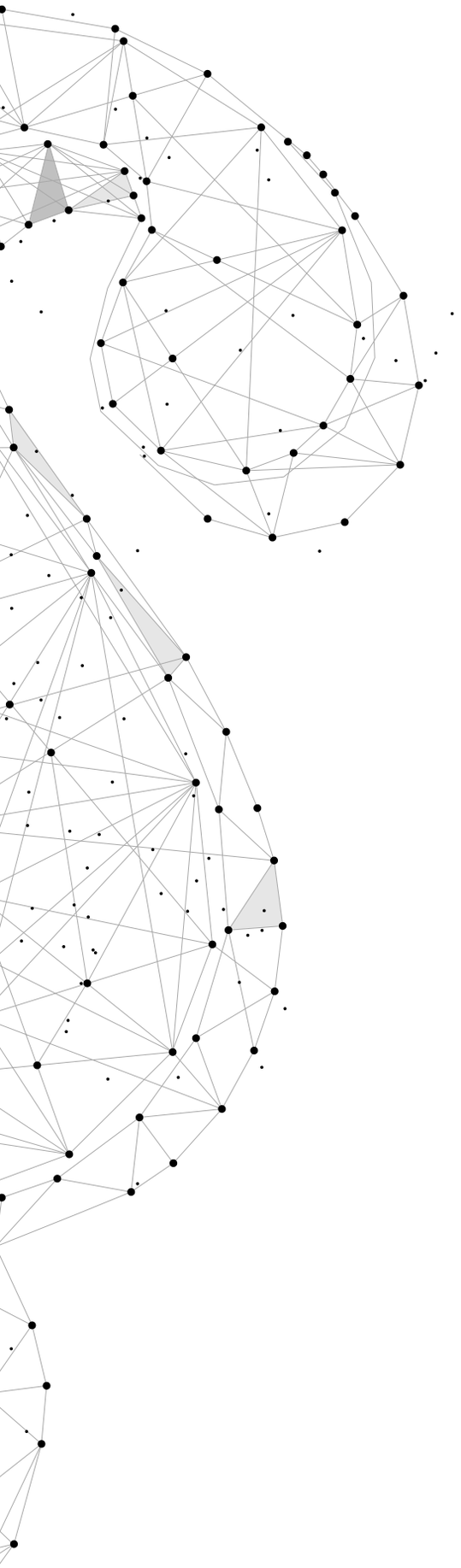
Úrad pri vybavovaní oznámení o protispoločenskej činnosti postupuje podľa zákona č. 54/2019 o ochrane oznamovateľov protispoločenskej činnosti a vnútorného systému vybavovania oznámení podľa nariadenia riaditeľa Národného bezpečnostného úradu č. 8/2024.

V rámci úradu sú nastavené vnútorné systémy oznamovania a vzdelávania príslušníkov úradu, 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.

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 tri novelizácie **zákona o ochrane utajovaných skutočností:**

- zákonom č. 161/2024, ktorým sa mení a dopĺňa zákon č. 143/1998o civilnom letectve (letecký zákon), prostredníctvom ktorého sa doplnilo nové ustanovenie o zákaze činnosti bezpilotného lietadla (§ 64a) s účinnosťou od 15.07.2024.

- zákonom č. 166/2024 o niektorých opatreniach na zlepšenie bezpečnostnej situácie v Slovenskej republike, prostredníctvom ktorého sa precizovali ustanovenia skutkových podstát priestupkov a správnych deliktov (§ 78 a § 79) s účinnosťou od 15.07.2024.

- zákonom č. 367/2024 o kritickej infraštruktúre, prostredníctvom ktorého sa doplnilo nové ustanovenie upravujúce inštitút limitovanej informácie (§ 3a) s účinnosťou od 01.01.2025.

Úrad kontinuálne pripravoval **návrh novej vyhlášky Národného bezpečnostného úradu o skúške bezpečnostného zamestnanca.** Hlavným cieľom návrhu vyhlášky je zosúladiť právny stav upravujúci agendu bezpečnostných zamestnancov s požiadavkami na elektronický výkon štátnej správy. Zároveň sa návrhom vyhlášky reaguje na nevyhovujúci stav bezpečnostného povedomia na úseku ochrany utajovaných skutočností, spôsobený zvýšenou fluktuáciou a generačnou obmenou na príslušných pracovných pozíciách.

S cieľom implementovať nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES v platnom znení (ďalej len „nariadenie (EÚ) č. 910/2014“) do národného právneho poriadku, vypracoval úrad návrh zákona, ktorým sa mení a dopĺňa zákon č. 272/2016 v znení zákona č. 211/2019 a ktorým sa mení zákon č. 305/2013 o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente) v znení neskorších predpisov.

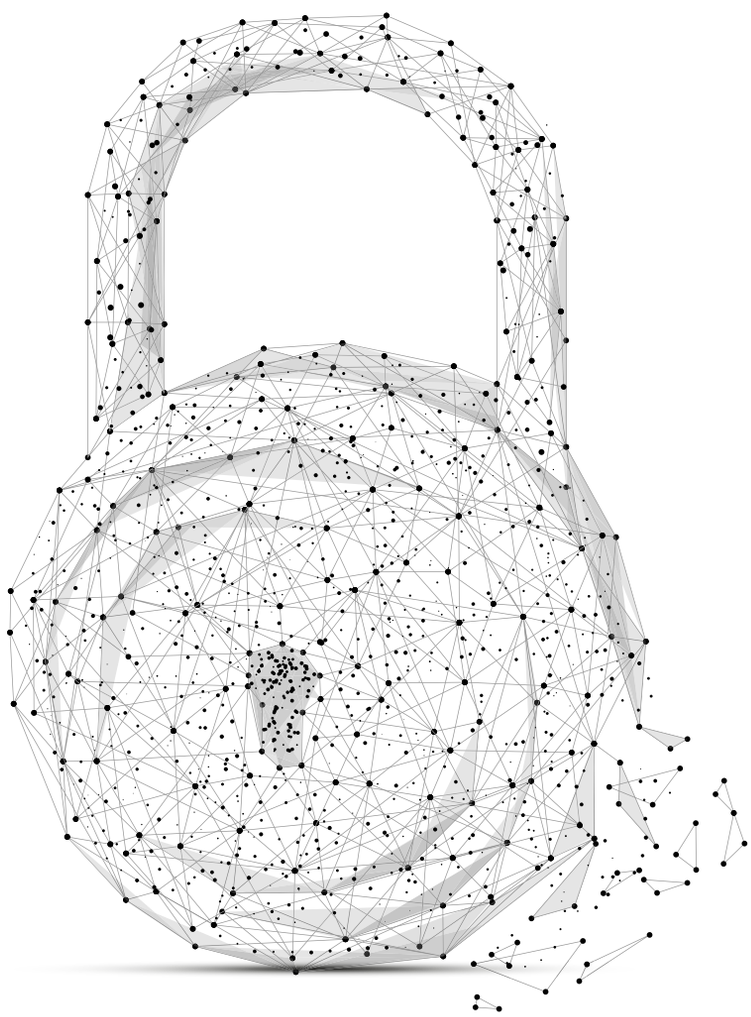
Novelou zákona o dôveryhodných službách sa okrem iného upravujú možnosti ako sa stať poskytovateľom európskej peňaženky digitálnej identity a upravuje sa postavenie a právomoci úradu pri výkone kontroly v súvislosti s európskou peňaženkou digitálnej identity. Ďalej sa upravujú aj úlohy Ministerstva vnútra Slovenskej republiky, ktoré je vlastníkom databáz totožností. Novela zákona o dôveryhodných službách nadobudla účinnosť 01.01.2025

S cieľom 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 NIS2) do národného právneho poriadku, úrad pripravil návrh zákona, ktorým sa mení a dopĺňa zákon č. 69/2018 o kybernetickej bezpečnosti.

Príprave **novely zákona o kybernetickej bezpečnosti** predchádzalo organizovanie odborných aktivít - workshopov, konferencií, stretnutí pracovných skupín, konzultácií s akademickou obcou i odbornou verejnosťou na národnej aj medzinárodnej úrovniUpravuje a precizuje sa ňou hlásenie incidentov, a hlásenie zraniteľností, zavádza sa minimálna úroveň bezpečnostných opatrení, posilňuje sa dohľadová činnosť, podporuje sa vzdelávanie, dopĺňa sa zodpovednosť a posilňuje sa funkcia manažéra kybernetickej bezpečnosti. Novela zákona o kybernetickej bezpečnosti nadobudla účinnosť 1. januára 2025.

Na zabezpečenie ochrany, odolnosti a posilnenie bezpečnosti subjektov ponúkajúcich služby v dôležitých sektoroch členských štátov Európskej únie boli okrem smernice NIS2 prijaté aj nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554 zo 14. decembra 2022 o digitálnej prevádzkovej odolnosti finančného sektora a o zmene a nariadení (ES) č. 1060/2009, (EÚ) č. 648/2012, (EÚ) č. 600/2014, (EÚ) č. 909/2014 a (EÚ) 2016/1011 a smernica Európskeho parlamentu a Rady (EÚ) 2022/2557 zo 14. decembra 2022 o odolnosti kritických subjektov a o zrušení smernice Rady 2008/114/ES. S cieľom zosúladiť národný právny rámec v oblasti kybernetickej bezpečnosti úrad v rámci harmonizácie s únijným právom aktívne participoval na implementácii a transpozícii predmetných právnych predpisov.

Okrem uvedených úloh na úseku legislatívy úrad pripomienkuje a vypracúva stanoviská k návrhom legislatívnych a nelegislatívnych materiálov v rámci **medzirezortného pripomienkového konania**. Celkovo úrad posúdil a vyhodnotil 581 materiálov v pripomienkových konaniach, čo predstavuje medziročný pokles o 119 materiálov.



SPRÁVNE A PRIESTUPKOVÉ KONANIE

NBÚ v roku 2024 evidoval 15 podaní vo veci podozrenia z priestupku na úseku ochrany utajovaných skutočností.

Z toho desať podaní bolo formou záznamu odložených, jedno podanie bolo odovzdané príslušnému orgánu, dve podania boli formou správy o výsledku objasňovania priestupku po zistení páchateľa priestupku predložené príslušnému správnemu orgánu a jedno podanie bolo odovzdané na ďalšie konanie z dôvodu, že objasňovaný skutok nebol priestupkom, ale správnym deliktom.

Úrad uložil pokuty za spáchanie priestupku na úseku ochrany utajovaných skutočností v súhrnnej sume 300 eur a za spáchanie správneho deliktu na úseku kybernetickej bezpečnosti v sume 33 300 eur.

Sekcia kontroly a bezpečnosti v roku 2024 zaevidovala 13 oznámení o neoprávnenej manipulácii s utajovanou skutočnosťou, pričom 12 oznámení bolo objasňovaných v režime zákona č. 372/1990 o priestupkoch a jedným oznámením sa zaoberal orgán činný v trestnom konaní.

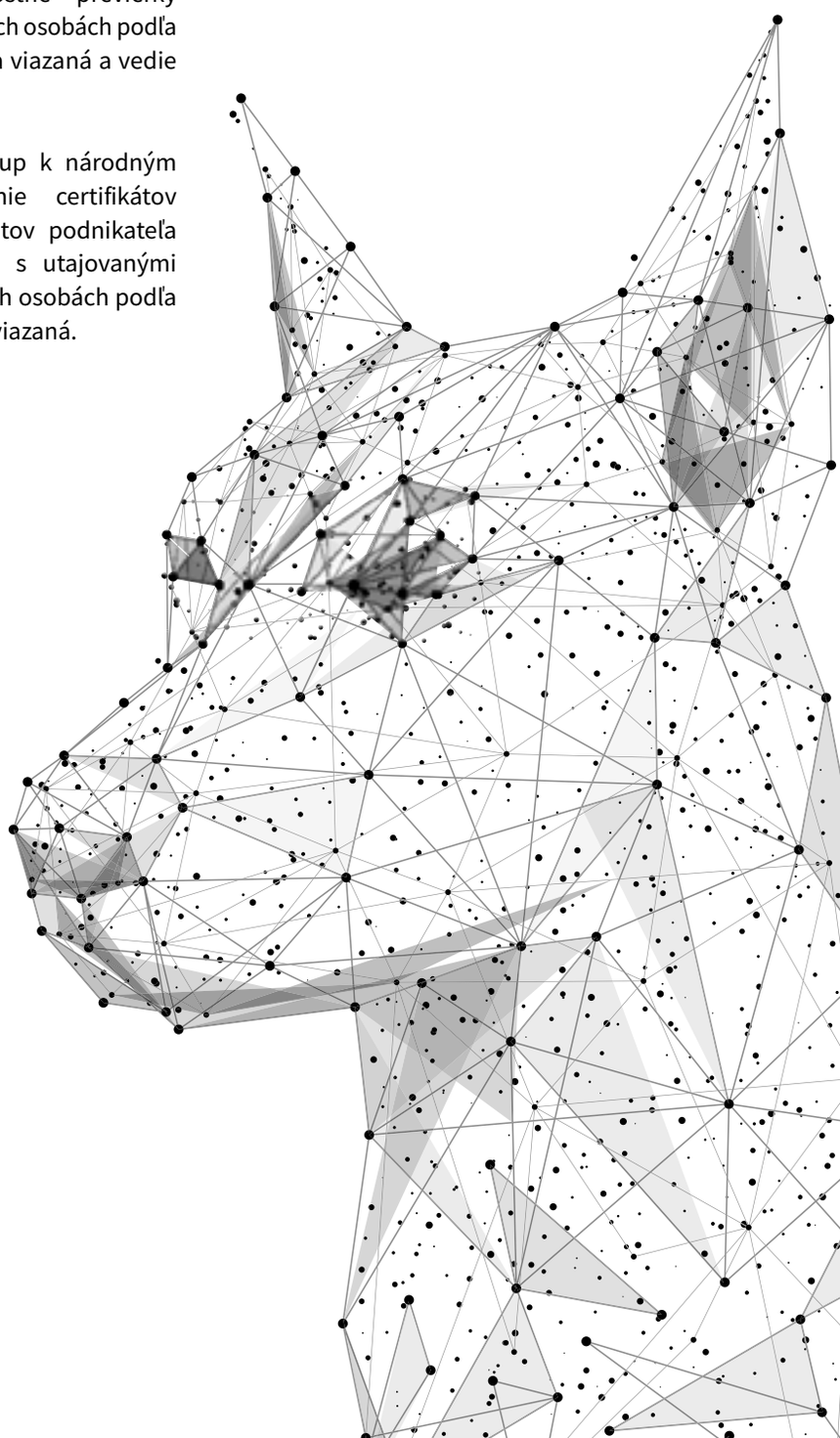
ZMLUVY O POSTUPOVANÍ UTAJOVANÝCH SKUTOČNOSTÍ

Úrad má celkovo uzatvorených 17 zmlúv o prístupe podnikateľa k utajovaným skutočnostiam, vlani uzatvoril 8 zmlúv a 5 dodatkov k uzatvoreným zmluvám.

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.

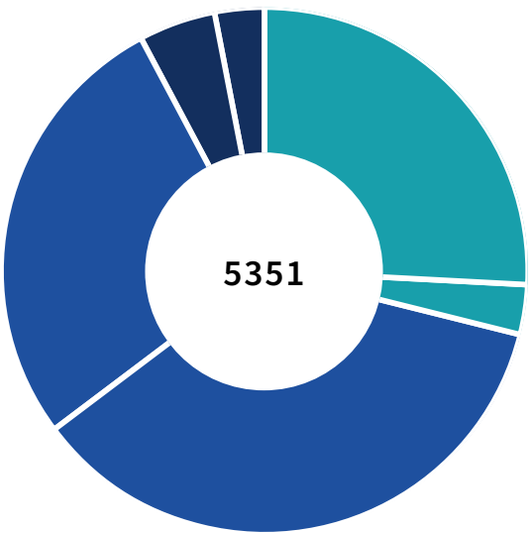


PERSONÁLNA BEZPEČNOSŤ

Národný bezpečnostný úrad vydal **5 351 osvedčení** na oboznamovanie sa s utajovanými skutočnosťami, **z toho 2 710 pre rezort obrany**.

Prehľad osvedčení vydaných v roku 2024

Stupeň utajenia	2024
DÔVERNÉ	**2087**
z toho Dôverné pre MO SR	248
TAJNÉ	**2889**
z toho Tajné pre MO SR	2225
PRÍSNE TAJNÉ	**375**
z toho Prísne tajné pre MO SR	237
Spolu	**5351**



NBÚ vydal 20 rozhodnutí. Proti rozhodnutiu úradu podali fyzické osoby 11 odvolaní. Jedno odvolanie nebolo úradom akceptované, o dvoch odvolaniach úrad rozhodol autoremedúrou.

Výbor Národnej rady Slovenskej republiky na preskúmanie rozhodnutí Národného bezpečnostného úradu rozhodol o šiestich odvolaniach, tri odvolania zamietol, dve rozhodnutia úradu zrušil v odvolacom konaní a jedno odvolanie rozhodol inak.

Na Najvyšší správny súd SR boli podané dve správne žaloby. Najvyšší správny súd rozhodol v roku 2024 o štyroch správnych žalobách, ktoré zamietol.

Na Ústavný súd SR nebola podaná žiadna ústavná sťažnosť. V roku 2024 Ústavný súd jednu ústavnú sťažnosť odmietol a jedno rozhodnutie Najvyšší správny súd zrušil.

Navrhovaným osobám bolo v roku 2024 vydaných **6 968 certifikátov o bezpečnostnej previerke fyzickej osoby - z toho 3 367 certifikátov NATO a 3 601 certifikátov EÚ**. Z celkového počtu certifikátov NATO **úrad vydal 31 certifikátov NATO ATOMAL**, ktoré oprávňujú na prístup k informáciám o strategickom jadrovom odstrašovaní NATO a vydávajú sa úzkemu okruhu osôb.

PRIEMYSELNÁ BEZPEČNOSŤ

V roku 2024 vydal úrad 137 potvrdení o priemyselnej bezpečnosti – z toho šesť potvrdení stupňa utajenia Vyhradené, 103 potvrdení stupňa utajenia Dôverné, 26 potvrdení stupňa utajenia Tajné a dve potvrdenie stupňa utajenia Prísne tajné.

V roku 2024 úrad vydal 16 rozhodnutí. Proti rozhodnutiu úradu podali podnikatelia štyri odvolania.

Na Najvyššom správnom súde Slovenskej republiky nebola v roku 2024 podaná žiadna žaloba a ani nezrušil žiadne rozhodnutie.

Na Ústavnom súde Slovenskej republiky bola podaná jedna ústavná sťažnosť a súd rozhodol jednu vec.

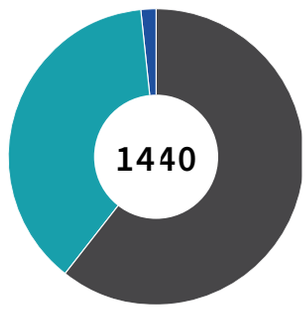
Vo vzťahu k utajovaným skutočnostiam NATO a EÚ bolo v roku 2024 podnikateľom vydaných **23 certifikátov NATO a 26 certifikátov EÚ**, ktoré oprávňujú podnikateľov oboznamovať sa s utajovanými skutočnosťami NATO a/alebo EÚ.

VÝMENA UTAJOVANÝCH SKUTOČNOSTÍ

V roku 2024 úrad prijal a odoslal 1 440 utajovaných skutočností – interná distribúcia medzi útvarmi sa do tejto hodnoty nepočíta. Od roku 2022 umožňuje elektronický informačný systém pre správu registratúry vytvárať utajované skutočnosti stupňa utajenia Vyhradené aj obsahovo. V roku 2024 prešiel Fabasoft na novú verziu, a to z verzie 2016 na verziu 2023.

Stupne utajenia utajovaných skutočností

Stupeň utajenia	2024
VYHRADENÉ	875
DÔVERNÉ	544
TAJNÉ	21
PRÍSNE TAJNÉ	0
Spolu	1440



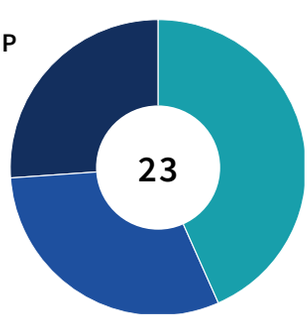
FYZICKÁ BEZPEČNOSŤ A OBJEKTOVÁ BEZPEČNOSŤ

Za rok 2024 vydal úrad **40 certifikátov** mechanických zábranných (MZP) a technických zabezpečovacích prostriedkov (TZP).

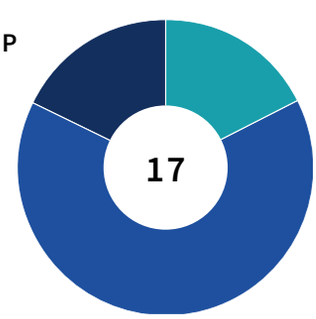
Stupne utajenia vydaných certifikátov

Stupeň utajenia	MZP	TZP	MZP a TZP
VYHRADENÉ	0	0	0
DÔVERNÉ	10	3	13
TAJNÉ	7	11	18
PRÍSNE TAJNÉ	6	3	9
Spolu	23	17	40

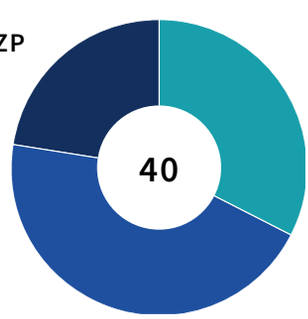
MZP



TZP



MZP a TZP

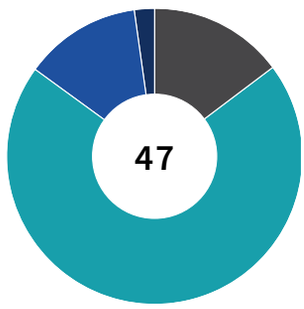


BEZPEČNOSŤ TECHNICKÝCH PROSTRIEDKOV

Za rok 2024 úrad vydal **47 certifikátov** technických prostriedkov (TP) a **23 dodatkov k už vydaným certifikátom** technických prostriedkov.

Stupne utajenia vydaných certifikátov

Stupeň utajenia	TP
VYHRADENÉ	7
DÔVERNÉ	33
TAJNÉ	6
PRÍSNE TAJNÉ	1
Spolu	47



AKREDITÁCIA KOMUNIKAČNÝCH A INFORMAČNÝCH SYSTÉMOV

V roku 2024 úrad vykonal osem akreditácií 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 (NEV) vykonávala v roku 2024 sekcia akreditácie a certifikácie merania NEV zariadení technických prostriedkov a prostriedkov šifrovej ochrany informácií (v TEMPEST laboratóriu), ako aj zónové merania chránených priestorov (mobilnou meracou aparatúrou).

K 31.12.2024 bolo prijatých 29 žiadostí (jedna žiadosť môže obsahovať viacero požiadaviek o stanovisko k certifikácii TP, vykonanie meraní NEV zariadení TP a o vykonanie zónových meraní priestorov), z ktorých bolo vybavených 29. V priebehu posudzovaného obdobia boli vykonané merania NEV desiatich zostáv zariadení (TP a prostriedkov šifrovej ochrany informácií) v Národnom laboratóriu TEMPEST.

V rámci doručených žiadostí bolo vykonaných 32 zónových meraní priestorov, na základe ktorých bolo kategorizovaných 28 miestností.

BEZPEČNOSTNÉ POVEDOMIE

Úrad na úseku budovania bezpečnostného povedomia vypracoval **Plán vzdelávacích aktivít na rok 2024** (ďalej len „plán“), ktorý bol počas celého roka zverejnený na webovom sídle úradu, a podľa ktorého aj na pravidelnej mesačnej báze vykonával školiacu činnosť v prezenčnej forme. Plán bol vypracovaný na základe požiadaviek a spätnej väzby odbornej verejnosti (pozostávajúcej z orgánov štátnej správy a podnikateľov), získanej prostredníctvom anonymizovaných dotazníkov z každej aktivity a na základe vlastnej kontrolnej činnosti úradu. S ohľadom na uvedené skutočnosti bolo v Bratislave vykonaných 13 prednášok v spolupráci s Inštitútom pre verejnú správu. V Košiciach bol v septembri 2024 venovaný celý jeden týždeň problematike ochrany utajovaných skutočností a jednotlivým oblastiam bezpečnosti. Školení sa zúčastnilo celkom 740 účastníkov.

Zároveň úrad na svojom webovom sídle, s cieľom zvýšenia bezpečnostného povedomia, publikoval jednotlivé prezentácie, ktoré priebežne aktualizoval podľa potrieb. Okrem týchto prezentácií je zverejnená aj samovzdelávacia prezentácia zameraná na konkrétnu aplikáciu vykonávacieho predpisu v oblasti administratívnej bezpečnosti.

Ďalším efektívnym nástrojom v tejto oblasti je, v súlade s vykonávacím predpisom, uskutočňovanie overovania získaných vedomostí bezpečnostných zamestnancov (taký zamestnanec osobitného pracoviska alebo iný zamestnanec, ktorý je štatutárom poverený na plnenie úloh na úseku ochrany utajovaných skutočností) prostredníctvom skúšok bezpečnostného zamestnanca a preškolenia bezpečnostných zamestnancov.

Pre uvedený účel bol v rámci projektu „Elektronické služby spracovania bezpečnostných spisov NBÚ – malé zlepšenie eGov služieb“ vytvorený a 15.05.2024 spustený Verejný portál Agenda Bezpečnostní zamestnanci, ktorý zaviedol plne elektronické služby pre agendu súvisiacu s bezpečnostnými zamestnancami s cieľom stať sa na tento účel výlučnou komunikačnou platformou úradu. Ide najmä o podávanie žiadosti o vykonanie skúšky alebo preškolenia bezpečnostných zamestnancov a zasielanie oznámenia o poverení bezpečnostného zamestnanca, zmene takéhoto poverenia alebo zániku poverenia. Táto elektronická služba umožňuje orgánu verejnej moci, podnikateľovi alebo fyzickej osobe vyplniť elektronický formulár, elektronicky ho autorizovať a následne odoslať na ďalšie spracovanie. Skúška a preškolenie bezpečnostných zamestnancov sa v roku 2024 vykonávala formou online testu najmä vo webovej aplikácii a cez agendový systém Bezpečnostní zamestnanci, pričom komunikácia prebieha vo virtuálnej video-konferenčnej miestnosti.

Na skúšku bezpečnostného zamestnanca bolo v roku 2024 pozvaných celkovo 635 uchádzačov, z ktorých úspešne absolvovalo skúšku 430 (z nich 342 vykonal úrad a 88 Ministerstvo vnútra SR na základe Vykonávacieho protokolu o vzájomnej spolupráci pri výkone skúšok bezpečnostného zamestnanca a preškoľovania). Neúspešných bolo 86 uchádzačov (z nich 76 vykonal úrad a desať Ministerstvo vnútra SR). Zostávajúci počet uchádzačov sa skúšky nezúčastnil. O preškolenie bezpečnostného zamestnanca požiadalo celkovo 226 uchádzačov, z ktorých úspešne absolvovalo preškolenie 213 (z nich 190 vykonal úrad a 23 Ministerstvo vnútra SR) a jeden uchádzač bol neúspešný. Zostávajúci počet uchádzačov sa preškolenia nezúčastnil. Úrad v roku 2024 vybavil všetky žiadosti o skúšku a preškolenie bezpečnostného zamestnanca. Ďalej boli na žiadosť držiteľa potvrdenia o úspešnom vykonaní skúšky bezpečnostného zamestnanca vydané štyri nové potvrdenia o absolvovaní skúšky (tzv. „duplikát“).

ŠIFROVÁ OCHRANA INFORMÁCIÍ

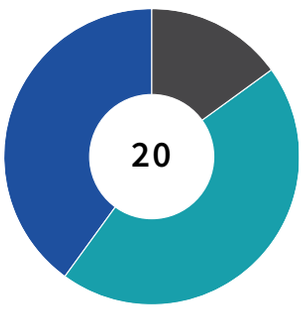
CERTIFIKÁCIA

Systém šifrovej ochrany je v Slovenskej republike založený na overenej štruktúre rezortných šifrových orgánov a ich úzkej spolupráci s úradom, ktorý plní rolu ústredného šifrového orgánu. Predmetom komunikácie v roku 2024 boli najmä oblasti certifikácie prostriedkov šifrovej ochrany informácií (PŠOI), vydávanie dodatkov k pravidlám na používanie prostriedkov šifrovej ochrany informácií a otázky ohľadom možností uznávania a preberania zahraničných certifikátov.

Za rok 2024 úrad vydal 20 certifikátov prostriedkov šifrovej ochrany informácií a dva dodatky k už vydaným certifikátom PŠOI.

Stupne utajenia vydaných certifikátov

Stupeň utajenia	TP
VYHRADENÉ	3
DÔVERNÉ	9
TAJNÉ	8
PRÍSNE TAJNÉ	0
Spolu	20



NÁRODNÁ DISTRIBUČNÁ AUTORITA

V roku 2024 pokračovala Národná distribučná autorita v štandardných evidenčných a distribučných činnostiach. Bol zaznamenaný mierny pokles evidovaných a distribuovaných materiálov v oblasti národných prostriedkov šifrovej ochranyinformácií, ktorý je spojený s menším množstvom nákupov nových prostriedkov na všetkých sledovaných rezortoch.

V oblasti výmeny elektronických kľúčov NATO došlo k značnému posunu vzhľadom na úspešný prechod na systém Key Management Infrastructure (KMI), ktorý v júni 2024 nahradil zastaraný systém DACAN Electronic key management system (DEKMS). Prechod na nový systém ďalej rozšíril množstvo možných zasielaných materiálov o softvérové balíčky, návody, manuály a certifikáty, ktoré budú potrebné z dôvodov nasadenia nových obranných systémov a zariadení v gescii Ministerstva obrany SR.

Počty transakcií a kusov šifrového materiálu k 31.12.2024

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

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. Prostredníctvom európskej peňaženky digitálnej identity tak užívateľ získa svoje potvrdenie (elektronické osvedčenie atribútov) a z potvrdení vie zaslať spoliehajúcej sa strane len nevyhnutné údaje.

K európskej peňaženke digitálnej identity boli vydané implementačné akty:

- Vykonávacie nariadenie Komisie (EÚ) 2024/2977 z 28. novembra 2024, ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014, pokiaľ ide o osobné identifikačné údaje a elektronické osvedčenia atribútov vydané pre európske peňaženky digitálnej identity

- Vykonávacie nariadenie Komisie (EÚ) 2024/2979 z 28. novembra 2024, ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014, pokiaľ ide o integritu a základné funkcie európskych peňaženiek digitálnej identity

- Vykonávacie nariadenie Komisie (EÚ) 2024/2980 z 28. novembra 2024, ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014, pokiaľ ide o oznámenia Komisii týkajúce sa ekosystému európskej peňaženky digitálnej identity

- Vykonávacie nariadenie Komisie (EÚ) 2024/2981 z 28. novembra 2024, ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014, pokiaľ ide o certifikáciu európskych peňaženiek digitálnej identity

- Vykonávacie nariadenie Komisie (EÚ) 2024/2982 z 28. novembra 2024, ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014, pokiaľ ide o protokoly a rozhrania, ktoré má podporovať európsky rámec digitálnej identity

Členské štáty majú povinnosť do dvoch rokov od vydania implementačných aktov vydať európsku peňaženku digitálnej identity občanom, ak o ňu požiadajú.

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 2024 úrad publikoval dôveryhodné zoznamy č. 114 až 120.

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 roku 2024 bolo na základe žiadostí štátnych orgánov a orgánov územnej samosprávy do zoznamu zapísaných 12 nových oprávnení a dvakrát boli aktualizované existujúce oprávnenia. V priebehu roka úrad publikoval deväť verzií zoznamu oprávnení. Jeho aktuálna verzia bola vždy doplnená archívom predchádzajúcich verzií.

NOVÉ DÔVERYHODNÉ SLUŽBY

Úrad vydal dve rozhodnutia o udelení kvalifikovaného štatútu na kvalifikovanú dôveryhodnú službu - kvalifikovaná dôveryhodná služba validácie kvalifikovaných elektronických podpisov a kvalifikovaná dôveryhodná služba validácie kvalifikovaných elektronických pečatí. V rámci procesu udelenia týchto kvalifikovaných štatútov bola vykonaná aj analýza správy o posúdení zhody od kvalifikovaného poskytovateľa týchto kvalifikovaných dôveryhodných služieb. Úrad vykonal posúdenie 13 zmien v poskytovaní kvalifikovanej dôveryhodnej služby, z čoho desať zmien bolo akceptovaných a pri troch zmenách bolo poskytovateľovi oznámené, aby požiadal o kvalifikovaný štatút.

TVORBA MEDZINÁRODNÝCH NORIEM

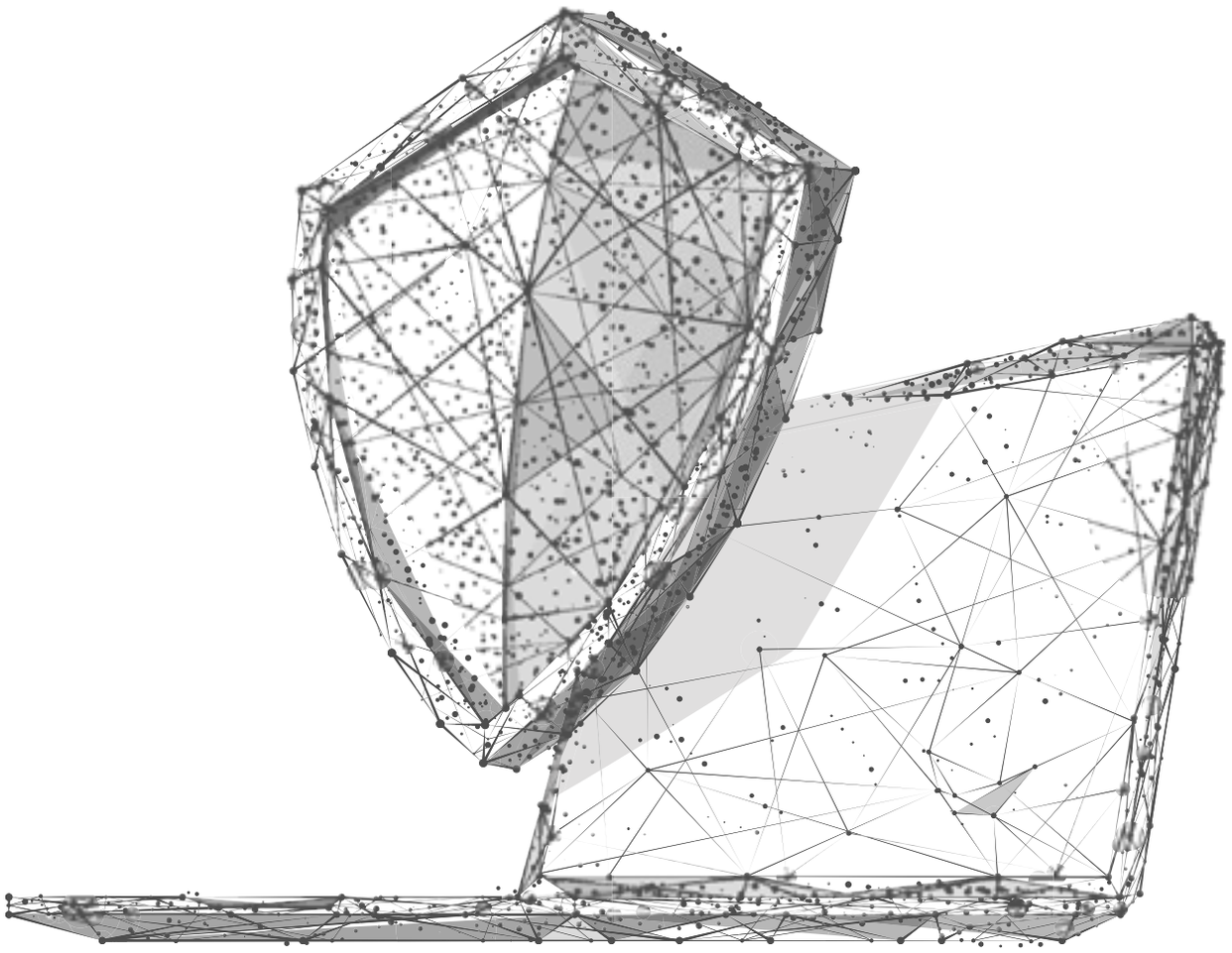
Pri tvorbe medzinárodných technických noriem použiteľných pre implementáciu nariadením EÚ č. 910/2014 je príslušník úradu súčasťou expertných skupín Európskej komisie, analyzujúcich riešenia, ktoré sú základom prípravy implementačných aktov k peňaženke digitálnej identity. Ako člen medzinárodných štandardizačných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

CERTIFIKÁCIA

V roku 2024 nedostala sekcia akreditácie a certifikácie žiadnu žiadosť o certifikáciu bezpečného produktu pre kvalifikovaný elektronický podpis. Kvalifikovaní poskytovatelia dôveryhodných služieb využívajú zariadenia na vyhotovenie kvalifikovaného elektronického podpisu alebo zariadenia na vyhotovenie kvalifikovanej elektronickej pečate už certifikované v inej krajine Európskej únie, ktoré sú zverejnené v zozname zariadení certifikovaných Európskou úniou. V roku 2024 boli vydané dve rozhodnutia o udelení kvalifikovaného štatútu na kvalifikovanú dôveryhodnú službu - kvalifikovaná dôveryhodná služba validácie kvalifikovaných elektronických podpisov a kvalifikovaná dôveryhodná služba validácie kvalifikovaných elektronických pečatí. V rámci procesu udelenia týchto kvalifikovaných štatútov bola vykonaná aj analýza správy o posúdení zhody. Taktiež boli posúdené tri správy o posúdení zhody z kontrolného auditu od dvoch kvalifikovaných poskytovateľov dôveryhodných služieb a za uvedené obdobie bol úrad požiadaný o vykonanie 13 zmien v poskytovaní kvalifikovanej dôveryhodnej služby, z čoho desať zmien bolo akceptovaných a pri troch zmenách bolo poskytovateľovi oznámené, aby požiadal o kvalifikovaný štatút.

DÔVERYHODNÁ INFRAŠTRUKTÚRA

Úrad v roku 2024 prevádzkoval v dôvernej infraštruktúre Koreňovú certifikačnú autoritu Slovenskej republiky, ktorá vydávala certifikáty verejných kľúčov a vedie dlhodobú databázu vydaných kvalifikovaných certifikátov s ich stavom platnosti, vydanými poskytovateľmi, ktorým úrad udelil kvalifikovaný štatút. Za rok 2024 odbor prevádzky IKT eviduje celkovo 160 040 certifikátov.



KYBERNETICKÁ BEZPEČNOSŤ

Národný bezpečnostný úrad prostredníctvom Národného centra kybernetickej bezpečnosti (NCKB) naďalej rozvíja svoje spôsobilosti pri zabezpečovaní otvoreného, bezpečného a chráneného národného kybernetického priestoru. Z tejto pozície úrad zabezpečuje služby spojené s riadením bezpečnostných incidentov, odstraňovaním ich následkov a následnou obnovou činnosti informačných systémov v spolupráci s vlastníkmi a prevádzkovateľmi týchto systémov.

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, vykonávadohľad a koordinuje ich riešenie. Zdrojom údajov pri riešení a koordinácii kybernetických bezpečnostných incidentov je vlastná detekcia, povinné a dobrovoľné hlásenia prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb

a informácie od partnerov a partnerských organizácií. NCKB zároveň distribuuje varovania a bezpečnostné bulletiny a zvyšuje tým úroveň prevencie.

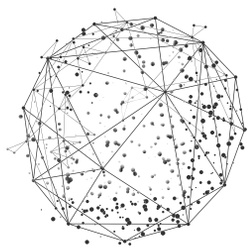
Činnosť NCKB sa na operatívnej úrovni v roku 2024 zameriavala najmä na aktivity súvisiace s kybernetickou bezpečnosťou prevádzkovateľov základných služieb (PZS) vrátane prvkov kritickej infraštruktúry. Okrem tvorby varovaní úrad zdieľal relevantné informácie s partnermi na základe medzinárodnej spolupráce a vlastnej činnosti, vyplývajúcej z analýzy hlásených a zaznamenaných incidentov.

NCKB kontinuálne rozvíja 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 sú v rámci NCKB vytvárané kvartálne reporty o kyberbezpečnostnej situácii v slovenskom kybernetickom priestore.

Počet hlásených kybernetických bezpečnostných incidentov

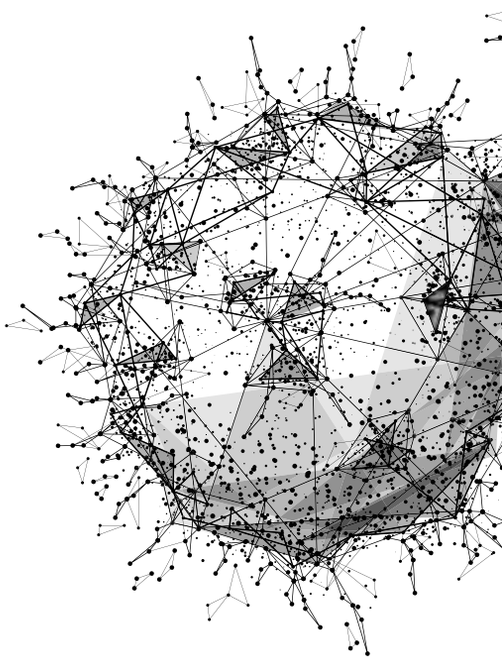
	Jan	Feb	Mar	Apr	Máj	Jún	Júl	Aug	Sep	Okt	Nov	Dec
Bankovníctvo	4	2	2	6	6	5	1	3	2	4	6	3
Doprava	2	3	0	3	0	1	1	0	0	2	1	1
Digitálna infraštruktúra	0	0	1	0	1	1	3	3	0	0	1	1
Elektronické komunikácie	0	0	0	1	0	0	1	0	0	3	0	0
Energetika	2	0	0	0	1	1	0	1	1	1	3	0
Infraštruktúra finančných trhov	0	0	0	0	0	0	0	0	0	0	0	0
Pošta	0	2	3	1	0	1	1	0	0	2	2	0
Priemysel	1	0	0	0	0	0	0	0	0	0	0	0
Voda a atmosféra	0	0	0	0	0	0	0	0	0	0	0	0
Verejná správa	24	45	48	63	52	61	58	57	74	84	71	66
Zdravotníctvo	5	5	3	2	9	17	4	6	3	6	0	2
Iné	37	20	25	27	23	31	31	21	21	17	32	32
CELKOM	**75**	**77**	**82**	**103**	**92**	**118**	**100**	**91**	**101**	**119**	**116**	**57**

NBÚ evidoval v roku 2024 celkovo 1 179 hlásení o kybernetických bezpečnostných incidentoch:



- 17 hlásení o závažných kybernetických bezpečnostných incidentoch I. stupňa
- 6 hlásenia o závažných kybernetických bezpečnostných incidentoch
- 1 hlásenie o závažných kybernetických bezpečnostných incidentoch III. stupňa
- 1155 dobrovoľných hlásení

Dominovali nasledujúce technické typy útokov: získavanie informácií (600), nedostupnosť (80), pokus o prienik (73), škodlivý kód (49) a zraniteľnosť (64). Väčšina hlásení pochádzala z dobrovoľných hlásení, ktoré prevládali nad povinnými kategorizovanými hláseniami.



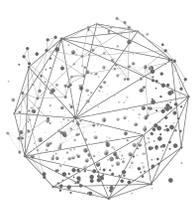
Pri dôvodoch nehlásenia bola najčastejšie pozorovaná neznalosť právnych noriem – subjekty nevedeli, že majú povinnosť hlásenia. S prichádzajúcou novelou zákona v nadväznosti na NIS2, ktorá nadobudla účinnosť 01. 01. 2025 je možné v ďalších rokoch očakávať nárast hlásení, nakoľko novela rozšíri pôsobnosť na ďalšie subjekty.

Najviac incidentov bolo nahlásených v sektore verejná správa (703).

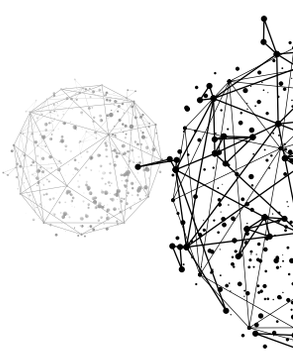
V roku 2024 bol phishing naďalej najrozšírenejšou a najúspešnejšou metódou získavania citlivých údajov a šírenia škodlivého obsahu. Pri phishingu naďalej prevládali impersonácie, resp. kampane zneužívajúce identitu vládnych inštitúcií.

Častým dôvodom prieniku do systému je kompromitácia e-mailovej schránky ako následok phishingu, alebo cez brute force útok na nezabezpečený prihlasovací web mailserveru a pod.

Trendy v získavaní citlivých informácií sa v porovnaní s predchádzajúcimi rokmi príliš nelíšili a prevládali nasledujúce tematiky:



- Phishingová kampaň zneužívajúca identitu Ministerstvo financií SR s tematikou vrátenia daní
- Phishingová kampaň zneužívajúca identitu Všeobecnej zdravotnej poisťovne
- Rozsiahla phishingová kampaň rozposielaná z kompromitovaných slovenských a českých e-mailových účtov, ktorej cieľom bolo získanie prihlasovacích a citlivých údajov
- Phishingová kampaň zneužívajúca identitu slovensko.sk tematicky zameraná na vrátenie daní a platbu pokút. Cieľom bolo získanie citlivých a bankových údajov



V roku 2024 sme boli svedkami výrazného nárastu sofistikovanosti phishingových útokov, najmä vďaka integrácii umelej inteligencie (AI) do arzenálu kybernetických zločincov. Nedávne štúdie a incidenty poukazujú na to, že AI umožňuje útočníkom vytvárať mimoriadne presvedčivé a personalizované phishingové kampane, ktoré sú ťažko odhaliteľné aj pre skúsených používateľov.

Ďalej bol v tomto roku pozorovaný výrazný nárast prípadov anonymných bombových vyhrážok. V treťom kvartáli 2024 došlo k niekoľkým zásadným zmenám v oblasti nahlasovania bombových hrozieb na Slovensku, ktoré výrazne ovplyvnili postupy a reakcie bezpečnostných zložiek štátu.

Bombové hrozby začali zasahovať aj letiská, jadrové elektrárne, verejné budovy samospráv, cirkevné objekty a miesta s vysokou koncentráciou ľudí. Tento posun poukazuje na zmenu taktiky zo strany útočníkov, ktorí cielia na širší okruh kritickej infraštruktúry s cieľom zvýšiť chaos a narušiť chod viacerých sektorov. Tento vývoj kladie vysoké nároky na bezpečnostné zložky, ktoré musia flexibilne reagovať na rôznorodé typy cieľov a zabezpečiť optimálnu koordináciu medzi viacerými orgánmi.

Ministerstvo školstva a ministerstvo vnútra na tieto hrozby reagovali vydaním manuálov a grafických vyhotovení pre školy a verejné inštitúcie, ktoré obsahujú postupy, ako reagovať na bombové hrozby. Tieto materiály slúžia ako praktické návody, pričom súčasťou je aj detailný popis postupov pri evakuácii, komunikácii s príslušnými orgánmi a prevencii paniky.

Aj v tomto roku pokračovali distribuované útoky odmietnutia služby (DDoS) na kritickú infraštruktúru a bankový sektor, ktoré viedli k nedostupnosti elektronického bankovníctva.

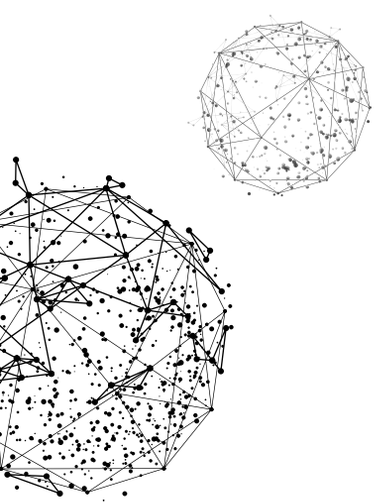
Národné centrum kybernetickej bezpečnosti vydávalo bezpečnostné odporúčania a varovania pred zraniteľnosťami a hrozbami – 51 súhrnných bezpečnostných bulletinov a 701 bezpečnostných varovaní. Upozornilo na 1 493 zraniteľností a hrozieb.

CYBERGAME

V treťom ročníku národnej kyberbezpečnostnej súťaže CyberGame sa registrovalo vyše 2 300 účastníkov. Počas desiatich týždňov riešili úlohy rôzneho zamerania, ktoré pripravili kolegovia z Národného centra kybernetickej bezpečnosti.

V roku 2024 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. Novinkou bola ofenzívna bezpečnosť.

CyberGame predstavuje atraktívny a netradičný spôsob, ako hľadať a nadchnúť profesionálov pre kybernetickú bezpečnosť. V súťaži bodovalo 874 hráčov a hráčok, počínajúc prvákmi na strednej škole a končiac skúsenými programátormi. Každý dostal šancu, takže ocenenie bolo udelené absolútnemu víťazovi, najlepšiemu študentovi, najlepšej hráčke a organizátori odmenili aj najmladšieho účastníka, expertov vo vetvách, najlepšieho hráča z verejnej správy a učiteľa.



NÁRODNÁ AUTORITA PRE CERTIFIKÁCIU KYBERNETICKEJ BEZPEČNOSTI

Európsky parlament a Rada (EÚ) dávnejšie prijali nariadenie 2019/881 o Agentúre Európskej únie pre kybernetickú bezpečnosť (ENISA) a o certifikácii kybernetickej bezpečnosti IKT, nazývaný aj akt o kybernetickej bezpečnosti. Zavádza aj celoúnijný rámec certifikácie kybernetickej bezpečnosti IKT produktov, služieb a procesov, ktorá má zvýšiť ich dôveryhodnosť.

V zmysle zákona č. 69/2018 o kybernetickej bezpečnosti je NBÚ Národnou autoritou pre certifikáciu kybernetickej bezpečnosti (NCCA) a orgánom posudzovania zhody. Napríklad vypracúva národnú stratégiu kybernetickej bezpečnosti, spravuje a prevádzkuje jednotný informačný systém kybernetickú bezpečnosti a v systéme certifikácie vydáva bezpečnostné štandardy, certifikačné schémy a postupy.

Národným akreditačným orgánom je Slovenská národná akreditačná služba (SNAS), ktorá akredituje orgány posudzovania zhody. SNAS je poverená vykonávaním akreditácie zákonom č. 53/2023 o akreditácii orgánov posudzovania zhody.

Orgánom posudzovania zhody (CAB) je subjekt, ktorý vykonáva činnosti posudzovania zhody (certifikácia, skúšanie a pod.). CAB musí pre danú činnosť získať akreditáciu.

V prípade, že európska schéma certifikácie kybernetickej bezpečnosti stanoví dodatočné požiadavky na orgány posudzovania zhody, musia byť aj tieto požiadavky zo strany orgánu posudzovania zhody splnené. Splnenie týchto dodatočných požiadaviek je potvrdené vydaním autorizácie zo strany NCCA.

Rok 2024 bol bohatý na oblasť legislatívy týkajúcej sa certifikácie kybernetickej bezpečnosti:

- Do platnosti vstúpila prvá schéma certifikácie kybernetickej bezpečnosti, a to konkrétne dňa 31.01.2024 prijatím vykonávacieho nariadenia Komisie (EÚ) 2024/482, ktorým sa ustanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881, pokiaľ ide o prijatie európskej schémy certifikácie kybernetickej bezpečnosti založenej na spoločných kritériách (EUCC). Schéma EUCC 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).

- Európsky parlament a Rada (EÚ) prijali dňa 23. 10. 2024 nariadenie 2024/2847 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 - CRA). Nariadenie je účinné od **10.12.2024** a uplatňovať sa začne postupne v troch fázach. V prvej fáze, kapitoly IV a články 35 až 51, sa začne uplatňovať od **11.06.2026**. V druhej fáze sa začne uplatňovať článok 14 od **11.09.2026**. Posledná fáza uplatňovania sa začne **11.12.2027**. CRA sa bude uplatňovať na všetky produkty s digitálnymi prvkami, ktorých zamýšľané a odôvodnene predvídateľné použitie zahŕňa priame alebo nepriame logické alebo fyzické dátové pripojenie k zariadeniu alebo sieti.

- Koncom roka 2024 bolo vydané vykonávacie nariadenie Komisie (EÚ) 2024/3144 zo dňa 18.12.2024, ktorým sa zmenilo vykonávacie nariadenie (EÚ) 2024/482, pokiaľ ide o uplatniteľné medzinárodné normy a ktorým sa uvedené vykonávacie nariadenie v niektorých častiach opravilo.

- K aktu kybernetickej bezpečnosti bolo vydané vykonávacie nariadenie Komisie (EÚ) 2024/3143 zo dňa 18.12.2024, ktorým sa stanovujú okolnosti, formáty a postupy notifikácie.

- Zároveň bola k aktu o kybernetickej bezpečnosti dňa 19.12.2024 schválená ďalšia jeho novela, ktorou sa bude meniť uvedený akt týkajúci sa riadených bezpečnostných služieb. Konkrétne sa týmto novým nariadením má doplniť horizontálny regulačný rámec, ktorým sa stanovujú komplexné požiadavky na kybernetickú bezpečnosť pre produkty s digitálnymi prvkami podľa nariadenia Európskeho parlamentu a Rady (EÚ) 2024/2847, a to stanovením bezpečnostných cieľov na riadené bezpečnostné služby, ako aj uplatňovanie a dôveryhodnosť uvedených služieb.

V oblasti certifikácie sa pripravujú a sú rozpracované tieto štyri schémy certifikácie kybernetickej bezpečnosti:

Schéma EUCC

Prvým návrhom európskej schémy certifikácie kybernetickej bezpečnosti je schéma pre certifikáciu cloudových služieb (CS). 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 EU5G

Druhý návrh európskej schémy certifikácie kybernetickej bezpečnosti pokrýva oblasť 5G sietí. Návrh stavia na súbore opatrení pre kybernetickej bezpečnosť sietí 5G, pričom sa očakáva, že schéma pomôže tlmiť ďalšie riziká spojené s týmto ekosystémom.

Schéma EUDI Wallet

Ďalším je návrh európskej schémy pre peňaženku digitálnej identity. Tá 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 EU AI

Poslednou pripravovanou schémou je európska schéma pre umelú inteligenciu, ktorá sa vzťahuje 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 sakonkrétneho použitia umelej inteligencie.

NBÚ sa ešte v roku 2023 úspešne uchádzal o realizáciu projektu zameraného na posilnenie testovacích a certifikačných kapacít na Slovensku, ktorého hlavným cieľom je podporiť zavedenie nových európskych certifikačných schém do praxe.

Projekt je rozdelený do troch etáp. V prvej sa aktivity zamerajú na vytvorenie právneho rámca na zavedenie schém. V druhej etape realizácie sa aktivity sústredia na podporu akreditácie orgánov posudzovania zhody pre jednotlivé schémy. V tretej sa zamerajú na podporu certifikácie produktov pre výrobcov, poskytovateľov služieb alebo procesov v IKT.

V priebehu implementačnej fázy, ktorá má trvať tri roky, plánujeme podporiť aktivity v celkovej sume približne milión eur. Projekt je plne financovaný zo zdrojov EÚ v programe Digital Europe.
Koncom roka 2024 vyhlásil NBÚ v rámci druhej etapy tohto projektu Výzvu na predkladanie žiadostí o nenávratný finančný príspevok (NFP) na podporu získania akreditácie orgánov posudzovania zhody na schému certifikácie podľa EUCC.

NBÚ sa v roku 2024 v oblasti certifikácie kybernetickej bezpečnosti zároveň zapojil do konzorcia v rámci projektu Trustboost. TrustBoost je iniciatíva zameraná na zvýšenie kybernetickej bezpečnosti, odolnosti a dodržiavania predpisov v celej Európskej únii. Hlavným cieľom iniciatívy TrustBoost je posilniť úsilie o spoluprácu v oblasti dodržiavania kybernetickej bezpečnosti a certifikácie.

V roku 2024 sa v rámci posilnenia informovanosti a spolupráce s verejnosťou pre oblasť certifikácie kybernetickej bezpečnosti spustil nový webový portál ncca.nbu.gov.sk.

Tento portál poskytuje prehľadné a aktuálne informácie o certifikácií produktov, služieb a procesov IKT v oblasti kybernetickej bezpečnosti. Zároveň bude slúžiť ako platforma na komunikáciu medzi odborníkmi, organizáciami a verejnosťou, čím prispieva k posilneniu dôvery v digitálnom priestore.

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 2024 uzavrelo KCCKB grantovú dohodu s Európskou komisiou na nový projekt NCC na roky 2025 - 2028.

V rámci aktivít Národného koordinačného centra bola v roku 2024 vyhlásená výzva FSTP – Kaskádové financovanie ako súčasť NCC projektu z Mechanizmu na podporu obnovy a odolnosti (RRF), ktorej cieľom je významne prispieť k získaniu finančných zdrojov na zabezpečenie svojich kyberbezpečnostných potrieb. Do výzvy sa úspešne prihlásilo 46 subjektov so svojimi projektmi.

Súčasťou cieľov KCCKB v roku 2024 bolo aj intenzívne budovanie odbornej komunity zameranej na kybernetickú bezpečnosť. Toto úsilie viedlo k vytváraniu silných partnerstiev, zdieľaniu osvedčených postupov a zvýšeniu povedomia o dôležitosti kybernetickej bezpečnosti medzi podnikmi, akademickou sférou a verejným sektorom. Prostredníctvom NCC-SK sa stalo členom európskej komunity kybernetickej bezpečnosti podľa Nariadenia (EÚ) č. 2021/887 162 slovenských subjektov.

Od 01. 01. 2024 je na základe súhlasu Národného bezpečnostného úradu v zmysle § 59 zákona č. 215/2004 o ochrane utajovaných skutočností KCCKB autorizované na:

- posudzovanie bezpečnostného projektu technického prostriedku podľa § 56 ods. 2 Zákona

- overovanie zhody vlastností technického prostriedku s požiadavkami bezpečnosti a na schvaľovanie použitia technických prostriedkov podľa § 2 a § 5 vyhlášky č. 339/2004 o bezpečnosti technických prostriedkov

O posudzovanie technických prostriedkov proti úniku utajovaných skutočností nežiaducim elektromagnetickým vyžarovaním (NEV) žiada výrobca, splnomocnený zástupca výrobcu, dovozca, distribútor alebo užívateľ. V roku 2024 bolo vykonané meranie u viac ako 40 subjektov. V rámci expertných činností vykonalo KCCKB 47 auditov kybernetickej bezpečnosti.

Počet certifikovaných osôb sa prostredníctvom KCCKB v roku 2024 navýšil o 14 certifikovaných audítorov a 37 certifikovaných manažérov.

Kompetenčné centrum bolo úspešné aj v oblasti vzdelávania dospelých. Vydaná bola aktualizovaná vzdelávacia schéma. Do portfólia vzdelávania pribudol nový špecializovaný kurz a workshop zameraný na riadenie dodávateľov a na riadenie kontinuity činností. Aktualizované boli sylaby viacerých existujúcich kurzov. Za rok 2024 bolo realizovaných celkovo 53 školení, z toho osem kurzov Základy KB, 20 kurzov Manažér KB, tri kurzy Audítor KB, sedem špecializačných kurzov a workshopov, jeden kurz manažérstva informačnej bezpečnosti podľa ISO/IEC 27001:2022, desať bezplatných webinárov Prehľad kybernetickej bezpečnosti s účelom zvyšovania povedomia o kybernetickej bezpečnosti, jeden seminár s témou transpozície smernice NIS2, jeden webinár s témou ako správne napísať projekt a získať európske financovanie. Celkovo sa na uvedených vzdelávacích aktivitách počas roku 2023 zúčastnilo 961 účastníkov.

Kompetenčné centrum sa aktívne zúčastňovalo na konferenciách a podujatiach na Slovensku aj v zahraničí. Celkovo zástupcovia v roku 2024 KCCKB uskutočnilo 47 odborných prednášok na konferenciách, ako aj na pôde vybraných vysokých škôl v SR.

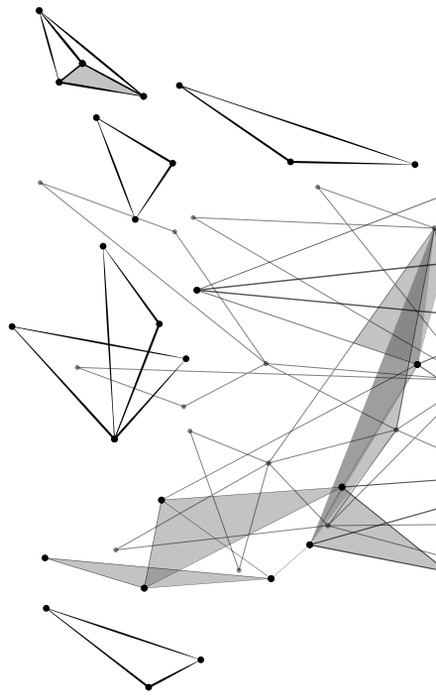
V rámci publikačných aktivít vydávalo KCCKB letáky na účely zvyšovania bezpečnostného povedomia:

- Kategórie osobných údajov
- Čo je to ransomvér a ako sa chrániť?
- 10 manažérskych chýb, ktoré vedú k incidentu
- Aké silné je vaše heslo?
- Najbežnejšie typy útokov na heslá
- Kybernetická bezpečnosť 2024 – materiál k prieskumu verejnej mienky

Už každoročne sú na základe zadania KCCKB spracované prieskumy stavu kybernetickej bezpečnosti, vydané následne aj vo forme verejného dokumentu. V roku 2024 bol uskutočnený prieskum verejnej mienky medzi verejnosťou na vzorke tisíc respondentov. Aj v roku 2024 KCCKB rozširovalo okruh organizácií, s ktorými uzatvorilo spoluprácu formou podpisu memoranda.

V spolupráci s SK-CERT postavilo Kompetenčné a certifikačné centrum kybernetickej bezpečnosti tím mladých, talentovaných ľudí, ktorí Slovensko reprezentovali v októbri 2024 na podujatí European CyberSecurity Challenge (ECSC) v talianskom Turíne. Aktivitu zastrešila ENISA. Prítomných bolo 44 národných tímov. Slovenský tím reprezentovalo desať mladých talentov – deväť chlapcov a jedno dievča. Na súťaž sa tím pripravoval niekoľko mesiacov. V júni sa zúčastnili medzinárodného bootcampu vo Viedni a následne šiestich tréningových bootcampov v Brunovciach. Tím sa pripravuje aj naďalej na účasť na ECSC v roku 2025.

MEDZINÁRODNÁ SPOLUPRÁCA



Príslušníci úradu rozvíjajú vzťahy so zahraničnými partnermi na dennej báze naprieč desiatkami organizácií, platforiem aj formátov. NBÚ v roku 2024 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

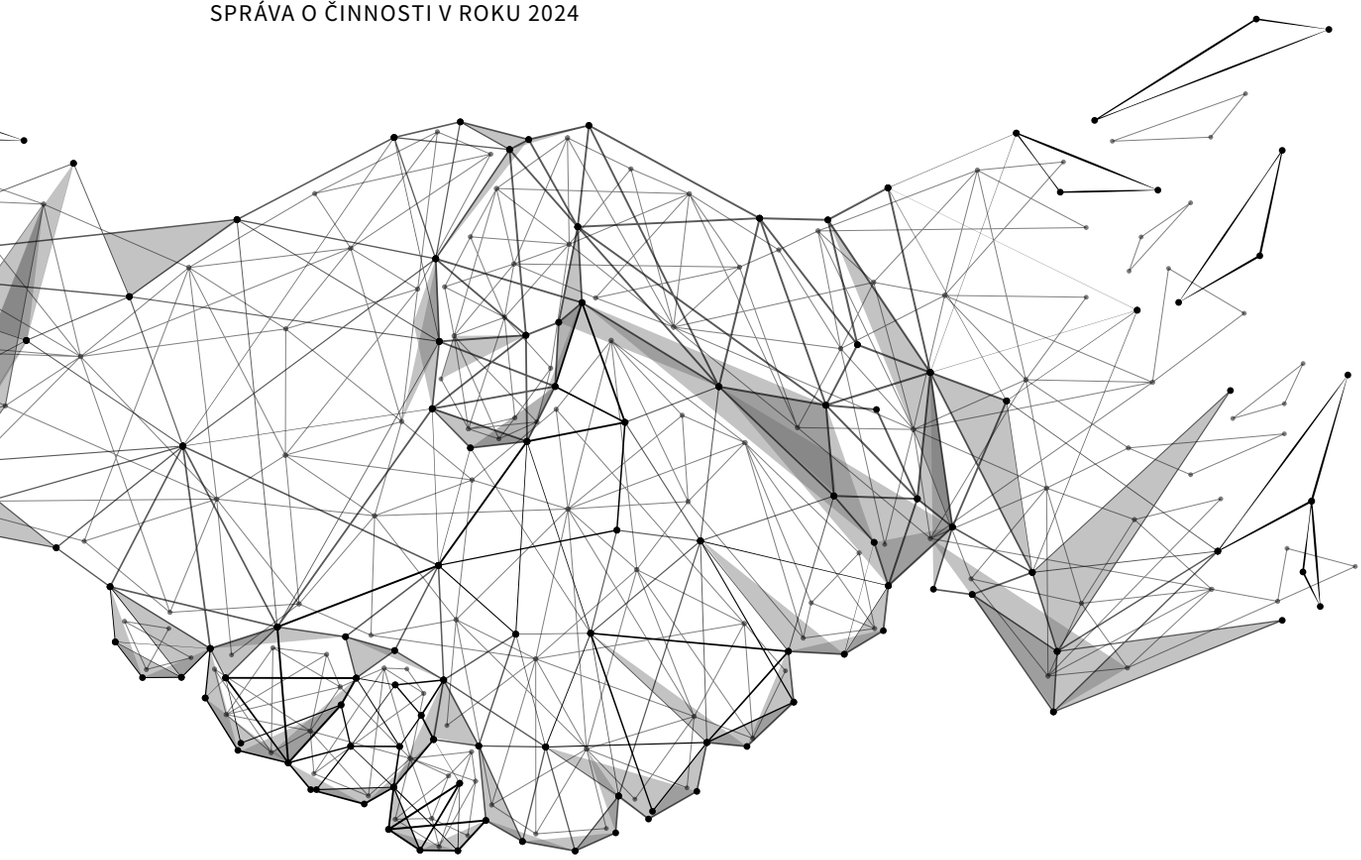
Na úseku ochrany utajovaných skutočností sa príslušníci úradu naďalejzúčastňujú, či už prezenčne alebo vo virtuálnom priestore, pravidelných zasadnutí Bezpečnostného výboru Rady EÚ (CSC), Skupiny expertov Európskej komisie pre bezpečnostnú politiku (ComSEG), Bezpečnostného výboru Európskej služby pre vonkajšiu činnosť (EEAS), Expertnej skupiny pre personálnu bezpečnosť EEAS, Bezpečnostného výboru Agentúry Európskej únie pre vesmírny program (EUSPA) a Implementačnej pracovnej skupiny pre TEMPEST (ITTF).

Na pôde Rady EÚ naďalej prebiehali práce na revízii bezpečnostných pravidiel s cieľom odstrániť nedostatky identifikované v aplikačnej praxi a za účelom zvýšenia komfortu adresátov týchto pravidiel. V uvedených pracovných formátoch sa úrad zapájal do prípravy bezpečnostných noriem, aby bola zvýšená úroveň ochrany utajovaných skutočností a aktívne sa zapájal aj do procesu revízie bezpečnostných pravidiel.

Aj v roku 2024 sa rokovania CSC primárne zameriavali na pokračujúcu rozsiahlu revíziu bezpečnostných pravidiel Rady pre ochranu utajovaných skutočností EÚ (EUCI). Diskusie k jednotlivým oblastiam bezpečnosti (personálna, priemyselná, administratívna, fyzická a objektová bezpečnosť), ako aj účel a pôsobnosť pravidiel boli ukončené.

Počas rokovaní CSC a ComSEG rezonovala problematika výkladu práva Európskej únie s poukázaním na konkrétny rozsudok Európskeho súdneho dvora v prípade BONUL (dnes PROTECTUS) C-185/23. Právna služba Rady EÚ (CLS) jednoznačne uviedla, že rozsudok výhradne rieši problematiku interpretácie práva EÚ, vonkoncom sa nevenoval národnému právu a ani fakty prípadu BONUL neboli predmetom rozsudku. CLS považuje za dôležité hlavné posolstvo rozsudku a to, že pre bezpečnostné pravidlá Rady z neho nevyplývajú žiadne povinnosti, a teda súčasné znenia sú dostatočné a nemusia sa v tomto smere upravovať ani dopĺňať. Členské štáty vyzvali Sekretariát Rady EÚ na pripravenie usmernenia, ktoré by zahŕňalo najlepšie postupy členských

1) Rozhodnutie Rady 2013/488/EÚ o bezpečnostných predpisoch na ochranu utajovaných skutočností EÚ



štátov v takýchto prípadoch, keďže sa predpokladá, že v členských štátoch, kde je možnosť odvolania voči rozhodnutiu Národného bezpečnostného úradu, sa budú podobné prípady opakovať.

Na úseku kybernetickej bezpečnosti bolo prioritou dokončiť legislatívny proces v spojitosti s očakávaným ukončením legislatívneho cyklu v Európskom parlamente ako aj príchodom nového Kolégia komisárov Európskej komisie. Počas belgického predsedníctva sa dokončila politická diskusia k návrhu Nariadenia o riadenýchbezpečnostných službách (CSA+), ktoré tvorilo súčasť kybernetického balíčka predstaveného Európskou komisiou v apríli 2023. Z dôvodu administratívnych komplikácií a nedostatku kapacít prekladateľov sa nakoniec CSA+ ako aj druhý návrh tohto balíčka - Nariadenie k opatreniam na posilnenie solidarity a kapacít v Únii na odhaľovanie kybernetických hrozieb a incidentov, prípravu a reakciu na ne (CySOLa), dostali do procedúry korigenda, čoho dôsledkom bolo záverečné schvaľovanie až v novom Európskom Parlamente a Rade EÚ počas maďarského predsedníctva. Akty EÚ tak boli publikované vo Vestníku EÚ až začiatkom roka 2025. Do procedúry korigenda sa dostal aj návrh Nariadenia o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami (CRA), ktorý bol formálne uzatvorený na jeseň 2024. Vo Vestníku Európskej únie bol publikovaný v októbri 2024.

V rámci aktivít v komitologických výboroch si osobitnú pozornosť zaslúžila aj príprava kandidátskych schém kybernetickej bezpečnosti EUCC (spoločné kritériá) a EUCS (cloudové schémy), z ktorých sa v priebehu roka 2024 práve EUCC dostalo do praxe. Príprava EUCS sa z politických dôvodov dočasne pozastavila.

Horizontálna pracovná skupina pre kybernetické záležitosti (HWPCI) v rámci svojich nelegislatívnych aktivít venovala svoju pozornosť aj ostatným strategickým prvkom kybernetickej diplomacie. V oblasti kybernetickej diplomacie, ktorá obsahovo

presahuje do domén Spoločnej zahraničnej a bezpečnostnej politiky EÚ (SZBP) a Spoločnej bezpečnostnej a obrannej politiky EÚ (SBOP), sa aktivity Slovenska a ostatných členských štátov sústredili prevažne na koordináciu spoločných pozícií EÚ pre rokovania Pracovnej skupiny s otvoreným koncom (OEWG) pre bezpečnosť a využívanie IKT pri OSN, či na diskusie ku Globálnemu digitálnemu paktu (GDC) a tiež k novému Dohovoru o boji proti počítačovej kriminalite. Slovensko sa tiež zapojilo do kybernetických dialógov s tretími partnerskými krajinami, osobitne s USA, Spojeným kráľovstvom, či Japonskom a zúčastnilo sa cvičenia aplikácie Súboru nástrojov kybernetickej diplomacie v praxi. Slovensko spolupracovalo v kontexte vyhodnocovania neustálych kybernetických hrozieb s ostatnými členskými štátmi, EEAS (Situačné centrum EÚ - INTCEN), ENISA, či CERT-EU a zúčastnilo sa prípravy nových sankčných kybernetických zoznamov pre dotknuté fyzické osoby. Aktívne sa tiež zapojilo do procesu prípravy strategického materiálu k zaujatiu pozície EÚ voči pokročilým aktérom hrozieb ako aj strategického materiálu ohľadom pozície EÚ v oblasti kybernetickej bezpečnosti v krajinách západného Balkánu.

Okrem toho sa v roku 2024 úrad aktívne zúčastňoval aj na zasadnutiach Skupiny pre spoluprácu – k transpozícii smernice NIS (NIS Cooperation Group) a v jej podskupinách pri oblastiach Work Stream Post-Quantum Cryptography, Work Stream on Election (volebné procesy), Work Stream on Health (zdravotníctvo) a Working Group on Aviation (letecká doprava).

Hlavnými témami Work Stream Post-Quantum Cryptography zasadaní boli prijatie a implementácia nových post-kvantových štandardov do národnej a medzinárodnej bezpečnostnej infraštruktúry, 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. Medzi hlavné úlohy patrí aj aktívna spolupráca pri príprave Plánu koordinovanej implementácie post-kvantovej kryptografie.

V skupine Work Stream on Election rezonovali na zasadnutiach k bezpečnosti a dôveryhodnosti volebných procesov s ohľadom na digitálne voľby a elektronické hlasovanie najmä témy pre oblasti ochrany pred kybernetickými útokmi počas volieb a ochrana osobných údajov voličov, zabezpečenie integrity volebného procesu vrátane prevencie pred manipuláciou a podvodmi, ako aj zdieľanie skúseností medzi členskými štátmi a medzinárodnými organizáciami v oblasti volebnej bezpečnosti.

V rámci rastúcej digitalizácie zdravotnej starostlivosti sa skupina Work Stream on Health sústreďuje 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 efektívne fungovanie zdravotných systémov. Na zasadnutiach sa členovia skupiny venovali transpozícii smernice NIS2 do národnej legislatívy, ktorá je zameraná na zlepšenie ochrany kritickej digitálnej infraštruktúry v oblasti zdravotnej starostlivosti, a tiež Európskemu akčnému plánu ku kybernetickej bezpečnosti nemocníc a zdravotníckych zariadení. Zástupcovia úradu tak aktívne mohli prispievať informáciami ohľadom napredovania legislatívneho procesu novelizácie zákona o KB s dopadom na sektor zdravotníctva.

Cieľom Working Group on Aviation počas roka 2024 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 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 danom prípade zástupcovia úradu zdieľali informácie napredovania legislatívneho procesu transpozície smernice NIS2 s dopadom na sektor leteckej dopravy.

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 prebieha strategická diskusia zameraná na efektívne zdieľanie informácií o kybernetickej bezpečnosti. Spolupráca podporuje výmenu dôležitých informácií v kybernetickom priestore. Stretnutia CyCLONu mali za cieľ v roku 2024 vylepšovanie a overovanie postupov pri riešení závažných incidentov s cezhraničným presahom a v rámci stretnutí prebehlo aj cvičenie Cyber Europe 2024, prostredníctvom simulácie eskalácie rozsiahleho kybernetického bezpečnostného incidentu so zameraním na energetický 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 schopnosti riešiť tieto krízy.

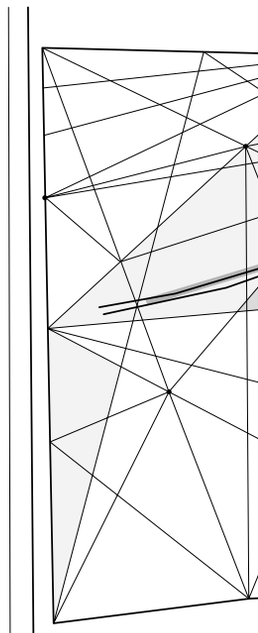
Národné centrum kybernetickej bezpečnosti prostredníctvom svojej organizačnej zložky SK-CERT – národná jednotka CSIRT, aktívne pôsobí aj v rámci medzinárodných organizácií, združujúcich jednotky CSIRT. V rámci CSIRT Network, ktorá združuje národné CSIRT jednotky členských štátov EÚ, si SK-CERT s ostatnými členskými štátmi vymieňal operatívne informácie o hrozbách a incidentoch. Keďže vojenská situácia na východe Európy sa nezmenila, jednotlivé štáty si vymieňali informácie a skúsenosti s incidentmi a útokmi, ktoré súviseli s vojnou na Ukrajine a poskytovali si vzájomnú pomoc podľa potreby. SK-CERT si v rámci CSIRT Network v roku 2024 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.

AGENTÚRA EURÓPSKEJ ÚNIE PRE VESMÍRNY PROGRAM (EUSPA)

V roku 2024 sa príslušníci úradu zúčastňovali na pravidelných zasadaniach Bezpečnostného výboru pre Vesmírne programy EÚ v rámci EUSPA. V rámci hlavného Bezpečnostného výboru EUSPA boli hlavným bodom diskusie vypracovanie základných bezpečnostných požiadaviek, a tiež aj 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 boli vytvorené nové pracovné skupiny spadajúce pod Bezpečnostný výbor EUSPA. Ide o pracovnú skupinu 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 má zabezpečiť vysokú mieru šifrovania, odolnosti a v konečnom dôsledku aj bezpečnosti, keďže táto sieť má byť prispôsobená aj na prenos utajovaných skutočností.

ORGANIZÁCIA PRE BEZPEČNOSŤ A SPOLUPRÁCU V EURÓPE (OBSE)

Zorganizované stretnutia účastníckych štátov OBSE, na ktorých mal aktívne zastúpenie v roku 2024 aj úrad, podčiarkli dôležitosť medzinárodnej spolupráce v oblasti kybernetickej bezpečnosti a zdieľania informácií o existujúcich a potenciálnych hrozbách. Napriek vysokému zastúpeniu účastníckych štátov OBSE boli zasadnutia aj naďalej ovplyvnené geopolitickou situáciou, najmä prebiehajúcim konfliktom na Ukrajine, čo následne vplývalo aj na priebeh rokovaní o ostatných témach, ako je bezpečnosť IKT. Na zasadnutia pracovnej skupiny vplývajú medzištátne konflikty aj prebiehajúce procesy v oblasti kybernetickej bezpečnosti a diplomacie na pôde iných medzinárodných organizácií. Preto je potrebné vynakladať väčšie úsilie zo strany Sekretariátu OBSE, Oddelenia OBSE pre nadnárodné hrozby (TNTD) ako aj účastníckych štátov za účelom dosiahnutia pokroku v rokovaniach o relevantných témach spojených s agendou OBSE. Rusko prostredníctvom svojich vstupov pravidelne namietalo politizáciu diskusie a odkazovalo na dvojitý štandard údajne propagovaný členskými štátmi EÚ a NATO.



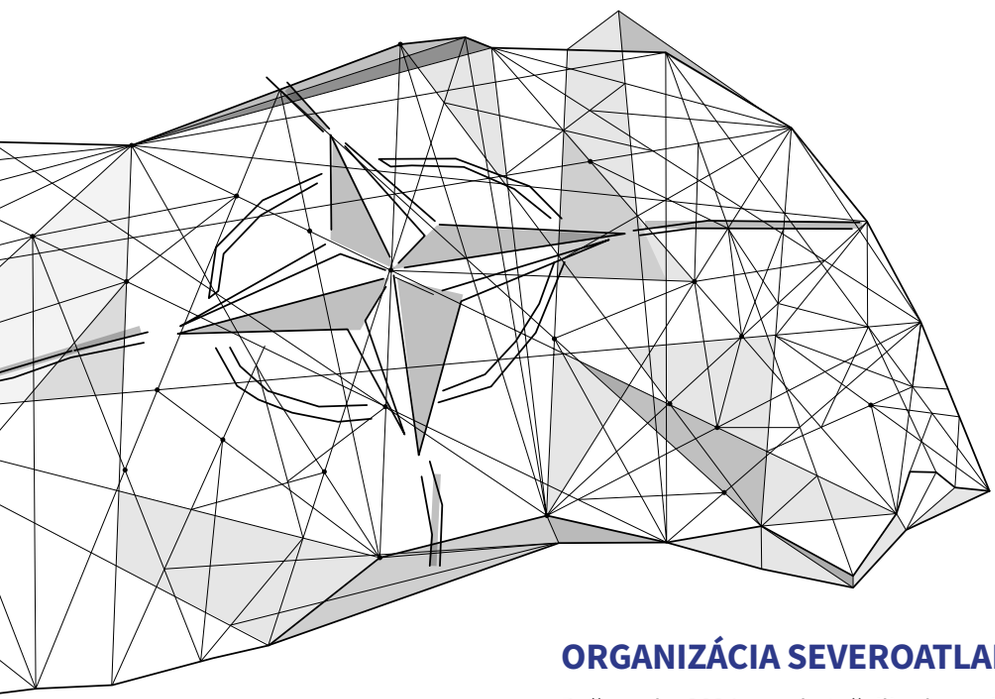
V uplynulom roku sa uskutočnili celkom štyri zasadnutia Neformálnej pracovnej skupiny OBSE pre oblasť kybernetickej bezpečnosti a informačných a komunikačných technológií (IWG). Výročné stretnutie kontaktných bodov OBSE (CBM8) sa konalo súbežne s druhým zasadnutím IWG v júni 2024. Obsah zasadnutí tvorili diskusie o prebiehajúcej implementácii existujúcich iniciatív v zmysle opatrení na budovanie dôvery (CBM) zúčastnených štátov OBSE, o národných iniciatívach (pripravované národné stratégie kybernetickej bezpečnosti a príslušné akčné plány ich implementácie) a vnútroštátnom vývoji v oblasti kybernetickej/IKT bezpečnosti. Krajiny tiež upriamili pozornosť na národné procesy spojené s novými a vznikajúcimi technológiami a umelou inteligenciou. Súčasťou zasadnutí boli i sprievodné podujatia zamerané na relevantné témy IKT prostredia napr. na Ženevský dialóg (Geneva Dialogue) a Ženevskú príručku (Geneva Manual) o zodpovednom správaní v kybernetickom priestore. Oddelenie OBSE pre nadnárodné hrozby prezentovalo sumarizáciu výsledkov kontroly komunikácie (CommCheck) týkajúcej sa CBM8. Sekretariát OBSE v spolupráci s predsedom OEWG OSN pracovali na tvorbe Globálneho adresára kontaktných bodov OSN, ktorý bol spustený v apríli 2024.

Maltské predsedníctvo organizovalo výročnú konferenciu o kybernetickej bezpečnosti, ktorá sa konala v júli vo Vallette. Hlavnými témami konferencie boli kybernetická bezpečnosť a odolnosť kritickej infraštruktúry účastníckych štátov OBSE. V septembri 2024 sa na úrovni OBSE uskutočnila Štvrtá medziregionálna konferencia o kybernetickej/IKT bezpečnosti s cieľom posilniť spoluprácu v oblasti kybernetickej bezpečnosti v regióne OBSE a v ázijskom regióne.

Prostredníctvom zasadnutí úrad zdieľal informácie o procese transpozície smernice NIS2 do národnej legislatívy, o stave kybernetickej bezpečnosti, ako aj o aktuálnych aktivitách a pokrokoch pri implementácii opatrení na budovanie dôvery. Vplyv slovenského predsedníctva Bezpečnostnému výboru OBSE sa výrazne ukázal pri rokovaniach o bezpečnostných otázkach, vrátane IKT, zberu vstupov, koordinácie a príprave výročnej konferencie Maltského predsedníctva 2024.

Slovensko sa v roku 2024 pripojilo do Komunikačnej siete OBSE (CommsNet) ako aj do Globálneho adresára kontaktných bodov OSN - kde máme aktualizované kontaktné body na úrovni Ministerstva zahraničných vecí a európskych záležitostí SR (MZVaEZ SR) ako aj na úrovni úradu. Úrad vníma prínos zasadnutí OBSE v bezpečnom zdieľaní informácií, posilňovaní medzinárodnej spolupráce, upevňovaní svojho postavenia ako spoľahlivého medzinárodného hráča a rozširovaní svojej siete kontaktných bodov o odborníkov z IKT oblasti pôsobiacich i mimo členských štátov EÚ. Úrad v spojitosti

s aktivitami OBSE pozitívne hodnotí i koordinovanie spolupráce na národnej úrovni so zástupcami MZVaEZ SR. Z perspektívy úradu boli kľúčové najmä témy týkajúce sa aplikácie medzinárodného práva v kybernetickom priestore, budovanie kapacít, tvorba národných aj regionálnych pozícií, stratégie boja proti aktuálnym kybernetickým a hybridným hrozbám (ich prevencia, reakcia na takéto hrozby a nástroje stabilizácie kybernetického priestoru) či zamedzenie možného zneužitia nových a vznikajúcich technológií hlavne v kontexte podvratných aktivít vykonávaných nielen štátnymi ale aj neštátnymi aktérmi.

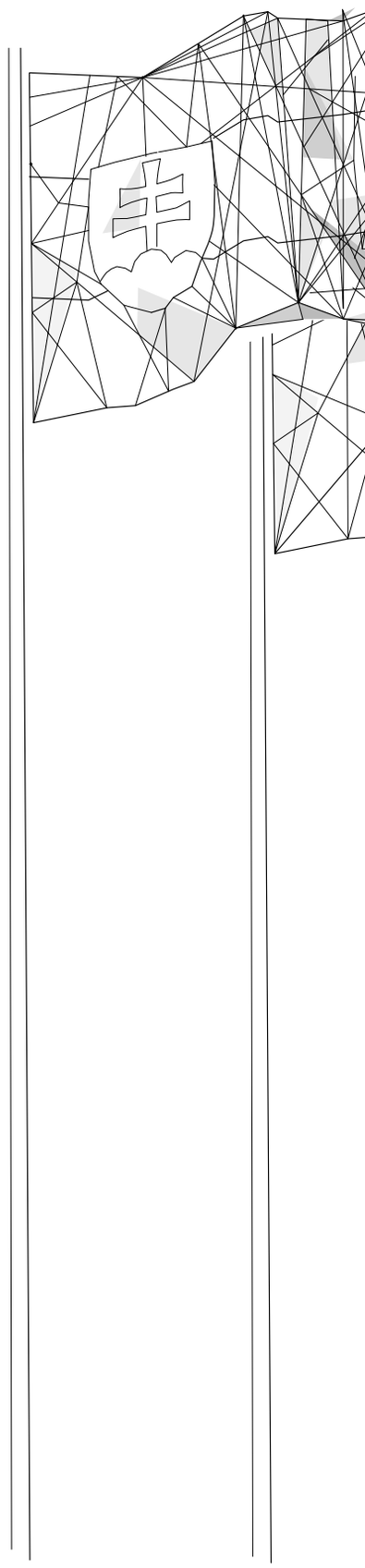


ORGANIZÁCIA SEVEROATLANTICKEJ ZMLUVY (NATO)

Počas roka 2024 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. Počas jarného zasadnutia SC mali zástupcovia národných bezpečnostných úradov možnosť navštíviť Akcelerátor obranných inovácií NATO - DIANA (Defence Innovation Accelerator for NATO), ktorý využíva svoj program a sieť testovacích centier na to, aby spojil start-up s operačnými koncovými používateľmi, vedcami a systémovými integrátormi s cieľom podporiť špičkové technológie s riešeniami s dvojakým použitím pre Alianciu. Do výziev projektov sa aktívne zapájajú aj slovenské spoločnosti, zatiaľ však bez väčších úspechov (bližšími informáciami disponuje Ministerstvo obrany SR).

Pokračuje sa aj v rozsiahlej revízii bezpečnostných pravidiel NATO. Revízie sa zamerali predovšetkým na podporné dokumenty k hlavnej bezpečnostnej politike NATO C-M(2002)49-REV1, a to napr. usmernenia o personálnej, fyzickej a objektovej, administratívnej bezpečnosti, o bezpečnostnej ochrane NATO Restricted informácií. V roku 2024 prebehli prvé spoločné rokovania pracovnej skupiny pozostávajúcej z členov Archívneho výboru a SC, ktorej úlohou je riešiť problematiku hromadného odtajovania utajovaných skutočností NATO. Na jesennom rokovaní SC na najvyššej úrovni námestníčka úradu delegátov informovala, že na jeseň 2025 bude Slovensko hostiť rokovanie SC s NNEs (Non-NATO Entities). Pôjde o veľkú udalosť, keďže podobné rokovanie za veľkej účasti členských a partnerských štátov a inštitúcií sa ešte na Slovensku neuskutočnilo. Téma hosťovania NATO podujatia na Slovensku je predmetom ďalšej diskusie.

V decembri 2024 sa uskutočnilo zasadanie Archívneho výboru (NATO AC), ktorého témou 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 z vojenských operácií, ako aj o zmeny v procesoch automatického odtajovania utajovaných skutočností vo Francúzsku.



Za hlavný míľnik v oblasti kybernetickej bezpečnosti/obrany Severoatlantickej aliancie (NATO) v 2024 možno považovať júlový Varšavský summit, počas ktorého došlo k schváleniu dvoch zásadných dokumentov, ktoré jednoznačne prispejú do budovania a upevňovania celkovej zostavy odstrašovania a obrany NATO. Prvým je Príručka strategických opatrení reakcií na závažné škodlivé kybernetické aktivity a kampane, ktorá umožní posilnenie integrovaného situačného povedomia, celkovej odolnosti NATO a podporí proces kolektívnej akcie. Druhým je Zriadenie NATO Integrated Cyber Defence Centre (NICC), ktoré posilní schopnosť Aliancie chrániť svoje komunikačno-informačné systémy, ako aj vnímanie kyberpriestoru ako operačnej domény v rámci multidoménových operácií. Preto bude rok 2025 rokom implementovania politicko-vojenských odporúčaní tak, aby NICC mohlo byť plne funkčné na jeseň 2026.

Ďalšou udalosťou roka bola konferencia Cyber Defence Pledge, ktorá sa uskutočnila v máji v Haagu. Veľvyslanci sa tak po ročnej prestávke, ktorá bola zameraná na efektívnu úpravu dotazníka reflektujúceho na rýchlo meniaci sa kyberpriestor, zhodnotenie dosiahnutého pokroku v oblasti kybernetickej bezpečnosti/obrany Aliancie. Členské štáty tak po prvýkrát na základe samohodnotenia pri vyplňovaní dotazníka (od roku 2016) mohli kvantitatívne merať dosiahnutie pokroku. Tieto merateľné ukazovatele tak uľahčia porovnávanie dosiahnutej úrovne kybernetickej bezpečnosti u daného spojenca nielen naprieč rokmi, ale aj naprieč porovnávaniami s ostatnými spojencami, prípadne partnermi.

Druhá výročná konferencia o kybernetickej obrane NATO bola ďalšou významnou udalosťou, a to nielen v oblasti kybernetickej obrany. Konferencia sa uskutočnila v novembri v Londýne a prepojila všetky zainteresované strany na všetkých troch úrovniach (politickej, technickej a vojenskej) nielen v rámci štruktúr NATO, ale aj u 32 spojencov. Slovensko bolo zastúpené predstaviteľmi úradu a Centra kybernetickej obrany.

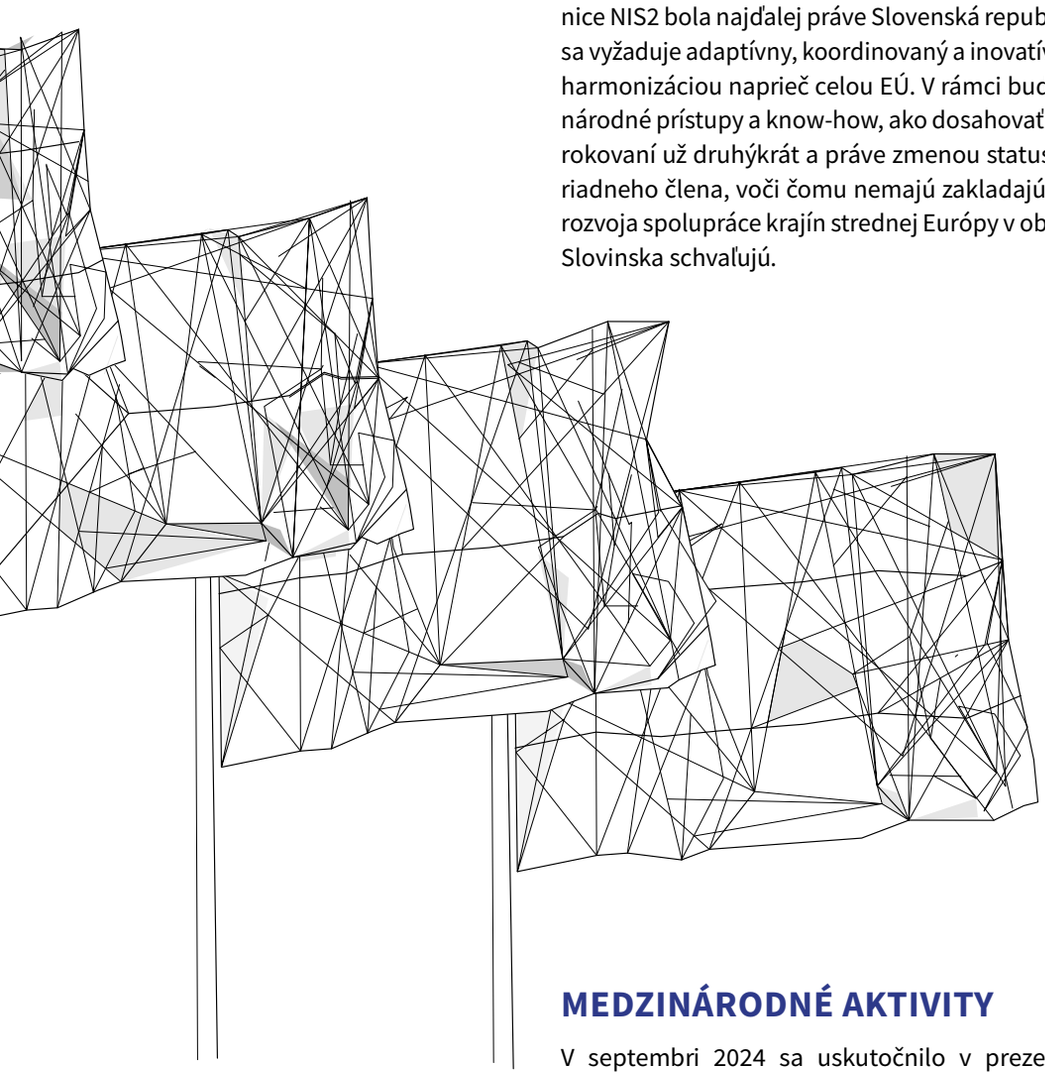
V roku 2024 úrad participoval aj na spoločnom aliančnom cvičení NATO Able Staff 2024, ktoré sa uskutočnilo v novembri 2024 a malo preveriť komunikačné procedúry súvisiace s jadrovým plánovaním, precvičiť použiteľné opatrenia systému krízovej odozvy aliancie, priniesť zdokonalenie v konzultačnej oblasti, 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.

REGIONÁLNA SPOLUPRÁCA

Na základe rotujúceho predsedníctva krajín, ktoré sú členmi Stredoeurópskej platformy pre kybernetickú bezpečnosť (CECSP), Úrad rakúskeho spolkového kancelára v roku 2024 predsedal tejto platforme. Zástupcovia úradu sa aktívne zúčastnili na rokovaniach platformy spolu s ďalšími kolegami zastúpenými krajinami Vyšehradskej štvorky (Česká republika, Maďarsko, Poľsko) a Rakúska. Predmetom rokovaní boli aktuálne témy, ktoré na úrovni EÚ rezonovali počas celého roka 2024 a súčasne sa partneri v rámci týchto tém snažili nájsť spoločné prieniky a vzájomnú podporu. Zároveň sa rakúske predsedníctvo zaoberalo revíziou zakladajúcich dokumentov

„Central European Cyber Security Platform – Declaration“ a „Working program for European Central Security Platform“.

Medzi najdôležitejšie témy stretnutia patrili aktuálny stav procesu transpozície smernice NIS2 v jednotlivých členských štátoch, kybernetická bezpečnosť a kyberdiplomacia, Certifikácia kybernetickej bezpečnosti, a nariadenie CRA. V procese aproximácie smernice NIS2 bola najďalej práve Slovenská republika. Experti sa zhodli, že pri aproximácii sa vyžaduje adaptívny, koordinovaný a inovatívny prístup, ktorým sa dosiahne najširšia harmonizáciou naprieč celou EÚ. V rámci budovania kapacít prezentovali zúčastnení národné prístupy a know-how, ako dosahovať stanovené ciele. Slovinsko sa zúčastnilo rokovaní už druhýkrát a práve zmenou statusových dokumentov sa vydalo na cestu riadneho člena, voči čomu nemajú zakladajúce krajiny žiadne výhrady a na princípe rozvoja spolupráce krajín strednej Európy v oblasti kybernetickej bezpečnosti členstvo Slovinska schvaľujú.



MEDZINÁRODNÉ AKTIVITY

V septembri 2024 sa uskutočnilo v prezenčnej forme 38. plenárne zasadanie Multinational Industrial Security Working Group (MISWG). Pracovná skupina MISWG je uznávaným orgánom pre spoluprácu v rámci najlepších postupov v oblasti medzinárodnej priemyselnej bezpečnosti, kde je zastúpených takmer 40 krajín sveta vrátane Slovenskej republiky. Hlavným cieľom stretnutia bolo podporiť, zlepšiť a harmonizovať spoločné medzinárodné osvedčené postupy na ochranu utajovaných skutočností (v oblasti priemyselnej bezpečnosti) a iných foriem vládou kontrolovaných informácií, ktoré čelia súčasným a novým bezpečnostným hrozbám a výzvam v tejto oblasti. Vyzdvihlo sa množstvo dôležitých rozhodnutí a dôležitý pokrok, ktorý sa dosiahol v priebehu plenárneho zasadnutia. V rámci MISWG zástupcovia úradu uskutočnili viacero bilaterálnych rozhovorov so zámerom prehĺbiť spoluprácu s partnermi v oblastiach ochrany utajovaných skutočností a kybernetickej bezpečnosti, zároveň prospeli aktívnou účasťou keď prezentovali tému priemyselnej kyberbezpečnosti z pohľadu Slovenska.

O nadviazaní bližšej spolupráce sa viedli rozhovory rovnako so zástupcami Dánskeho kráľovstva, Maďarska, Českej republiky, Poľskej republiky, Rakúskej republiky a Izraelským štátom. Témami boli ochrana utajovaných skutočností v segmente obrana spolupráca a obranný priemysel.

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 na bilaterálnej úrovni.

Za hlavnú udalosť roka z pohľadu úradu možno považovať prijatie riaditeľa NATO Office of Security Galena Nacea (NOS NATO) na pôde NBÚ v septembri 2024. Počas stretnutia s riaditeľom a námestníčkou úradu sa riaditeľ NOS NATO zaujímal o praktické fungovanie úradu, nielen za jednotlivé oblasti ochrany utajovaných skutočností, ale aj úradu ako gestora tém kybernetickej bezpečnosti, dôveryhodných služieb a šifrovej ochrany informácií. Galen Nace ocenil rozvoj vzájomných vzťahov. Cieľom rokovaní bolo posilniť spoluprácu medzi Slovenskou republikou a NATO v oblasti ochrany utajovaných skutočností, predchádzania kybernetických incidentov a hrozieb.

V júni 2024 bola podpísaná medzinárodná zmluva medzi vládou Slovenskej republiky a Európskou vesmírnou agentúrou (ESA) o výmene a vzájomnej ochrane utajovaných skutočností. V priebehu roka boli taktiež uzavreté medzivládne dohody o výmene a vzájomnej ochrane utajovaných skutočností s Holandským kráľovstvom (júl 2024) a Brazílskou federatívnou republikou (december 2024). Zástupcovia úradu tiež participovali na uzavretí zmluvy medzi vládou Slovenskej republiky a Organizáciou pre spoluprácu v spoločnom vyzbrojovaní (OCCAR), ktorá bola schválená vládou Slovenskej republiky v novembri 2024. Predmetná zmluva, ktorá umožní slovenským subjektom účasť na európskych projektoch v oblasti zbrojného priemyslu, bola podpísaná vo februári 2025.

V nadväznosti na podpísanie memoranda o spolupráci v oblasti kybernetickej bezpečnosti s Kenskou republikou v prvej polovici roka 2024 a v záujme prehlbovan a rozvojovej spolupráce zástupcovia Národného bezpečnostného úradu opäť navštívili Kenskú republiku v októbri 2024. Návšteva jednoznačne zvýraznila vzájomné snahy o výmenu skúseností a poznatkov v oblasti kybernetickej bezpečnosti a kybernetickej diplomacie. V daných témach sa okrem úradu angažovali aj predstavitelia MZVaEZ SR a Vojenského spravodajstva. Návšteva slovenských odborníkov z viacerých rezortov bola financovaná z prostriedkov oficiálnej rozvojovej spolupráce SlovakAid, konkrétne z nástroja na zdieľanie skúseností a expertízy. Kenská protistrana prejavila eminentný záujem o účasť na projekte CyberGame 2025, kde sa realizujú ďalšie konzultácie a podpora zo strany úradu.

Okrem uvedených prijatí a zaužívaných bilaterálnych spoluprác prejavili záujem o nadviazanie spolupráce alebo o informácie týkajúce sa agendy kybernetickej bezpečnosti, alebo ochrany utajovaných skutočností prostredníctvom krátkych návštev a stretnutí aj predstavitelia Španielskeho kráľovstva v zastúpení Instituto nacional de ciberseguridad (INCIBE). Prijatie sa uskutočnilo v apríli 2024 a témami boli transpozícia NIS2 a nariadenie CRA, aplikačná prax na Slovensku, európska certifikačná schéma a fungovanie národných kompetenčných centier. Španielska strana predstavila svoju víziu budúcej spolupráce v daných oblastiach.

V rámci bilaterálnych vzťahov príslušníci úradu a zástupcovia NCKB pravidelne komunikovali a vymieňali si informácie o aktuálnych právnych predpisoch na národnej úrovni, zraniteľnostiach, hrozbách a incidentoch, a tiež osvedčené postupy a o dobrú prax so svojimi zahraničnými partnermi aj mimo EÚ. 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 a bezpečnostných politík sekcie regulácie a dohľadu.

V roku 2024 úrad rozvinul aktívnu spoluprácu s partnerskou inštitúciou vo Francúzsku, l´Agence nationale de la sécurité des systèmes d´information (ANSSI), ktorá sa pretavila nielen do intenzívnej spolupráce pre oblasť európskej certifikačnej schémy pre cloudové služby, ale aj do zdieľania analýz a správ o stave hrozieb vo Francúzskej republike (Olympijské hry, voľby do Európskeho parlamentu, potenciálne hrozby a incidenty ...).

VÝMENA ZAHRANIČNÝCH INFORMÁCIÍ

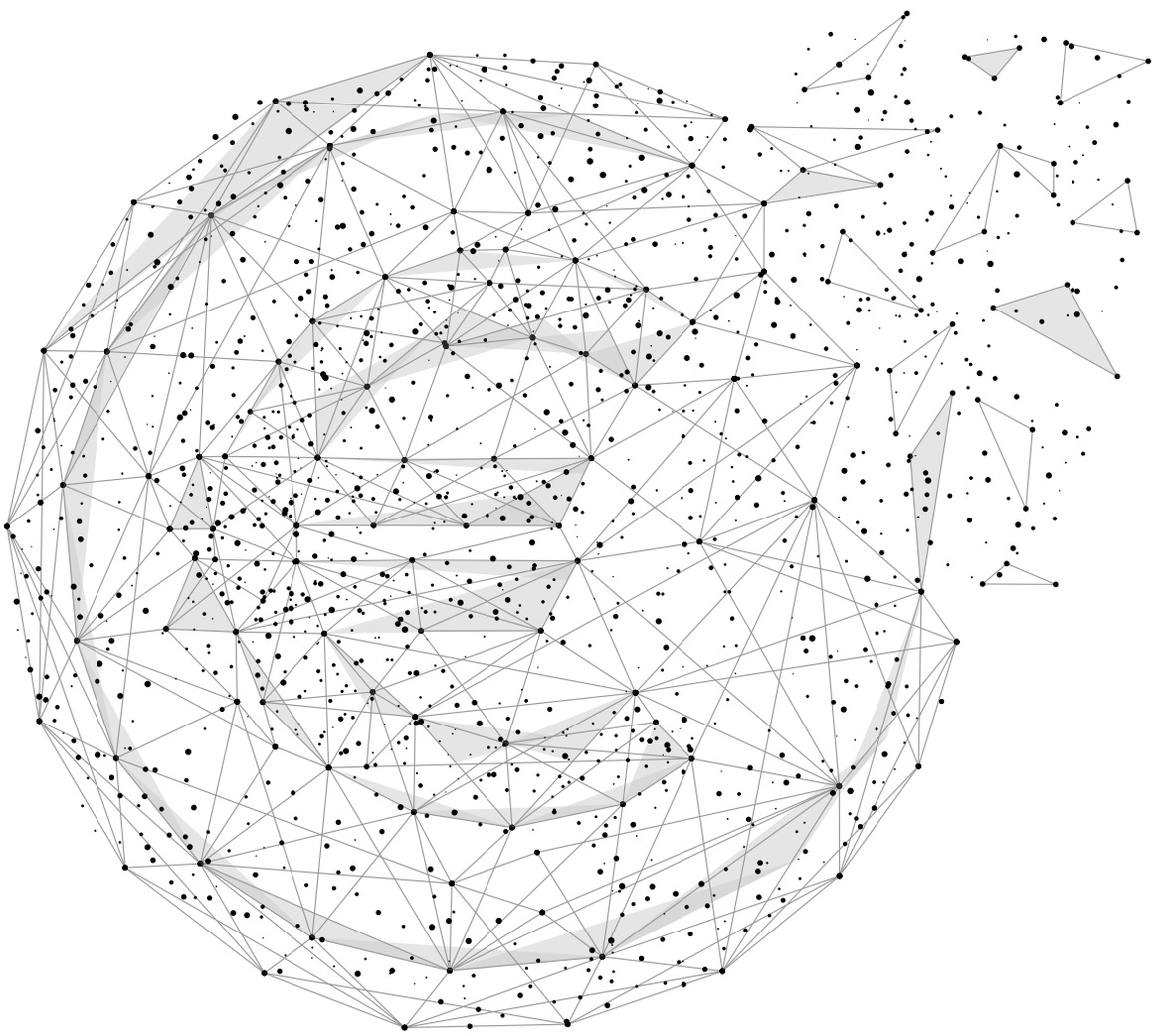
Elektronizácia registrov zahraničných utajovaných skutočností prostredníctvom online prepojenia s registrami utajovaných skutočností orgánov verejnej moci umožňuje bezpečnú, rýchlejšiu a flexibilnejšiu evidenciu a elektronickú distribúciu utajovaných skutočností. NBÚ naďalej poskytoval v roku 2024 jednotlivým registrom utajovaných metodickú pomoc pri elektronickej evidencii utajovaných skutočností.Pracovisko centrálneho registra spracovalo 2 430 utajovaných skutočností NATO a 3053 utajovaných skutočností EÚ. Úrad sprostredkoval aj výmenu 547 utajovaných skutočností cudzej moci. Na úrade od roku 2010 pôsobí register utajovaných skutočností NATO ATOMAL. V roku 2024 v ňom neboli zaevidované žiadne ATOMAL utajované písomnosti.

Stupeň utajenia	2024
NATO — RESTRICTED	1198
EU — RESTRICTED	1232
CUDZIA MOC — VYHRADENÉ	484
NATO — CONFIDENTIAL	7413
EU — CONFIDENTIAL	939
CUDZIA MOC — DÔVERNÉ	41
NATO — SECRET	819
EU — SECRET	882
CUDZIA MOC — TAJNÉ	22
NATO — TOP SECRET	0
EU — TOP SECRET	0
CUDZIA MOC — PRÍSNE TAJNÉ	0
NATO – spolu	**2430**
EU — spolu	**3053**
CUDZIA MOC — spolu	**547**

Národný bezpečnostný úrad má od roku 2021 zriadené centrálne úložisko utajovaných skutočností pre dočasné uloženie utajovaných skutočností, ktoré majú trvalú dokumentárnu hodnotu. Je zriadené na detašovanom pracovisku v Topoľčiankach.
V roku 2024 bola spustená obojsmerná čiastočná integrácia vonkajšieho prostredia s elektronickým informačným systémom pre správu registratúry.

HOSPODÁRENIE

Rozpis záväzných ukazovateľov rozpočtu kapitoly 41 - Národný bezpečnostný úrad na rok 2024, vplyv rozpočtových opatrení na výšku upraveného rozpočtu, skutočné čerpanie rozpočtových prostriedkov k 31. decembru 2024 a percentuálne vyhodnotenie plnenia k upravenému rozpočtu je uvedený v tabuľke č. 1



Záväzné ukazovatele rozpočtu úradu pre rok 2024 schválené zákonom č. 534/2023 o štátnom rozpočte na rok 2024 zo dňa 21. decembra 2023 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: Rozpočet Národného bezpečnostného úradu v roku 2024 (v eurách)

UKAZOVATELE	SCHVÁLENÝ ROZPOČET	UPRAVENÝ ROZPOČET	SKUTOČNOSŤ K 31.12.2024	PLNENIE K UPR. ROZPOČTU
I. Príjmy kapitoly	**20 000,00**	**20 000,00**	**102 367,66**	**511,84%**
A. Záväzný ukazovateľ	20 000,00	20 000,00	102 367,66	511,84%
B. Prostriedky Európskej únie	0,00	0,00	0,00	
II. Výdavky kapitoly celkom (A + B+ C + C.1)	**15 881 633,00**	**18 963 409,06**	**18 732 351,69**	**98,78%**
A. Výdavky spolu bez prostriedkov podľa § 17 ods. 4 zákona				
č. 523/2004 Z. z. a prostriedkov Európskej únie	**15 879 633,00**	**18 812 813,01**	**18 581 755,64**	**98,77%**
z toho:				
A.1. rozpočtové prostriedky kapitoly	15 879 633,00	18 750 958,46	18 519 901,09	98,77%
z toho: kód zdroja 111 + 11H + 11UA	0,00	17 208 801,78	16 981 344,41	98,68%
kód zdroja 131	0,00	1 542 156,68	1 538 556,68	99,77%
A.2. prostriedky na spolufinancovanie	0,00	61 854,55	61 854,55	100,00%
z toho: kód zdroja 3AA2	0,00	3 350,68	3 350,68	100,00%
kód zdroja 3AA3	0,00	2 879,86	2 879,86	100,00%
kód zdroja 3AC2	0,00	22 272,23	22 272,23	100,00%
kód zdroja 3AC3	0,00	33 351,78	33 351,78	100,00%
A.3. mzdy, platy, služ. príj. a ost. os. vyrovnania (610), kód zdroja 111+11H+11UA)	8 030 345,00	8 096 265,00	7 893 884 ,93*	97,50%
toho: mzdy, platy, služ. príjmy a ost. os. vyrovnania aparátu ústred.				
orgánu (kód zdroja 111 + 11H + 11UA)	8 030 345,00	8 096 265,00	7 893 884,93*	97,50%
Počet zamestnancov RO podľa prílohy č. 1 k uzneseniu vlády SR č. 712/2023	254 osôb	258 osôb	234 osôb**	90,70%
z toho: aparát ústredného orgánu	254 osôb	258 osôb	234 osôb**	90,70%
administratívne kapacity rozp. org. osobitne sledované podľa prílohy č. 1 k uzneseniu vlády SR č. 712/2023	0 osôb	0 osôb	0 osôb	
z toho: aparát ústredného orgánu	0 osôb	0 osôb	0 osôb	
A.4. kapitálové výdavky (700) (bez prostriedkov na spolufinancovanie)	634 421,00	2 176 577,68	2 171 469,63	99,77%
z toho: kód zdroja 111	634 421,00	634 421,00	632 912,95	99,76%
kód zdroja 131M	0,00	89 492,40	89 492,40	100,00%
kód zdroja 131N	0,00	1 452 664,28	1 449 064,28	99,75%
A.5. Plán obnovy a odolnosti – prostriedky na úhradu DPH	0,00	0,00	0,00	0,00
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**	**5 399,49**	**5 399,49**	**100,00%**
C. Prostriedky Európskej únie	**0,00**	**145 196,56**	**145 196,56**	**100,00%**
z toho: kód zdroja 1AA1	0,00	9 053,07	9 053,07	100,00%
kód zdroja 3AA1	0,00	9 934,16	9 934,16	100,00%
kód zdroja 3AC1	0,00	126 209,33	126 209,33	100,00%
C.1 Prostriedky z plánu obnovy a odolnosti	**0,00**	**0,00**	**0,00**	
D. Výdavky štátneho rozpočtu na realizáciu programov vlády SR a časti programov vlády SR	**15 881 633,00**	**18 963 409,06**	**18 732 351,69**	**98,78%**
0D9 Bezpečnosť informácií	15 797 888,00	18 862 312,29	18 633 498,08	98,79%
0EK0U Informačné technológie financované zo štátneho rozpočtu – NBÚ	83 745,00	89 073,00	86 829,84	97,48%
0EJ0P Informačná spoločnosť 2014-2020 - MF SR - NBÚ	0,00	12 023,77	12 023,77	100,00%
E. Systemizácia policajtov v štátnej službe	**232 osôb**	**234 osôb**	**212 osôb****	**90,60%**
	7 319 598,00	**7 350 518,00**	**7 348 878,99*****	**99,98%**

* plus 139 911,61 eur financovaných z ostatných samostatných účtov (projekty NIS2 a TestCertSK)

** počet zamestnancov k 31.12.2024 (vrátane 11 obsadených tabuľkových miest na materskej a rodičovskej dovolenke)

*** plus 104 592,24 eur financovaných z ostatných samostatných účtov (projekty NIS2 a TestCertSK)

ROZPOČET NA ROK 2025

Zákonom č. 345/2024 o štátnom rozpočte na rok 2025 zo dňa 3. decembra 2024 boli schválené záväzné ukazovatele štátneho rozpočtu jednotlivých kapitol na rok 2025. V nadväznosti na bod C.1. uznesenia vlády SR č. 606 zo dňa 15. októbra 2024 k návrhu rozpočtu verejnej správy na roky 2025 až 2027 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 2025.

Výdavky úradu pre rok 2025 sú rozpočtované v rámci programu 0D9 – Bezpečnosť informácií a medzirezortného podprogramu 0EK0U – Informačné technológie financované zo štátneho rozpočtu – NBÚ v celkovej sume 17 984 619,00 eur. Príjmy úradu ako záväzný ukazovateľ sú rozpočtované v sume 20 000 eur, príjmy pod kódom zdroja 72e sú rozpočtované v sume 2 000 eur.

Rozpočtové prostriedky úrad 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

Analytici z portálu Transparex.sk každoročne zostavujú rebríček zodpovedných verejných obstarávateľov. V roku 2023 hodnotili 3 428 subjektov, vrátane ústredných orgánov štátnej správy, miest a obcí, škôl, nemocníc a ostatných štátnych organizácií a podnikov.

Národnému bezpečnostnému úradu sa opäť podarilo obhájiť titul „Veľmi zodpovedný obstarávateľ“ s celkovým výsledkom A+. So ziskom 80,1 bodov obsadil 33. miestomedzi ústrednými orgánmi štátnej správy. Z hodnotenia vyplýva, že verejné obstarávanie sa realizuje profesionálne, rýchlo, s dôrazom na výskoku hospodárnosť a zabezpečenie čestnej hospodárskej súťaže.

NÁRODNÁ KULTÚRNA PAMIATKA – KAŠTIEĽ BRUNOVCE

Národný bezpečnostný úrad má vo svojej správe renesančný kaštieľ z druhej polovice 17. storočia nachádzajúci sa v obci Brunovce v okrese 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.

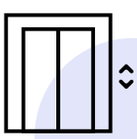
Po minulé roky bol kaštieľ v obmedzenej miere prístupný verejnosti a zároveň bol využívaný predovšetkým na služobné účely ako školiace stredisko alebo priestor na rokovania, či konferencie úradu. Kaštieľ vrátane záhrady a kaplnky sa dal využiť aj na súkromné akcie pracovníkov úradu a ostatných občanov, 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 bol zrealizovaný 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 Trenčín za účelom vydania záväzného stanoviska. Po zapracovaní všetkých pripomienok do projektovej dokumentácie bolo vydané 19. 12. 2024 záväzné stanovisko. Následne bude projektová dokumentácia postúpená príslušnému stavebnému úradu Ministerstva vnútra 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 národnej kultúrnej pamiatky, boli v zmysle povolení KPÚ Trenčín vykonané sanačné výruby, ozdravné orezy a následná výsadba nových drevín.



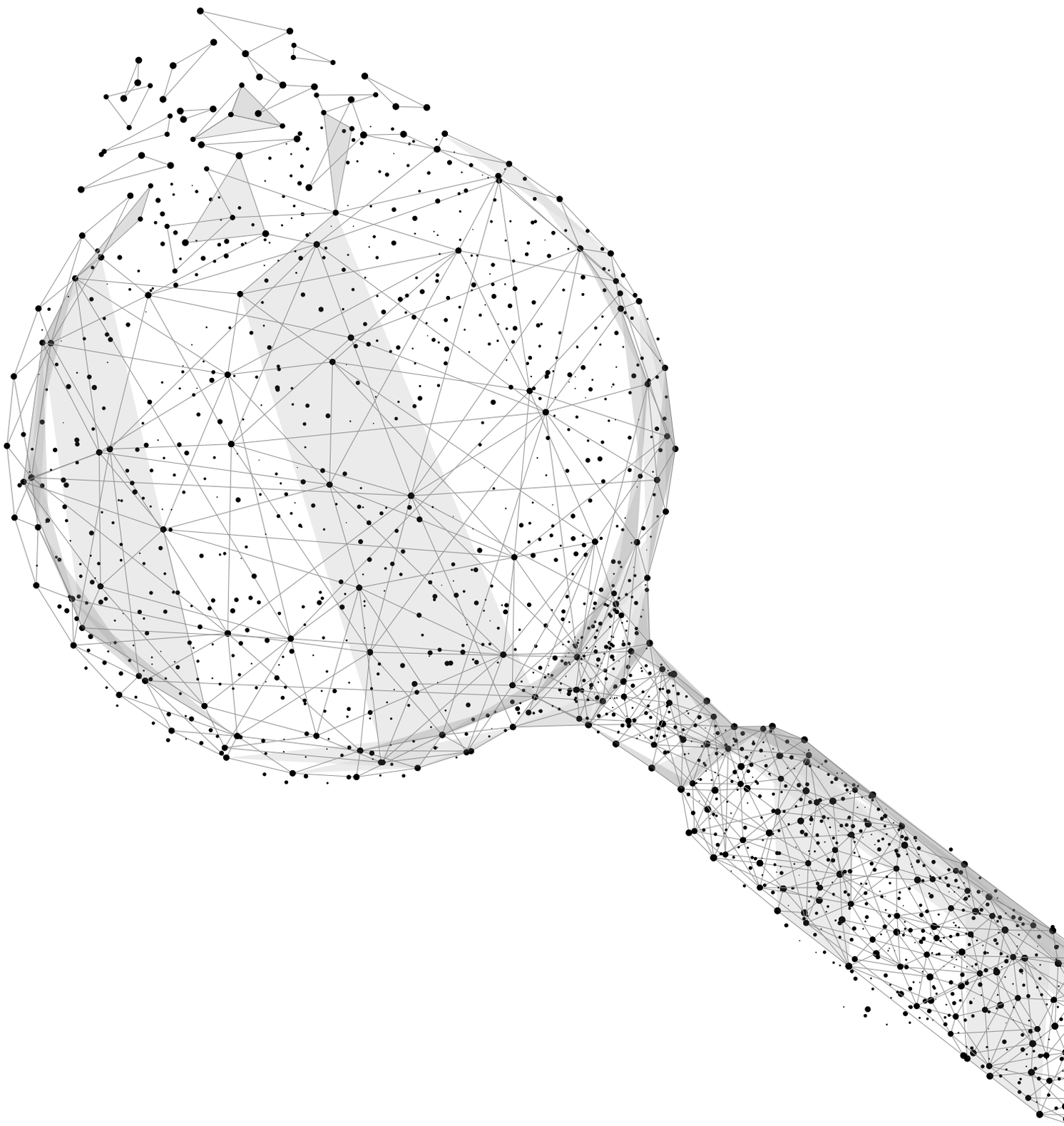
OBNOVA VÝŤAHOV

Národný bezpečnostný úrad pristúpil v roku 2024 k výmene štyroch opotrebovaných osobných výťahov značky OTAN v administratívnej budove úradu.

Dôvodom nutnej výmeny a modernizácie osobných výťahov bol ich nevyhovujúci technický stav. Výťahy boli vyrobené v roku 2004 a za posledné obdobie vykazovali neustále poruchy s nutnosťou ich odstávok, a potrebných servisných zásahov, ktoré boli ekonomicky neefektívne. Výťahy boli vymenené v zmysle vypracovanej projektovej dokumentácie, zmluvy o dielo a po ohlásení na príslušnom stavebnom úrade.

Tri nové výťahy sú štandardné s nosnosťou 630 kg /8 osôb a jeden s nosnosťou 800 kg /10 osôb, zvýšila sa aj prevádzková rýchlosť z 1 m/s na 1,75 m/s.

KONTROLA A AUDIT



KONTROLA A AUDIT KONTROLNÁ ČINNOSŤ

Úrad vykonal kontrolu naprieč všetkými úsekmi pôsobnosti zverenej zákonmi v 35 subjektoch:

- kontroly na úseku ochrany utajovaných skutočností – 16 subjektov (deväť štátnych orgánov a sedem držiteľov potvrdenia o priemyselnej bezpečnosti)
- dohľad a inšpekcia v rozsahu plnenia záväzkov vyplývajúcich z členstva v NATO – jeden subjekt
- kontroly na úseku dôveryhodných služieb – dva subjekty (jeden štátny orgán a jeden poskytovateľ kvalifikovaných dôveryhodných služieb)
- kontroly na úseku kybernetickej bezpečnosti 16 subjektov (prevádzkovateľov základných služieb – sedem orgánov verejnej moci a deväť subjektov súkromného sektora).

Kontrolné skupiny sa zamerali najmä na komplexnosť prijatých opatrení a ich koordináciu naprieč jednotlivými úsekmi. Celkovo bolo v kontrolovaných subjektoch zaznamenaných 49 kontrolných zistení:

- 33 na úseku ochrany utajovaných skutočností
- 14 na úseku kybernetickej bezpečnosti
- 2 na úseku dôveryhodných služieb

DOHĽADOVÁ ČINNOSŤ

Úrad 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 a v zákone o dôveryhodných službách.

Úrad posúdil tri správy o posúdení zhody z kontrolného auditu od dvoch kvalifikovaných poskytovateľov dôveryhodných služieb.

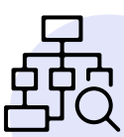
Úrad vykonal ex post dohľad u jedného kvalifikovaného poskytovateľa dôveryhodných služieb, u ktorého bol zistený nesúlad s nariadením (EÚ) č. 910/2014. Úrad zároveň v roku 2024 vykonal kontrolu u jedného kvalifikovaného poskytovateľa dôveryhodných služieb, u ktorého bolo kontrolou zistené nedodržiavanie zákona č. 272/2016.

Úrad vykonal desať zmien v poskytovaní kvalifikovanej dôveryhodnej služby a pri troch žiadostiach bolo poskytovateľovi oznámené, aby požiadal o kvalifikovaný štatút.

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 2024 vydal 143 metodických usmernení a odborných stanovísk:

NA ÚSEKU OCHRANY UTAJOVANÝCH SKUTOČNOSTÍ	**95**
PERSONÁLNA BEZPEČNOSŤ	17
ADMINISTRATÍVNA BEZPEČNOSŤ	9
PRIEMYSELNÁ BEZPEČNOSŤ	16
FYZICKÁ BEZPEČNOSŤ A OBJEKTOVÁ BEZPEČNOSŤ	4
BEZPEČNOSŤ TECHNICKÝCH PROSTRIEDKOV	12
BEZPEČNOSTNÍ ZAMESTNANCI	0
CUDZIA MOC	**1**
V OBLASTI ŠIFROVEJ OCHRANY INFORMÁCIÍ	5
NA ÚSEKU KYBERNETICKEJ BEZPEČNOSTI	33
NA ÚSEKU DÔVERYHODNÝCH SLUŽIEB	13
PRIEREZOVÉ STANOVISKÁ	33



VNÚTORNÁ KONTROLA

V roku 2024 sekcia vnútornej bezpečnosti vykonala päť kontrol podľa zákona č. 10/1996 o kontrole v štátnej správe na jednotlivých útvaroch úradu, pričom tri kontroly boli vyhodnotené v rámci protokolov o výsledku kontroly, jedna kontrola bola vyhodnotená bez kontrolných zistení a jedna kontrola prebieha. Ich predmetom bola kontrola dodržiavania základného času služby v týždni a udelenia služobného voľna, pracovného času a prekážky v práci, kontrola ochrany utajovaných skutočností za oblasť administratívnej bezpečnosti, kontrola zahraničných ciest a prijatí zahraničných delegácií, kontrola fyzickej a objektovej bezpečnosti a kontrola prevádzky služobných motorových vozidiel úradu.

VNÚTORNÝ AUDIT

V roku 2024 boli útvarom vnútorného auditu vykonané štyri plánované vnútorné audity, ktorých cieľom bolo overiť a hodnotiť:

- dodržiavanie zákona č. 10/1996 o kontrole v štátnej správe a Nariadenia riaditeľa NBÚ č. 5/2017 o previerkovej činnosti a vnútornej kontrole za rok 2023 v povinnej osobe NBÚ,
- dodržiavanie zákona č. 343/2015 o verejnom obstarávaní za rok 2023 v povinnej osobe NBÚ,
- hospodárnosť, efektívnosť, účinnosť a účelnosť pri hospodárení s verejnými financiami – prostriedky EÚ - za obdobie od 10.04.2021 – 09.07.2024 v povinnej osobe NBÚ,
- hospodárnosť, efektívnosť, účinnosť a účelnosť pri hospodárení s verejnými financiami – prostriedky ŠR - za obdobie od 10.08.2023 do 30.06.2024 v povinnej osobe NBÚ.

Vykonanými vnútornými auditmi bolo zistených päť nedostatkov. Štyri nedostatky boli strednej závažnosti, systémové – finančne nevyčísliteľné a jeden nedostatok bol nízkej závažnosti, nesystémový – finančne nevyčísliteľný.

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.

SŤAŽNOSTI A PETÍCIE

Sekcia vnútornej bezpečnosti prijala 11 sťažností, z toho tri sťažnosti boli vyhodnotené ako neopodstatnené, tri sťažnosti boli postúpené na vecné útvary úradu a päť sťažností bolo odložených záznamom.

PRIORITY NA ROK 2025

Prioritou je aj projekt Vybudovanie novej fyzickej a objektovej bezpečnosti. Okrem neho budeme pracovať aj na zintenzívnení získavania informácií o bezpečnostných rizikách týkajúcich sa pôsobnosti úradu, nastavení správneho fungovania vnútorného kontrolného systému.

NBÚ bude ďalej podporovať vzdelávanie a výcvik špecialistov na odborných kurzoch, seminároch a školeniach doma i v zahraničí s cieľom nadobúdať nové zručnosti, a prehlbovať ich kvalifikáciu. Ako najdôležitejším kurzom sa v tomto roku javí tréning pracovníkov certifikačných orgánov na štandard Common Criteria. Tento kurz sa uskutoční pod vedením pracovníkov z akreditovaného zahraničného laboratória pracujúceho v rámci certifikačných schém založených na normách ISO/IEC 15048 Common Criteria, ktorí tak odovzdajú svoje praktické skúsenosti a vedomosti technickým expertom zo Slovenska.

Úrad bude ďalej rozvíjať spôsobilosti v oblasti certifikácie mechanických zábranných, technických zabezpečovacích a technických prostriedkov, či prostriedkov šifrovej ochrany informácií a certifikácie v oblasti kybernetickej bezpečnosti

K prioritám pre rok 2025 patrí aj realizácia projektov financovaných z prostriedkov EÚ ako napríklad „Výskum a vývoj post kvantových šifrovacích algoritmov“, na ktorých sa okrem príslušníkov technickej sekcie bude podieľať aj akademická obec a to najmä zo Slovenskej akadémie vied a Fakulty elektrotechnicky a informatiky Slovenskej technickej univerzity. Projekt je primárne zameraný na praktickú aplikáciu novej generácie šifrovacích algoritmov do knižníc programovacích jazykov a vývojových prostredí. Nasledovným cieľom je potom vytvorenie a otestovanie softvéru zabezpečenej pracovnej stanice, v ktorej sa reálne nasadania nové knižnice do reálnej prevádzky a testovania bežnými užívateľmi.