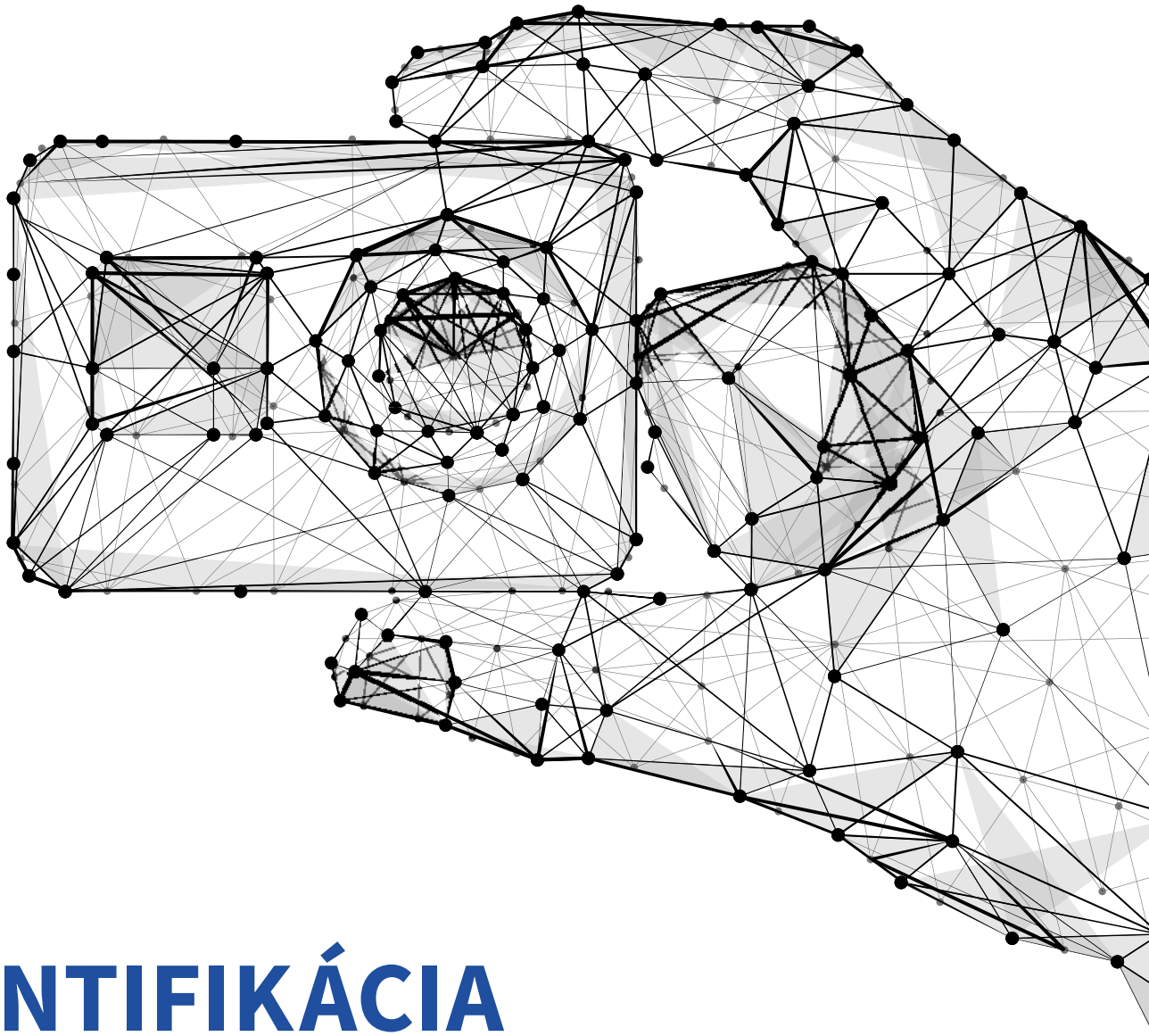
NÁRODNÝ
BEZPEČNOSTNÝ
ÚRAD

SPRÁVA O ČINNOSTI V ROKU 2023

NÁRODNÝ
BEZPEČNOSTNÝ
ÚRAD

SPRÁVA O ČINNOSTI V ROKU 2023

OBSAH

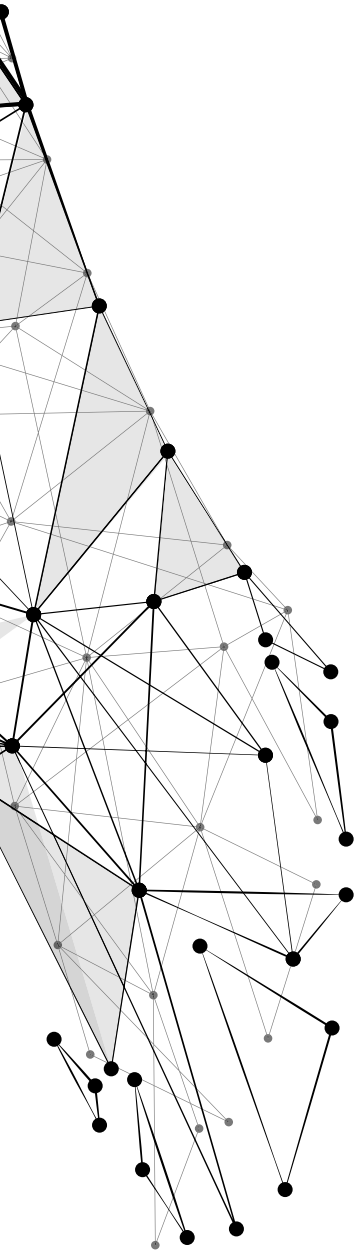


IDENTIFIKÁCIA ORGANIZÁCIE

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

Zákona č. 215/2004 o ochrane utajovaných skutočností, súvisiace vyhlášky a platné štandardy.

Zákon č. 272/2016 o dôveryhodných službách pre elektronické transakcie na vnútornom trhu.

Zákona č. 69/2018 o kybernetickej bezpečnosti a jeho vyhlášky. Príslušné a súvisiace medzinárodné, európske aj národné právne predpisy.

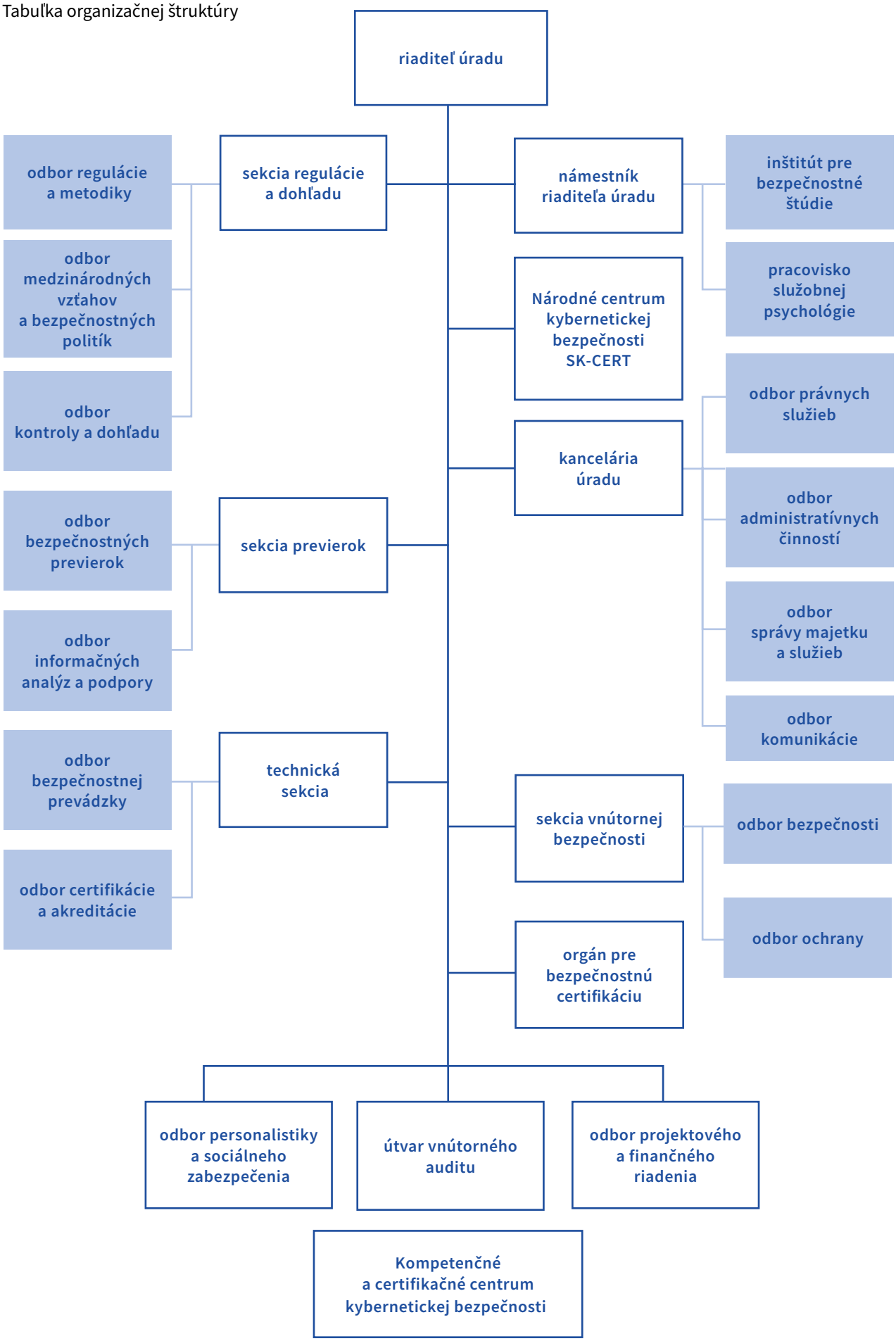
VEDENIE ÚRADU

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

Tabuľka organizačnej štruktúry



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.

Sekcia previerok

Vykoná 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.

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.

Plní úlohy v oblasti výkonu kontroly, auditu a dohľadu. Udeľuje a odníma kvalifikovaný štatút, určuje základnú službu a jej prevádzkovateľa, určuje digitálnu službu a jej poskytovateľa.

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.

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.

Technická sekcia

Technická sekcia sa skladá z odboru bezpečnostnej prevádzky a odboru certifikácie a akreditácie.

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.

Realizuje chod a prevádzku informačných a komunikačných systémov úradu, správu a prevádzku utajovaných systémov vládneho a zahraničného spojenia. Vykonáva aj bezpečnostný dohľad nad sieťovými a aplikačnými parametrami komunikačných a informačných systémov na ochranu utajovaných skutočností.

Národné centrum kybernetickej bezpečnosti SK-CERT

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, ale aj výkon analytických činností, výskumu, rozširovania bezpečnostného povedomia a vzdelávania v oblasti kybernetickej bezpečnosti a ďalšie úlohy na úseku kybernetickej bezpečnosti.

Odbor personalistiky a sociálneho zabezpečenia

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

Odbor projektového a finančného riadenia

Zabezpečuje projektové a programové riadenie v podmienkach úradu.

Útvar vnútorného auditu

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

Inštitút pre bezpečnostné štúdie

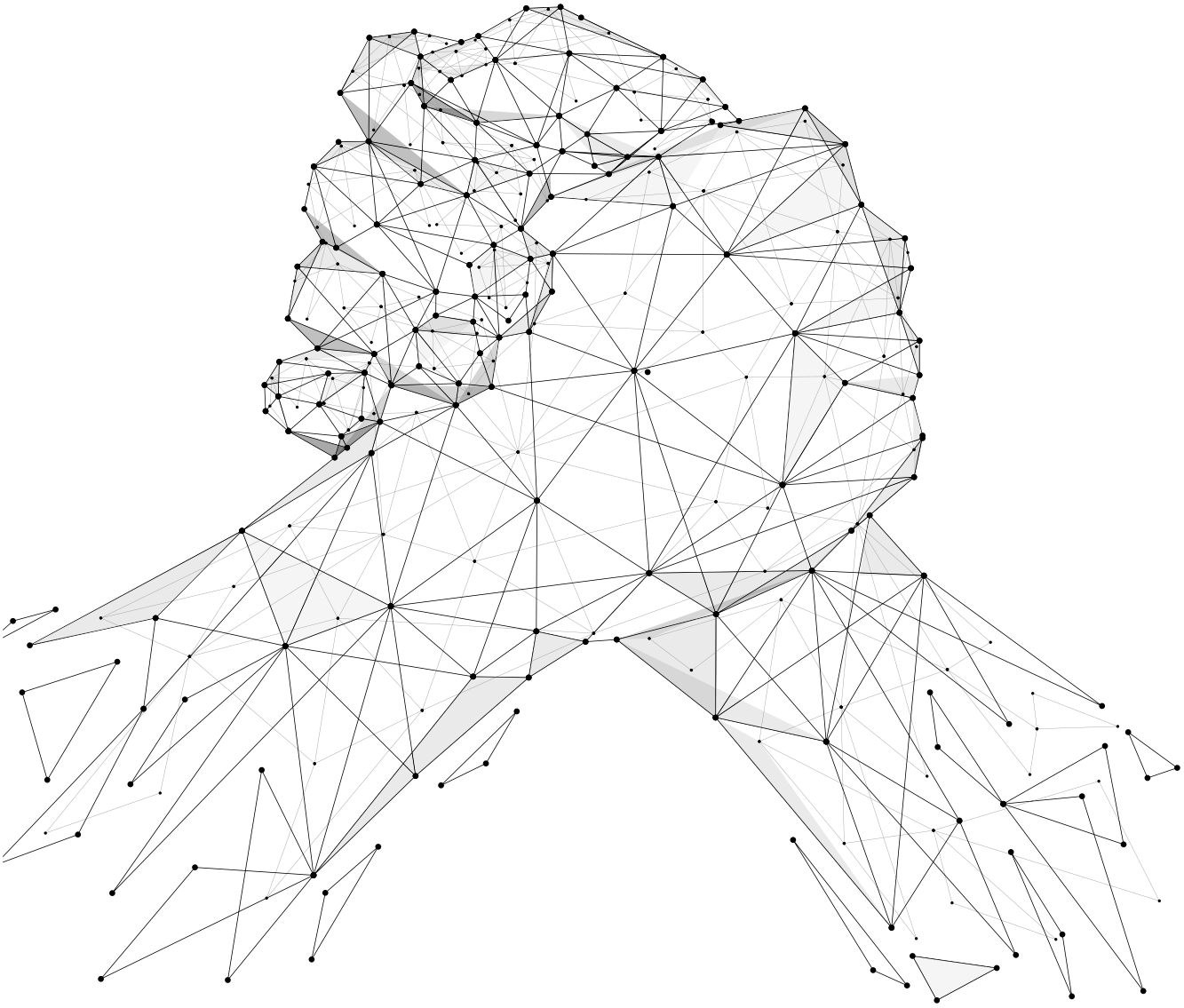
Plní úlohy na úseku všeobecnej analytiky, posudzovania bezpečnostných rizík, vyhodnocovania politík, tvorby prognóz, stratégií a implementačných plánov úradu, ako aj úlohy v oblasti boja proti hybridným hrozbám a šíreniu dezinformácií.

Orgán pre bezpečnostnú certifikáciu

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

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti 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	**37**	16,8 %				
Stála štátna služba	**176**	80 %				
Dočasná štátna služba	**7**	3,2 %				
Spolu	**220**	92,8 %	**17**	7,2 %	**237**	100 %

Veková štruktúra príslušníkov a zamestnancov

	Príslušníci		Zamestnanci		Príslušníci a zamestnanci	
do 34 rokov	46	20,9 %	4	23,5 %	50	21,1 %
35 — 49 rokov	117	53,2 %	7	41,2 %	124	52,3 %
50 — 59 rokov	48	21,8 %	3	17,7 %	51	21,5 %
60 a viac rokov	9	4,1 %	3	17,7 %	12	5,1 %
Spolu	220	90,4 %	17	9,6 %	237	100 %

Ženy a muži v NBÚ

	Príslušníci		Zamestnanci		Príslušníci a zamestnanci	
Ženy	103	94,5 %	6	5,5 %	109	46 %
Muži	117	91,4 %	11	8,6 %	128	54 %
Spolu	220	92,8 %	17	7,2 %	237	100 %

Vzdelanostná štruktúra príslušníkov a zamestnancov

Príslušníci			Zamestnanci	
0	0 %	Základné vzdelanie	0	0 %
36	16,4 %	Úplné stredné vzdelanie	7	41,2 %
8	3,6 %	Vysokoškolské vzdelanie I.st.	0	0 %
164	74,5 %	Vysokoškolské vzdelanie II.st.	10	58,8 %
12	5,5 %	Vysokoškolské vzdelanie III.st.	0	0 %
220	100 %	Spolu	17	100 %

SLUŽOBNÁ PRÍPRAVA

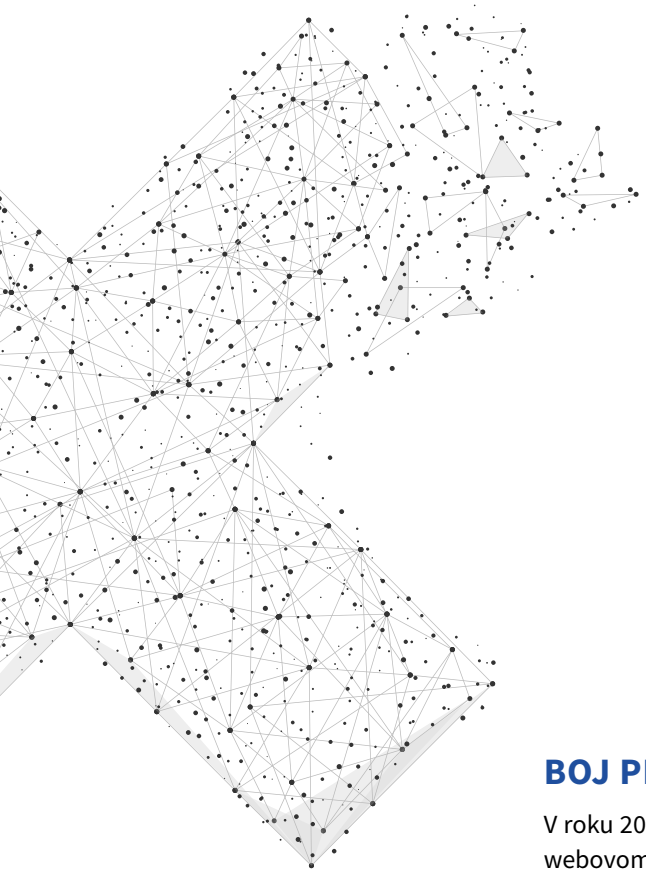
Príslušníci sekcie vnútornej bezpečnosti plnili úlohy v rámci služobnej prípravy cvičeniami v oblasti telesnej prípravy, streleckej prípravy, špeciálnej prípravy a zdravotníckej prípravy. Na streleckú a špeciálnu prípravu využívajú zariadenia ozbrojených bezpečnostných zborov, ozbrojených zborov, Slovenskej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

PRACOVISKO SLUŽOBNEJ PSYCHOLÓGIE

Služobný psychológ počas roka 2023 realizoval 59 psychologických vyšetrení žiadateľov o prijatie do služobného pomeru príslušníka NBÚ, z toho 57 z nich bolo ku koncu roka uzavretých, pričom úspešnosť žiadateľov bola 79 %. Vykonal aj 4 dopravno-psychologické vyšetrenia, 2 analýzy s cieľom zmapovať aktuálnu situáciu na vybraných útvaroch a bolo poskytnutých viac ako 140 hodín psychologického poradenstva.

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 2023 sme aktualizovali Protikorupčný program úradu, ktorý je zverejnený na webovom sídle.

V aktualizovanom programe stanovil za cieľ vzdelávanie príslušníkov a zamestnancov úradu o protikorupčnej legislatíve na národnej a medzinárodnej úrovni či vzdelávanie príslušníkov a zamestnancov úradu o interných nariadeniach úradu upravujúcich opatrenia úradu v oblasti prevencie korupcie, ktorých cieľom je vytvárať, implementovať, udržiavať, preskúmavať a zlepšovať systém riadenia protikorupčných činností na úrade v súlade s požiadavkami normy STN ISO 37001 Systémy manažérstva proti korupcii.

V roku 2023 bolo do špecializovaného vzdelávania príslušníkov úradu zaradené školenie v oblasti podávania oznámení v súvislosti s ochranou oznamovateľov podľa zákona č. 54/2019 o ochrane oznamovateľov protispoločenskej činnosti.

Úrad v oblasti prevencie korupcie posudzoval dôveryhodnosť partnerov vecného vzťahu, pričom do zmlúv so subjektmi vecných vzťahov zaviedol tzv. protikorupčnú doložku. Inicioval aj rokovania o možnostiach spolupráce úradu s tretími stranami v oblasti prevencie a v boji proti korupcii, pričom pokračovala spolupráca najmä s Úradom vlády SR a Úradom na ochranu oznamovateľov.

Opatrenia úradu v oblasti prevencie korupcie majú ambíciu monitorovať a hodnotiť nastavenie protikorupčného systému úradu s cieľom odstraňovať systémové zlyhania súvisiace s korupciou. Podozrenia z korupcie príslušníkov a zamestnancov úradu môžu občania oznamovať prostredníctvom protikorupčného e-mailu bojprotikorupcii@nbu.gov.sk zverejnenom na webovom sídle úradu. Úrad neeviduje v roku 2023 žiadne oznámenie príslušníkov alebo zamestnancov úradu v súvislosti s oznámením protispoločenskej činnosti.

Na účely zavedenia certifikovaného systému manažérstva proti korupcii podľa normy ISO 37001 spracoval v roku 2023 príslušný útvar úradu analýzu implementácie predmetného protikorupčného manažérskeho systému.

LEGISLATÍVA

Národný bezpečnostný úrad pokračoval v systematickom zbere, analýze a vyhodnocovaní informácií z činnosti útvarov úradu, zo spätnej väzby odbornej verejnosti alebo zo žiadostí o poskytnutie odborného stanoviska. Harmonizoval národnú právnu úpravu s medzinárodne uznávanými prameňmi práva.

Úrad inicioval šesť legislatívnych procesov vykonávacích predpisov **zákona č. 215/2004 o ochrane utajovaných skutočností.** Dôvodom boli najmä nové hrozby, ktoré vyplynuli z globálnych konfliktov a neustály technologický vývoj.

Návrh novej vyhlášky Národného bezpečnostného úradu o skúške bezpečnostného zamestnanca – predbežná informácia bola zverejnená v marci 2023. Cieľom návrhu je zabezpečiť vyššiu úroveň bezpečnostného povedomia u fyzických osôb, ktoré na subjektoch zodpovedajú za ochranu utajovaných skutočností alebo plnia jednotlivé úlohy na tomto úseku (úprava lehôt platnosti skúšky bezpečnostného zamestnanca, povinnosť pravidelne overovať odbornú spôsobilosť). Návrh je predmetom interného posudzovania, aby mohol byť predložený do medzirezortného pripomienkového konania.

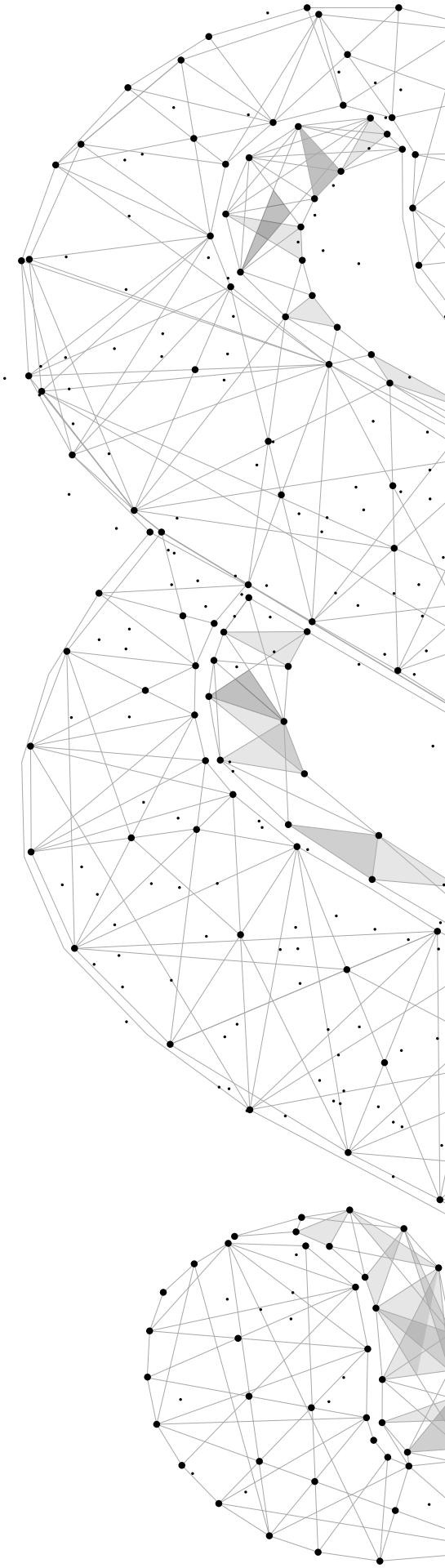
Novelizácia vyhlášky NBÚ č. 301/2013 o priemyselnej bezpečnosti a o bezpečnostnom projekte podnikateľa – predbežná informácia bola zverejnená v marci 2023. Cieľom návrhu vyhlášky je precizovať ustanovenia o potvrdeniach priemyselnej bezpečnosti podnikateľov, najmä upravujúce postup pri uznávaní potvrdení podnikateľov cudzej moci alebo opačne a podporovať tak plnenie medzinárodných zmlúv a záväzkov.

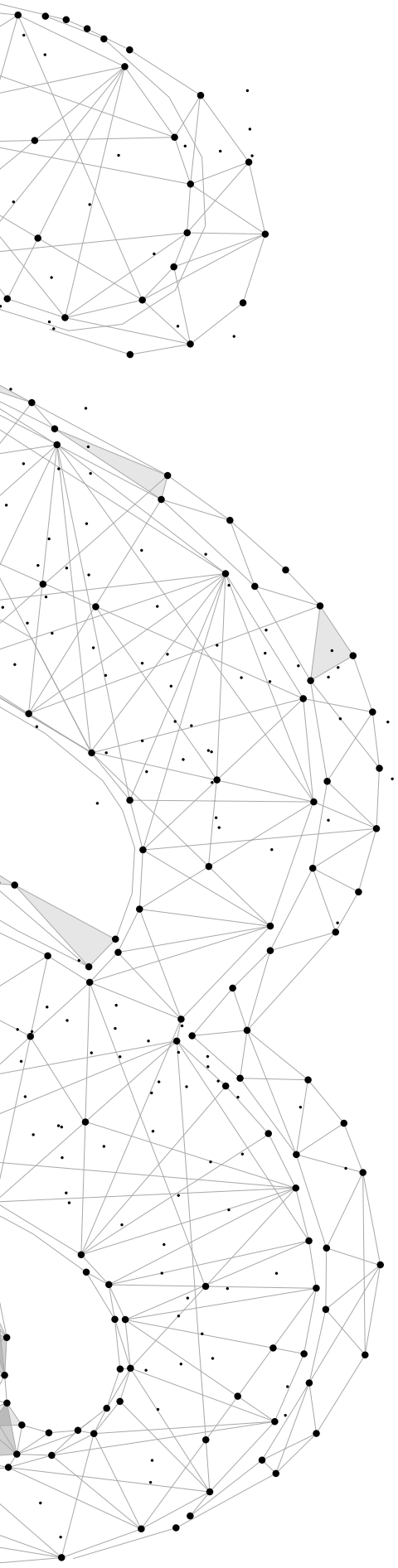
Navrhuje sa doplnenie inštitútu overovania potvrdení a postupu pri vydávaní potvrdení v prípade zmeny údajov. Úprava umožní podnikateľom reagovať na zmenu právnej formy ich podnikania. Novela je predmetom interného posudzovania, aby mohla byť predložená do medzirezortného pripomienkového konania.

Novelizácia vyhlášky NBÚ č. 134/2016 o personálnej bezpečnosti – predbežná informácia bola zverejnená v marci 2023. Cieľom návrhu vyhlášky je precizovať niektoré ustanovenia pri vykonávaní bezpečnostných previerok, ustanoviť postup pri uznávaní bezpečnostných previerok cudzinca a podrobnosti o osvedčení. Návrh novely sa priebežne upravuje, aby mohol byť predložený do medzirezortného pripomienkového konania.

Novela vyhlášky NBÚ č. 48/2019, ktorou sa upravujú podrobnosti o administratívnej bezpečnosti – predbežná informácia bola zverejnená v marci 2023. Cieľom návrhu je reagovať na zistenia vyplývajúce z aplikačnej praxe a odstrániť nejasnosti brániace jednoznačnému výkladu alebo spôsobujúce prekážky pri dosahovaní účelu, ktorým je zabezpečenie dostatočnej sledovateľnosti manipulácie s utajovanými skutočnosťami.

V súlade s predpismi EÚ a NATO a s ohľadom na spôsobenú ujmu pri neoprávnenej manipulácii sa navrhuje zníženie administratívnej záťaže pri manipulácii s utajovanými skutočnosťami stupňa utajenia Vyhradené.





Nová bezpečnostná situácia, ktorá vznikla na východnej hranici Slovenskej republiky vo februári 2022, bola podnetom na administratívne zabezpečenie ochrany osobitnej kategórie utajovaných skutočností (napríklad výrobok obranného priemyslu, strelivo a pod.). Návrh precizuje aj inštitút neoprávnenej manipulácie, ktorý nie je dostatočne upravený v aktuálnej právnej úprave.

Návrh novely právneho predpisu sa priebežne upravuje, aby mohol byť predložený do medzirezortného pripomienkového konania.

Novelizácia vyhlášky NBÚ č. 336/2004 o fyzickej bezpečnosti a objektovej bezpečnosti – predbežná informácia bola zverejnená v marci 2023. Cieľom je doplniť do bezpečnostného štandardu bodové ohodnotenie za využitie certifikovaných prostriedkov šifrovej ochrany informácií na ochranu utajovaných skutočností pri ich ukladaní namiesto ich ukladania v bezpečnostnom úschovnom objekte.

V súlade s právnou úpravou EÚ a NATO sa do slovenskej právnej úpravy doplní administratívna zóna ako špecifický druh chráneného priestoru kategórie Vyhradené. Navrhuje sa doplniť možnosť ukladať utajované skutočnosti stupňa Vyhradené v uzamykateľnom nábytku v chránenom priestore vrátane možnosti započítania bodového ohodnotenia za takéto uloženie.

Upraví sa aj bezpečnostná dokumentácia fyzickej bezpečnosti a objektovej bezpečnosti objektov a chránených priestorov kategórie Dôverné spočívajúca v rozšírení obsahových náležitostí na úroveň bezpečnostnej dokumentácie objektov a chránených priestorov kategórie Tajné a Prísne tajné.

V procese prípravy uvedeného návrhu bol na základe neodkladnej požiadavky Ministerstva obrany Slovenskej republiky zrealizovaný skrátený legislatívny proces k urgentnej novelizácii vyhlášky Národného bezpečnostného úradu č. 336/2004 o fyzickej bezpečnosti a objektovej bezpečnosti.

Išlo o neodkladné doplnenie výnimky iba v súvislosti s ochranou výrobkov obranného priemyslu, zbraní, zbraňových systémov alebo streliva, ktoré sú buď utajovanou skutočnosťou alebo obsahujú utajované skutočnosti postúpené Slovenskej republike cudzou mocou. Ministerstvo obrany Slovenskej republiky dlhodobo deklaruje problémy s aplikáciou platnej legislatívy v súvislosti s modernizáciou ozbrojených síl.

Požadované zmeny si vyžadujú rozsiahlu novelizáciu viacerých právnych predpisov. Urgentná novelizácia (vyhláška Národného bezpečnostného úradu č. 233/2023) nadobudla účinnosť 27. 6. 2023.

Proces k novému nariadeniu vlády Slovenskej republiky, ktorým sa ustanovujú oblasti utajovaných skutočností – v júli 2023 bol predložený do medzirezortného pripomienkového konania. Hlavným zámerom navrhovaného nariadenia je aktualizovať oblasti utajovaných skutočností v Slovenskej republike, a tým reagovať na potreby štátu a jeho chránené záujmy.

Zámerom je aj ustanoviť mechanizmus regulácie orgánov verejnej moci pri určovaní stupňov utajenia a v súlade s predpismi EÚ a NATO zabezpečiť prehodnotenie určovania najnižšieho stupňa utajenia utajovaným skutočnostiam (Vyhradené), pretože

neoprávnenou manipuláciou s nimi môže dôjsť „len“ k poškodeniu právom chránených záujmov právnickej osoby alebo fyzickej osoby.

Podobne ako v roku 2022 sa potvrdil paradox, že ostatné orgány verejnej moci požadujú sprísnenie ochrany utajovaných skutočností stupňa utajenia Vyhradené.

Ďalšou legislatívnou aktivitou úradu v roku 2023 bol inicializovaný proces dvoch vykonávacích predpisov k **zákonu č. 69/2018 o kybernetickej bezpečnosti.**

Novela vyhlášky NBÚ č. 165/2018, ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov – predbežná informácia bola zverejnená vo februári 2023.

Cieľom novely je jasné vymedzenie kritérií na identifikáciu závažných kybernetických bezpečnostných incidentov. Vyhláškou sa zavádza štandardizovaný systém hodnotenia zraniteľností predstavujúci jednotný spôsob, ktorý slúži na vyjadrenie technických vlastností zraniteľností v hardvéri, softvéri, firmvéri a číselné ohodnotenie ich závažnosti. Novelu momentálne posudzujeme interne.

Novela vyhlášky Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (vyhláška NBÚ č. 264/2023) nadobudla účinnosť 1. septembra 2023.

Cieľom novely je vytvorenie funkčného legislatívneho rámca nevyhnutného pre efektívnu realizáciu kľúčových opatrení pre bezpečnosť národného kybernetického priestoru transponujúceho priority a požiadavky, ktoré boli vytvorené na európskej úrovni. Tento rámec sa zameriava na rozšírenie obsahu bezpečnostných opatrení, obsah a štruktúru bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.

Ministerstvo spravodlivosti Slovenskej republiky predložilo do medzirezortného pripomienkového konania návrh novelizácie **vyhlášky Ministerstva spravodlivosti Slovenskej republiky č. 228/2018, ktorou sa vykonáva zákon č. 382/2004 o znalcoch, tlmočníkoch a prekladateľoch.**

Úrad si uplatnil zásadnú pripomienku a požadoval doplniť odvetvie kybernetická bezpečnosť do Zoznamu znaleckých odborov a odvetví, ďalej do Obsahového vymedzenia znaleckých odborov a odvetví a tiež do Zoznamu odborov a odvetví, v ktorých je podmienkou zápisu do zoznamu úspešné absolvovanie špecializovaného vzdelávania. Pripomienka bola akceptovaná a novela (vyhláška Ministerstva spravodlivosti Slovenskej republiky č. 160/2023) nadobudla účinnosť 1. júla 2023.

Okrem uvedených úloh na úseku legislatívy úrad pripomienkuje a vypracúva stanoviská k návrhom legislatívnych a nelegislatívnych materiálov v medzirezortnom pripomienkovom konaní. Úrad posúdil 700 pripomienkových konaní.

SPRÁVNE A PRIESTUPKOVÉ KONANIE

NBÚ evidoval 18 podaní vo veci podozrenia z priestupku na úseku ochrany utajovaných skutočností podľa zákona č. 215/2004 o ochrane utajovaných skutočností.

1 prípad = bola predložená správa o výsledku objasňovania priestupku po zistení páchateľa priestupku príslušnému správnemu orgánu

1 prípad = vec, ktorá sa týkala 1 skutku z 2 skutkov podania odovzdaná príslušnému orgánu;

7 prípadov = útvar objasňujúci priestupok vec odložil záznamom a v 10 prípadoch = vec sa naďalej objasňuje.

V roku 2023 sme zaevidovali 17 oznámení o neoprávnenej manipulácii s utajovanou skutočnosťou.

Vec evidovanú ako neoprávnenú manipuláciu s utajovanou skutočnosťou v 2 prípadoch vyšetruje príslušný orgán činný v trestnom konaní.

ZMLUVY O POSTUPOVANÍ UTAJOVANÝCH SKUTOČNOSTÍ

Úrad má celkovo uzatvorených 13 zmlúv o prístupe podnikateľa k utajovaným skutočnostiam, vlani uzatvoril 1 zmluvu a 4 dodatky 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.

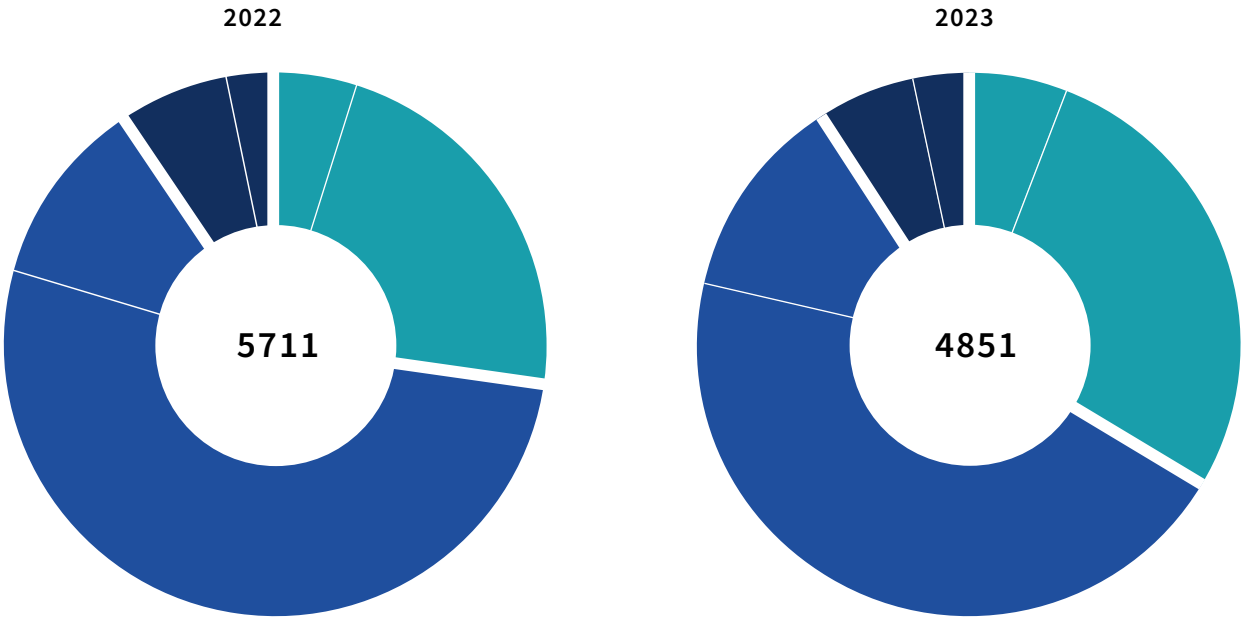
Okrem osvedčení a potvrdení, ktoré umožňujú prístup k národným utajovaným skutočnostiam, zabezpečuje vydávanie certifikátov o bezpečnostnej previerke fyzickej osoby a certifikátov podnikateľa o priemyselnej bezpečnosti pre oboznamovanie sa s utajovanými skutočnosťami NATO a EÚ a vyjadruje sa o navrhovaných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

PERSONÁLNA BEZPEČNOSŤ

Národný bezpečnostný úrad vydal **4 851 osvedčení** na oboznamovanie sa s utajovanými skutočnosťami, **z toho 2 757 pre rezort obrany**.

Prehľad osvedčení vydaných v rokoch 2022 a 2023

Stupeň utajenia	2022	2023
DÔVERNÉ	**1570**	**1639**
z toho Dôverné pre MO SR	279	290
TAJNÉ	**3614**	**2771**
z toho Tajné pre MO SR	2985	2181
PRÍSNE TAJNÉ	**527**	**441**
z toho Prísne tajné pre MO SR	355	286
Spolu	**5711**	**4851**



NBÚ vydal 31 rozhodnutí. Proti rozhodnutiu úradu podali fyzické osoby 13 odvolaní.

V dvoch odvolaniach rozhodol úrad autoremedúrou. Výbor Národnej rady Slovenskej republiky na preskúmanie rozhodnutí Národného bezpečnostného úradu rozhodol o 13 odvolaniach, sedem odvolaní zamietol, dve rozhodnutia úradu zrušil v odvolacom konaní a dve rozhodnutia zrušil následkom rozhodnutia Najvyššieho správneho súdu Slovenskej republiky. K 31. 12. 2023 bolo v odvolacom procese jedno odvolanie. Jedno odvolanie nebolo úradom akceptované.

Proti rozhodnutiu výboru nebola na najvyššom správnom súde podaná žiadna žaloba. Najvyšší správny súd rozhodol v roku 2023 spolu o siedmich žalobách – z toho tri

žaloby zamietol, zrušil dve rozhodnutia výboru spolu s rozhodnutím úradu a zrušil dve rozhodnutia úradu.

Na Ústavnom súde Slovenskej republiky boli podané dve ústavné sťažnosti. Ústavný súd jednu sťažnosť odmietol.

Rozhodnutia úradu, odvolania fyzických osôb proti rozhodnutiam úradu a žaloby v rokoch 2022 a 2023

	2022	2023
ROZHODNUTIA ÚRADU	**47**	**31**
ODVOLANIA	**16**	**13**
Odvolania – autoremedúra (OA)	2	2
Odvolania zamietnuté výborom (OZ)	15	7
Rozhodnutia zrušené výborom (RZ)	3	4
Podané žaloby na najvyššom súde (NS)	6	0

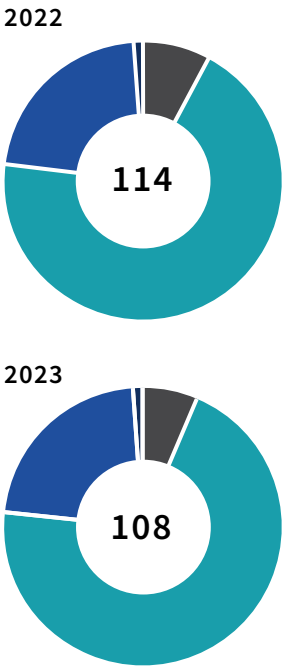
Navrhovaným osobám bolo v roku 2023 vydaných **8 699 certifikátov – z toho 4 369 certifikátov NATO a 4 330 certifikátov EÚ**. Z celkového počtu certifikátov NATO **úrad vydal 40 certifikátov NATO ATOMAL**, ktoré oprávňujú na prístup k informáciám o strategickom jadrovom odstrašovaní NATO a vydávajú sa úzkemu okruhu osôb.

PRIEMYSELNÁ BEZPEČNOSŤ

V roku 2023 vydal úrad 108 potvrdení o priemyselnej bezpečnosti – z toho 7 potvrdení stupňa utajenia Vyhradené, 76 potvrdení stupňa utajenia Dôverné, 24 potvrdení stupňa utajenia Tajné a 1 potvrdenie stupňa utajenia Prísne tajné.

Prehľad potvrdení o priemyselnej bezpečnosti vydaných v rokoch 2021 a 2022

Stupeň utajenia	2022	2023
VYHRADENÉ	**9**	**7**
DÔVERNÉ	**79**	**76**
TAJNÉ	**25**	**24**
PRÍSNE TAJNÉ	**1**	**1**
Spolu	**114**	**108**



V roku 2023 úrad vydal 12 rozhodnutí. Proti rozhodnutiu úradu podali podnikatelia 4 odvolania.

Úrad nerozhodol o žiadnom odvolaní autoremedúrou. Výbor jedno odvolanie zamietol a zrušil jedno rozhodnutie. K 31.12.2023 sú v odvolacom procese dve odvolania.

Na najvyššom správnom súde nebola v roku 2023 podaná žiadna žaloba. Najvyšší správny súd zamietol jednu žalobu a zrušil jedno rozhodnutie.

Na Ústavnom súde Slovenskej republiky nebola podaná žiadna sťažnosť.

Vo vzťahu k utajovaným skutočnostiam NATO a EÚ bolo v roku 2023 podnikateľom vydaných **16 certifikátov NATO** a **14 certifikátov EÚ**, ktoré oprávňujú podnikateľov oboznamovať sa s utajovanými skutočnosťami NATO a/alebo EÚ.

Rozhodnutia úradu, odvolania podnikateľov proti rozhodnutiam úradu a žaloby v rokoch 2021 a 2022

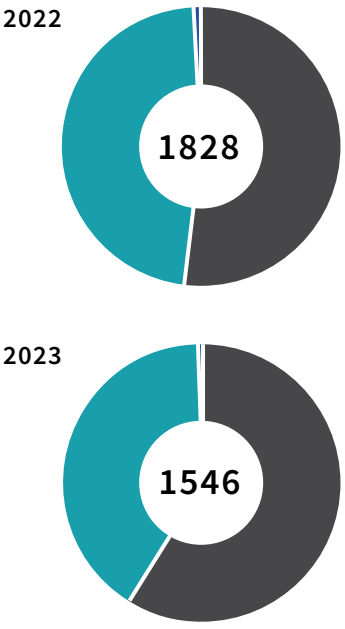
	2022	2023
ROZHODNUTIA ÚRADU	**13**	**12**
ODVOLANIA	**4**	**4**
Odvolania – autoremedúra (OA)	2	0
Odvolania zamietnuté výborom (OZ)	2	1
Rozhodnutia zrušené výborom (RZ)	0	1
Podané žaloby na najvyššom súde (NS)	0	0

VÝMENA UTAJOVANÝCH SKUTOČNOSTÍ

V roku 2023 úrad prijal a odoslal 1 546 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.

Stupne utajenia utajovaných skutočností

Stupeň utajenia	2022	2023
VYHRADENÉ	**950**	**912**
DÔVERNÉ	**867**	**631**
TAJNÉ	**11**	**3**
PRÍSNE TAJNÉ	**0**	**0**
Spolu	**1828**	**1546**

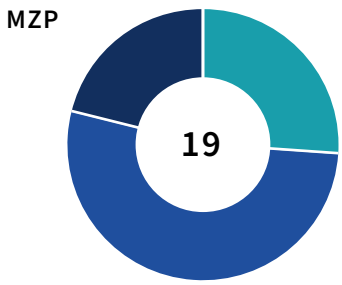


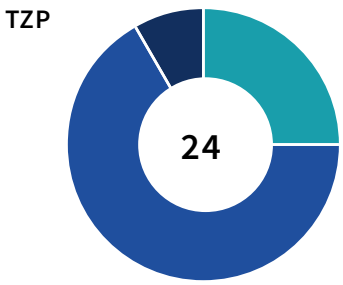
FYZICKÁ BEZPEČNOSŤ A OBJEKTOVÁ BEZPEČNOSŤ

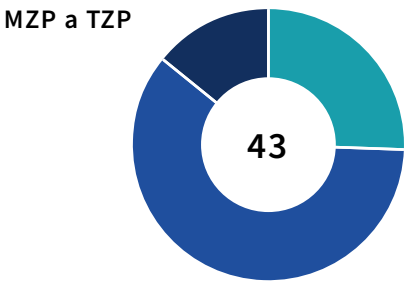
NBÚ vydal **43 certifikátov** mechanických zábranných a technických zabezpečovacích prostriedkov.

Stupne utajenia vydaných certifikátov

Stupeň utajenia	MZP	TZP	MZP a TZP
VYHRADENÉ	0	0	0
DÔVERNÉ	5	6	11
TAJNÉ	10	16	26
PRÍSNE TAJNÉ	4	2	6
Spolu	19	24	43





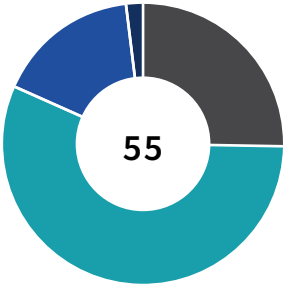


BEZPEČNOSŤ TECHNICKÝCH PROSTRIEDKOV

Úrad vydal **55 certifikátov** technických prostriedkov a **23 dodatkov k vydaným certifikátom** technických prostriedkov.

Stupne utajenia vydaných certifikátov

Stupeň utajenia	TP
VYHRADENÉ	14
DÔVERNÉ	31
TAJNÉ	9
PRÍSNE TAJNÉ	1
Spolu	55



AKREDITÁCIA KOMUNIKAČNÝCH A INFORMAČNÝCH SYSTÉMOV

Národný bezpečnostný úrad vykonal 2 akreditácie komunikačných a informačných systémov BICES SVK ELEMENT, SVK DEKMS v súlade s Bezpečnostnou politikou NATO C-(2002)49-REV1 a 2 akreditácie komunikačných a informačných systémov SVK EU DELEGATES PORTAL-R a SVK EU CORTESY v súlade s Rozhodnutím rady (2013/488/EÚ).

OCHRANA PRED NEŽIADUCIM ELEKTROMAGNETICKÝM VYŽAROVANÍM

Na zabezpečenie ochrany utajovaných skutočností pred únikom cez nežiaduce elektromagnetické vyžarovanie vykonávali príslušníci úradu zónové merania chránených priestorov (mobilnou meracou aparatúrou).

V danom období neboli vykonané žiadne merania NEV zariadení technických prostriedkov (TP) a prostriedkov šifrovej ochrany informácií (PŠOI) v špecializovanom TEMPEST laboratóriu, z dôvodu nefunkčnosti meracej techniky v laboratóriu TEMPEST.

Laboratóriu TEMPEST bolo doručených 38 žiadostí na meranie – na ich základe technici vykonali 92 zónových meraní priestorov a kategorizovali 101 miestností.

Boli prijaté aj **2 žiadosti o vykonanie technických bezpečnostných prehliadok** priestorov a motorových vozidiel, na základe ktorých bolo vykonaných **14 prehliadok miestností a 18 prehliadok služobných motorových vozidiel**.

BEZPEČNOSTNÉ POVEDOMIE

Šírenie bezpečnostného povedomia v oblasti ochrany utajovaných skutočností sa okrem aktívnej vonkajšej komunikácie úradu spravidla uplatňuje skúškami bezpečnostných zamestnancov a odbornými školeniami. Skúšky a preškolenia úrad vykonáva formou on-line testu cez video.

V roku 2023 bolo na testy pozvaných 486 uchádzačov – skúšku úspešne vykonalo 292 uchádzačov, 95 uchádzačov bolo neúspešných a zvyšok sa na skúške nezúčastnil.

Na preškolení sa zúčastnilo celkovo 139 uchádzačov –úspešne ho absolvovalo 127 uchádzačov, zvyšný počet sa na skúške nezúčastnil.

Na žiadosť držiteľa potvrdenia o úspešnom vykonaní skúšky boli vydané štyri nové potvrdenia o absolvovaní skúšky (tzv. „duplikát“).

Na základe vykonávacieho protokolu o vzájomnej spolupráci pri výkone skúšok bezpečnostného zamestnanca a preškoľovania uzatvoreného medzi ministerstvom vnútra a úradom boli vykonané dve kontroly dodržiavania tohto protokolu.

Prednášková činnosť je realizovaná najmä v spolupráci s Inštitútom pre verejnú správu a je určená pre verejný i súkromný sektor. V roku 2023 boli prednášky rozšírené o tému Zákon o ochrane utajovaných skutočností.

Úrad vyhodnocuje aj spätnú väzbu z týchto podujatí, aby dostatočne reflektoval potreby odbornej verejnosti.

ŠIFROVÁ OCHRANA INFORMÁCIÍ

CERTIFIKÁCIA

Systém šifrovej ochrany funguje na štruktúre rezortných šifrových orgánov a ich úzkej spolupráci s úradom, ktorý plní rolu ústredného šifrového orgánu.

Predmetom vzájomnej komunikácie boli v roku 2023 najmä oblasti certifikácie prostriedkov šifrovej ochrany informácií, vydávanie dodatkov k pravidlám na používanie prostriedkov šifrovej ochrany informácií a otázky ohľadom možností uznávania a preberania zahraničných certifikátov.

Úrad vydal 8 certifikátov prostriedkov šifrovej ochrany informácií.

Stupne utajenia vydaných certifikátov

Stupeň utajenia	TP
VYHRADENÉ	2
DÔVERNÉ	2
TAJNÉ	4
PRÍSNE TAJNÉ	0
Spolu	8

2022

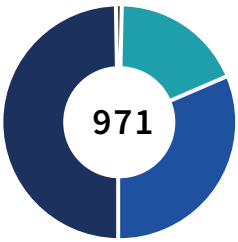
ZABEZPEČENÁ INFRAŠTRUKTÚRA

Úrad pokračoval v distribúcii prostriedkov určených na bezpečnú výmenu informácií medzi vládnymi inštitúciami v režime stupňa utajenia Vyhradené, Dôverné a Tajné. NBÚ zabezpečoval ochranu videokonferencií a prenosu informácií pre členov vlády.

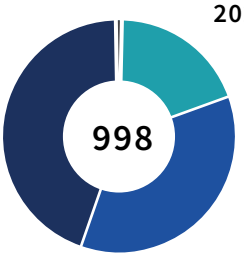
V hodnotenom období sa podarilo zvýšiť bezpečnosť a prevádzkovú spoľahlivosti týchto systémov použitím nových technológií prostriedkov šifrovej ochrany informácií. Pre udržateľnosť plnenia stanovených cieľov sme realizovali výcvik personálu zameraný na získanie a rozvoj odborných spôsobilostí pre správu informačných systémov, spôsobilostí zabezpečujúcich ochranu informačných systémov, webových služieb, technických prostriedkov a prostriedkov šifrovej ochrany informácií v správe NBÚ.

V roku 2023 úrad v podmienkach zabezpečenej infraštruktúry priamo prevádzkoval 6 systémov so šifrovou ochranou informácií, prevádzkoval alebo poskytoval podporu pre 482 koncových zariadení a poskytoval služby a podporu pre 2 088 používateľov, pričom v hodnotenom období celkovo evidujeme 1 510 vybavených požiadaviek od týchto používateľov. Zároveň sme priebežne zabezpečovali operatívne požiadavky rezortov a poskytovali podporu pri výrobe a distribúcii šifrového materiálu.

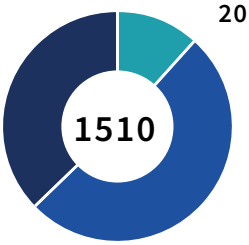
2021



2022



2023



Zabezpečená infraštruktúra

Stupeň utajenia	2021	2022	2023
SYSTÉMY	5	6	6
KONCOVÉ ZARIADENIA	360	433	482
POUŽÍVATEĽSKÉ ÚČTY	621	805	2088
POŽIADAVKY	971	998	1510

DÔVERYHODNÉ SLUŽBY

Rada Európskej únie prijala spoločnú pozíciu k návrhu revízie **nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu** (eIDAS).

Revízia má za cieľ univerzálny prístup k bezpečnej a dôveryhodnej elektronickej identifikácii a autentifikácii cez európsku peňaženku digitálnej identity na mobilnom telefóne, cez ktorú si osoba získa svoje potvrdenie (elektronické osvedčenia atribútov) a z potvrdení vie zaslať spoliehajúcej sa strane (napr. požičovňa auta) len potrebné údaje.

Proces oznamovania, prostredníctvom ktorého spoliehajúca sa strana oznamuje svoj zámer spoliehať sa na peňaženku, by mal byť nákladovo efektívny, primeraný riziku a malo by sa ním zabezpečiť, aby spoliehajúca sa strana poskytla aspoň informácie potrebné na autentifikáciu prístupu do peňaženky. Rada navrhuje, aby sa vykonávacie obdobie stanovené na 24 mesiacov počítalo od prijatia vykonávacích aktov.

Úrad na úrovni expertnej eIDAS skupiny pripravuje podklady a aktívne sa zúčastňuje na prácach, ktoré definujú postupy podľa článku 45d. Členské štáty v tom prípade zabezpečia, aby sa prijali opatrenia, ktoré kvalifikovaným poskytovateľom elektronických osvedčení atribútov umožnia na žiadosť používateľa elektronickými prostriedkami overiť pravosť týchto atribútov.

Overenie bude na základe príslušného autentického zdroja na vnútroštátnej úrovni alebo cez určených sprostredkovateľov uznaných na vnútroštátnej úrovni v súlade s vnútroštátnym právom alebo právom Únie a v prípadoch, keď sa tieto atribúty opierajú o autentické zdroje vo verejnom sektore.

Dôveryhodná infraštruktúra

	2022	2023
CERTIFIKÁTY	122 357	219 248

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 priebehu roka 2023 úrad publikoval dôveryhodné zoznamy č. 100 až 113.

ZOZNAM OPRÁVNENÍ

Zoznam oprávnení, ktorý je informačným zdrojom pre kvalifikovaných poskytovateľov dôveryhodných služieb pre vydávanie mandátnych certifikátov, zverejňuje úrad na svojom webovom sídle.

V roku 2023 bolo na základe žiadostí štátnych orgánov a orgánov územnej samosprávy do zoznamu zapísaných osem nových oprávnení a boli aktualizované viaceré existujúce oprávnenia.

V priebehu roka úrad publikoval osem verzií zoznamu oprávnení. Jeho aktuálna verzia bola vždy doplnená archívom predchádzajúcich verzií.

NOVÉ DÔVERYHODNÉ SLUŽBY

Úrad prijal oznámenie štyroch kvalifikovaných poskytovateľov o zámere poskytovať kvalifikovanú dôveryhodnú službu.

Celkovo bolo udelených osem kvalifikovaných štatútov na kvalifikovanú dôveryhodnú službu. V roku 2023 bolo kvalifikovanými poskytovateľmi dôveryhodných služieb predložených orgánu dohľadu päť správ o posúdení zhody vykonaných orgánom posudzovania zhody do 24 mesiacov od vykonania posledného auditu, ktoré potvrdzujú, že kvalifikovaní poskytovatelia dôveryhodných služieb a kvalifikované dôveryhodné služby, ktoré poskytujú, spĺňajú požiadavky stanovené v nariadení Európskeho parlamentu a Rady (EÚ) č. 910/2014.

U jedného kvalifikovaného poskytovateľa dôveryhodných služieb bolo zastavené konanie na udelenie dvoch kvalifikovaných štatútov z dôvodu nesplnenia požiadaviek nariadenia.

TVORBA MEDZINÁRODNÝCH NORIEM

Pri tvorbe medzinárodných technických noriem použiteľných pre implementáciu nariadenia eIDAS bol príslušník úradu súčasťou expertných skupín Európskej komisie, ktoré analyzujú riešenia a stanú sa základom prípravy implementačných aktov k peňaženke digitálnej identity po prijatí revízie nariadenia eIDAS.

CERTIFIKÁCIA

V roku 2023 technická sekcia nedostala žiadnu žiadosť o certifikáciu bezpečného produktu pre kvalifikovaný elektronický podpis.

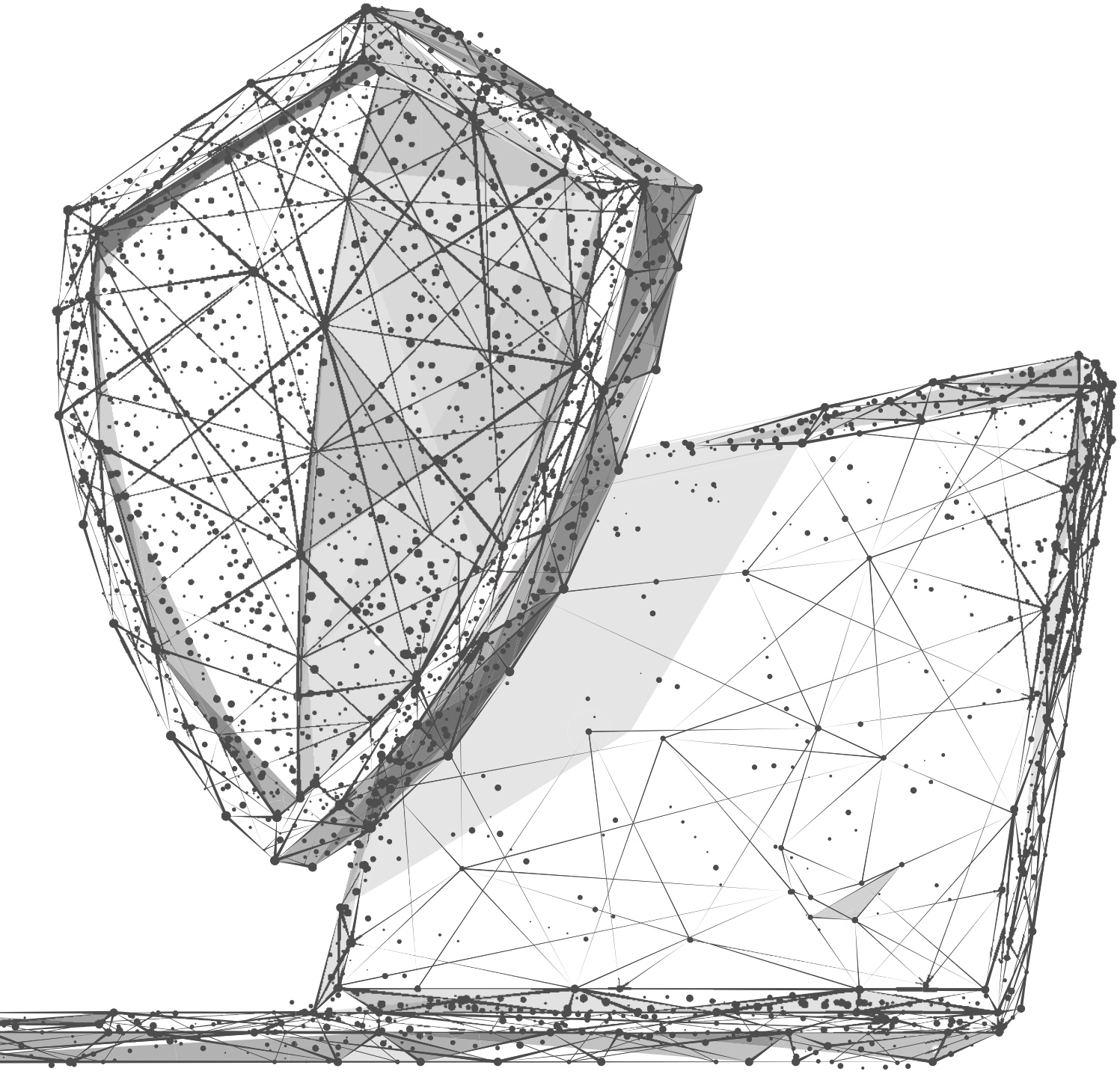
Kvalifikovaní poskytovatelia dôveryhodných služieb využívajú zariadenia na vyhotovenie kvalifikovaného elektronického podpisu alebo zariadenia na vyhotovenie kvalifikovanej elektronickej pečate už certifikované v inej krajine Európskej únie, ktoré sú zverejnené v zozname zariadení certifikovaných Európskou úniou.

DÔVERYHODNÁ INFRAŠTRUKTÚRA

Úrad prevádzkuje v dôveryhodnej infraštruktúre Koreňovú certifikačnú autoritu Slovenskej republiky, ktorá vydáva certifikáty verejných kľúčov a vedie dlhodobú databázu vydaných kvalifikovaných certifikátov s ich stavom platnosti, vydaných poskytovateľmi, ktorým úrad udelil kvalifikovaný štatút.

Za rok 2023 evidujeme celkovo 219 248 certifikátov.

KYBERNETICKÁ BEZPEČNOSŤ



Národný bezpečnostný úrad prostredníctvom Národného centra kybernetickej bezpečnosti (NCKB SK-CERT) rozvíja svoje spôsobilosti pri zabezpečovaní otvoreného, bezpečného a chráneného národného kybernetického priestoru. NCKB prijíma hlásenia o kybernetických bezpečnostných incidentoch, analyzuje ich, vyhodnocuje, vykonáva dohľad a koordinuje ich riešenie.

Vykonáva bezpečnostný monitoring za účelom zberu informácií o kybernetických bezpečnostných incidentoch z rôznych zdrojov špecializovanými nástrojmi na dohľadovom centre. Zároveň distribuuje varovania a zvyšuje tým úroveň prevencie.

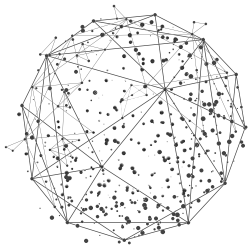
Činnosť NCKB sa na operatívnej úrovni v roku 2023 zameriavala najmä na aktivity súvisiace s kybernetickou bezpečnosťou prevádzkovateľov základných služieb vrátane prvkov kritickej infraštruktúry. Okrem tvorby varovaní úrad zdieľal relevantné informácie s partnermi na základe medzinárodnej spolupráce a vlastnej činnosti, vyplývajúcej z analýzy hlásených a zaznamenaných incidentov.

Počet hlásených kybernetických bezpečnostných incidentov v roku 2023

	Jan	Feb	Mar	Apr	Máj	Jún	Júl	Aug	Sep	Okt	Nov	Dec
Bankovníctvo	6	17	10	7	6	6	4	6	3	1	8	3
Doprava	0	0	2	1	0	0	0	2	2	0	1	0
Digitálna infraštruktúra	0	0	0	1	0	1	0	0	1	0	1	0
Elektronické komunikácie	0	0	0	0	3	0	1	0	0	0	1	0
Energetika	0	0	0	0	0	0	1	0	0	0	1	0
Infraštruktúra finančných trhov	0	0	0	0	0	0	0	0	0	0	0	0
Pošta	0	2	2	1	1	0	1	2	0	3	0	0
Priemysel	0	0	0	0	0	0	0	1	0	0	1	0
Voda a atmosféra	0	0	0	0	0	0	0	0	0	0	0	0
Verejná správa	39	55	53	28	45	29	22	39	45	44	51	28
Zdravotníctvo	3	1	2	1	4	2	1	5	1	0	5	1
Iné	34	38	36	23	29	28	24	31	18	35	39	25
CELKOM	**82**	**113**	**105**	**62**	**88**	**66**	**54**	**86**	**70**	**83**	**108**	**57**

NBÚ evidoval v roku 2023 celkovo **974 hlásení o kybernetických bezpečnostných incidentoch:**

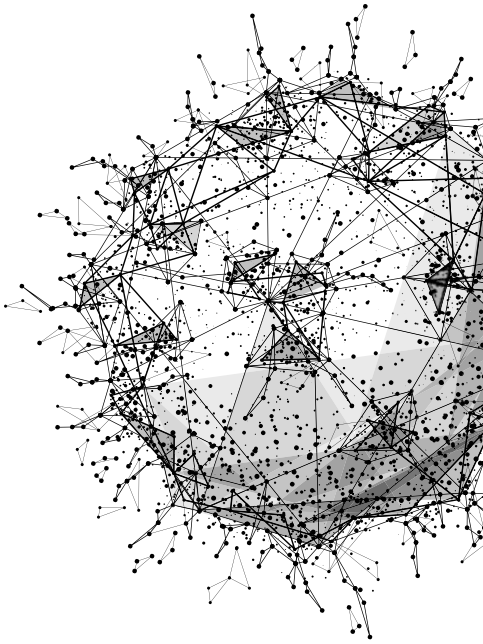
- 19 hlásení o závažných kybernetických bezpečnostných incidentoch I. stupňa,
- 4 hlásenia o závažných kybernetických bezpečnostných incidentoch,
- 3 hlásenia o závažných kybernetických bezpečnostných incidentoch III. stupňa.



Dominovali nasledujúce technické typy útokov: získavanie informácií (611), nedostupnosť (88), prienik do systému (64), škodlivý kód (49) a zraniteľnosť (46).

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 je možné v ďalších rokoch očakávať nárast hlásení – novela rozšíri pôsobnosť na ďalšie subjekty.

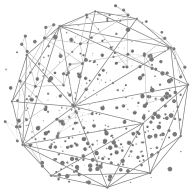
Najviac incidentov bolo nahlásených v sektoroch verejná správa (478), bankovníctvo (77) a zdravotníctvo (26). Vyšší počet hlásení implikuje viac incidentov v sektore a môže indikovať vyššiu úroveň zrelosti hlásiaceho subjektu (nebojí sa hlásiť, komunikuje, hlási aj dobrovoľné incidenty a pod).



Aj v roku 2023 bolo znefunkčnenie služieb pomocou DDoS útokov populárnou formou medzi útočníkmi s rôznou mierou znalostí a sofistikovanosti.

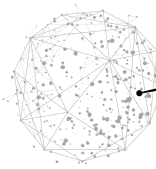
Na vzostupe bol aj ransomvér. V porovnaní s rokom 2022 sa počet ransomvérových útokov zvýšil o 95 % a celosvetovo zasiahol až 72 % spoločností. Naďalej v tejto oblasti prevláda aktivita profesionálnych gangov poskytujúcich ransomvér ako službu (RaaS). Pokračovali vo vylepšovaní svojich postupov a nástrojov, napríklad pomocou zrýchleného zašifrovania dát, obfuskácie stôp a efektívnejšej exfiltrácie dát.

Primárnym vektorom naďalej ostáva únik prihlasovacích údajov priamo do infraštruktúry alebo do VPN, ich kúpa alebo nález z uniknutých databáz. Útočník vie takisto získať prístupy pomocou phishingu či už vlastnou činnosťou alebo kúpou služby ponúkanou inou hackerskou skupinou, ktorá mu prihlasovacie údaje získa.

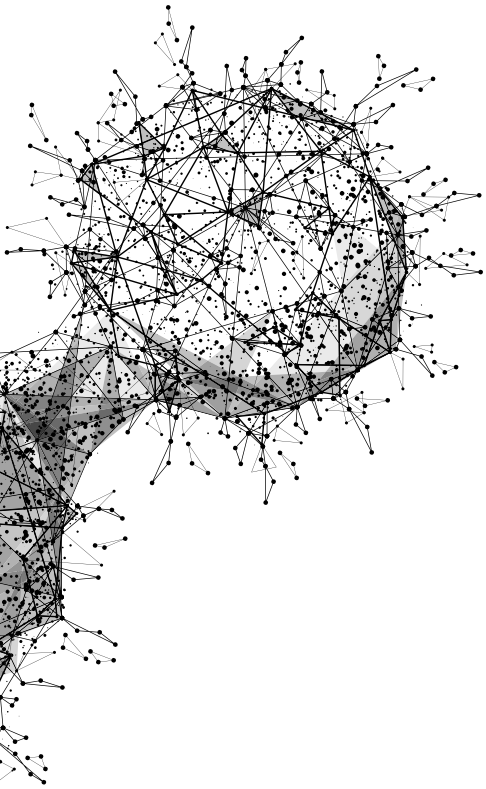


Naďalej boli evidované nedostatky na strane používateľov, ako miskonfigurácie a nedostatočné zabezpečenie systémov s nedostatočnou kybernetickou hygienou. Najvyšší počet zneužitých zraniteľností bol zaznamenaný v odvetví médií, rekreácie a zábavného priemyslu. Tieto nedostatky sa objavovali vo forme otvorených nastavení vzdialeného prístupu a iných služieb do internetu, slabých hesiel, opakovaného používania rovnakých hesiel medzi rôznymi službami a neimplementovanej multifaktorovej autentifikácie.

Nárast popularity umelej inteligencie a sprístupnenie jazykových modelov, ako napríklad ChatGPT, Azure alebo Grok, otvorili nové dvere útočníkom a dodali im nové nástroje na zefektívnenie ich činností. Umožňujú im napríklad generovať kvalitnejšie preklady a texty phishingových e-mailov a automatizáciu generovania phishingových e-mailov v rôznych jazykoch. Vyššia sofistikovanosť útokov bola takisto spôsobená používaním vlastných generatívnych modelov, ako napr. WormGPT, ktoré neobsahuje bezpečnostné obmedzenia.



Čo sa týka metód, útočníci najčastejšie využívali presmerovacie linky používané na obchádzanie e-mailových bezpečnostných mechanizmov. Zároveň poklesol výskyt využívania zraniteľných webov, ktoré mali otvorené presmerovanie (open redirect). Pokračuje používanie skracovačov URL adries na vyhnutie sa detekčným prostriedkom. K neprehľadnosti situácie prispelo aj používanie legitímnych skracovačov (napr. bit.



ly, cutt.ly), ako aj skracovacie mechanizmy veľkých sociálnych sietí, napr.: X (Twitter), LinkedIn a významný nárast počtu malých poskytovateľov URL skracovačov.

Motiváciu útočníkov vykonávať phishingové aktivity môžeme rozdeliť na získavanie citlivých údajov, ktoré sa následne predávajú tretím stranám a na vykonávanie phishingovej aktivity na šírenie malvéru, ktorý však rovnako môže slúžiť na zber citlivých údajov.

Malwaretisement kampane pokračovali aj v roku 2023 a šírili trojanizované verzie frekventovane používaných softvérov. Primárny problém predstavoval tendenciu ľudí automaticky klikať na reklamy, ktoré majú popredné miesta v search resultoch na Google.

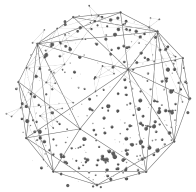
Phishing je stále najrozšírenejšou a najúspešnejšou metódou získavania citlivých údajov a šírenia škodlivého obsahu. Častým dôvodom prieniku do systému je kompromitácia e-mailovej schránky ako následok phishingu, alebo cez brute force útok na nezabezpečený prihlasovací web mailserveru a pod.

Phishingové kampane boli naďalej populárnou metódou na získavanie citlivých údajov, čo sa odzrkadlilo na výraznom náraste phishingových amatérov. Nárast bol pravdepodobne spôsobený jednoduchosťou získania phishingových nástrojov, ktoré sú vyvíjané a následne predávané alebo poskytované útočníkom ako služba (Phishing as a Service).

Vo phishingu naďalej prevládajú impersonácie, napr. bánk, pošty/doručovateľských firiem či sociálnych sietí. Boli zaznamenané aj aktivity, ktoré využívali geopoliticky relevantné udalosti, napr. vojna na Ukrajine alebo vojna v Izraeli.

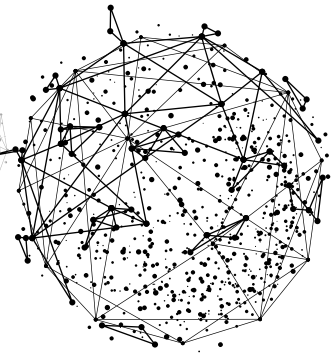
Phishingové kampane naďalej využívali sociálne inžinierstvo na efektívnejšie dosiahnutie svojho cieľa. Trendy v získavaní citlivých informácií sa s predchádzajúcim rokom príliš nelíšili. Prevládali nasledujúce naratívy phishingu:

- impersonácia doručovateľských služieb;
- impersonácia sieťového dodávateľa, banky, poštových služieb;
- impersonácia polície a Interpolu;
- impersonácia ústredných orgánov štátnej správy a iné.
- phishing a smishing boli naďalej vykonávané cez SMS a e-mail.



Pretrváva fenomén sextortion a crypto podvody (rôzne služby a pyramídové koncepty súvisiace s investíciami do kryptomien. Útočník si získa dôveru obete tým, že jej prvotne vypláca provízie, no v istom bode prestane. Tento typ podvodov má masívnu propagáciu – napr. na sociálnych sieťach či organizovaných fyzických stretnutiach.

Ďalším typom bol whaling, a aj napriek nižšej incidencii, je stále relevantný. Môžete sa s ním stretnúť napríklad vo forme impersonácie riaditeľa spoločnosti so žiadosťou o stav účtu a platbu.



Vzrástol aj počet interaktívnych foriem sociálneho inžinierstva – často spojený s phishingovými útokmi. Phishingové weby obsahujú interaktívny chat, útočník vedie obeť cez rôzne služby na vzdialenú správu alebo ju naviguje počas telefonátu sa vydáva za technickú podporu.

V roku 2023 boli časté DDoS útoky na kritickú infraštruktúru, bankový sektor a dopravu (napr. útoky na online parkovací systém a útoky na weby ZSSK, ktoré znemožnili online nákup lístkov na vlak a pod.). Takisto bolo zaznamenaných viacero kategorizovaných incidentov.

Pozitívnym javom bola zvyšovaná odolnosť infraštruktúry obetí po útoku, ale aj pri prevencii (vysoký počet medializovaných úspešných útokov) a vplyv osvety realizo-

vanej bezpečnostnými zložkami (celoštátne varovania, adresné/sektorové varovania organizácií, na ktoré hacktivisti plánujú útok). Vo väčšine prípadov sa po ukončení útoku podarilo obnoviť prevádzku.

Na Slovensku bolo identifikovaných hneď niekoľko zariadení infikovaných malvérom a to najmä SystemBC, IcedID, Ursnif, Trickbot, JS.Agent.USU, QuakBot, Qbot, Redline, Raccoon Stealer, Amadey, Lockbit 3.0. Známe boli medializované prípady z Univerzity Mateja Bela, ktorá bola napadnutá Medusalockerom a kampaň zneužívajúca zraniteľnosť VMware ESXi.

Najčastejším vektorom prieniku boli v roku 2023 phishingové útoky. Medzi nevhodné nastavenia systémov patrili otvorené RDP, FTP, SSH, SMB a prihlasovacie rozhrania do ICS s nastaveniami od výroby a heslami/bez prihlasovania alebo so zlou politikou hesiel. Preto je dôležité prízvukovať nutnosť dodržiavať security best practices, ako sú dobre zabezpečená sieť, napr. pomocou VPN, MFA, segmentácia, minimalizovanie threat surface (do internetu by mali mať prístup/byť pripojené len nevyhnutné služby a zariadenia).

Národné centrum kybernetickej bezpečnosti vydávalo bezpečnostné odporúčania a varovania pred zraniteľnosťami a hrozbami – 52 súhrnných bezpečnostných bulletinov a 428 bezpečnostných varovaní. Upozornilo na 1097 zraniteľností a hrozieb.

CYBERGAME

NBÚ zorganizoval druhý ročník súťaže v oblasti kybernetickej bezpečnosti s názvom CyberGame.

Cieľom hry bolo zaujímavou a hravou formou priblížiť tému kybernetickej bezpečnosti verejnosti a šíriť povedomie o hrozbách a spôsoboch ochrany svojich dôležitých dát. Hra mala zároveň motivovať ľudí venovať sa kybernetickej bezpečnosti a identifikovať talenty v tejto oblasti.

Cybergame trvala od 1. marca do 10. mája 2023 a kombinovala technické aj netechnické úlohy. Celkovo bolo pripravených viac ako 70 úloh. Hra bola rozdelená na 6 vetiev – analýza škodlivého softvéru, forenzná analýza, kryptografia, OSINT, hardening a procesné a bezpečnostné riadenie.

Každá vetva obsahovala niekoľko scenárov (príbehov), ktoré počas trvania hry pribúdali. V každom scenári bolo niekoľko úloh, ktoré na seba logicky nadväzovali. Princípom hry bolo zbierať body za tzv. „vlajky“. Vyhral ten, kto získal najviac bodov.

Do hry sa zapojilo celkovo 2 333 hráčov. V roku 2023 bolo umožnené hrať aj hráčom zo zahraničia a to vytvorením anglickej mutácie hry. Zo Slovenska bolo zapojených 1 788 hráčov z anglickej platformy súťažilo 545 používateľov. Do hry sa pripojili hráči zo 73 krajín. Registrovaných bolo 264 žien, 67 učiteľov, 420 študentov stredných škôl a 304 študentov z univerzít. Najmladší registrovaný hráč mal 9 rokov.

Víťazi Cybergame získali vecné ceny a najlepší hráč, druhý najlepší hráč a najlepšia hráčka v ženskej kategórii mali možnosť vycestovať do kyberbezpečnostného laboratória v Izraeli.

VNÚTROŠTÁTNY ORGÁN PRE CERTIFIKÁCIU KYBERNETICKEJ BEZPEČNOSTI

Európsky parlament a Rada (EÚ) dávnejšie prijali nariadenie 2019/881 o agentúre ENISA (Agentúra Európskej únie pre kyberbezpečnosť) a o certifikácii kyberbezpečnosti IKT, nazývaný aj Akt o kyberbezpečnosti. Zavádza aj celoúniový rámec certifikácie kyberbezpečnosti IKT produktov, služieb a procesov, ktorá má zvýšiť ich dôveryhodnosť.

V zmysle zákona č. 69/2018 o kybernetickej bezpečnosti je NBÚ vnútroštátnym orgánom pre certifikáciu kyberbezpečnosti a orgánom posudzovania zhody (NCCA). Napríklad vypracúva národnú stratégiu kyberbezpečnosti, spravuje a prevádzkuje jednotný informačný systém kyberbezpečnosti 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 k vykonávaniu 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 kyberbezpečnosti 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.

V súčasnosti sú rozpracované tri schémy kyberbezpečnosti:

Schéma EUCC

Prvou z pripravovaných schém podľa Aktu o kyberbezpečnosti je návrh európskej schémy certifikácie kyberbezpečnosti založenej na Common Criteria (CC). Vychádza z celosvetovo uznávanej schémy a je použiteľná výhradne pre IKT produkty. Zahŕňa úroveň záruky „významná a vysoká“ a nie je v nej možné aplikovať posúdenie zhody samohodnotením (conformity self-assessment). Platnosť certifikátu je stanovená na päť rokov a je ho možné obnoviť.

Schéma EUCS

Druhým návrhom európskej schémy certifikácie kyberbezpečnosti 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).

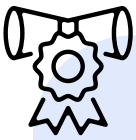
Schéma EU5G

Posledný pripravovaný návrh európskej schémy certifikácie kyberbezpečnosti pokrýva oblasť 5G sietí. Návrh stavia na súbore opatrení pre kyberbezpečnosť sietí 5G, pričom sa očakáva, že schéma pomôže tlmiť ďalšie riziká spojené s týmto ekosystémom.

V roku 2023 sa NBÚ 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 1 milióna eur. Projekt je plne financovaný zo zdrojov EÚ v programe Digital Europe.



KOMPETENČNÉ A CERTIFIKAČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI

Štátna príspevková organizácia Kompetenčné a certifikačné centrum kybernetickej bezpečnosti (KCCKB) 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 Kompetenčného centra manažovať európske finančné fondy pre kybernetickú bezpečnosť z priamo riadených programov EÚ.

Vo finančných programoch Slovensko dosiahlo výnimočný úspech na celoeurópskej úrovni. V programe Digital Europe v roku 2023 dominovalo medzi členskými štátmi v počte úspešných projektov. Aktivity Národného koordinačného centra významne prispeli k tomu, že slovenské spoločnosti získali podstatné finančné zdroje na zabezpečenie svojich kyberbezpečnostných potrieb.

V roku 2023, KCCKB v spolupráci s NBÚ a Ministerstvom dopravy SR tiež uzavrelo grantovú dohodu s Európskou komisiou, zameranú na efektívnu implementáciu smernice NIS2 v podmienkach SR. S cieľom neustále posilňovať odborné kapacity boli na MIRRI podané žiadosti na dofinancovanie európskych projektov z Plánu obnovy a odolnosti.

Súčasťou cieľov kompetenčného centra v roku 2023 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. Členmi európskej komunity kybernetickej bezpečnosti podľa Nariadenia (EÚ) č. 2021/887 sa cez NCC-SK stalo už niekoľko desiatok slovenských subjektov.

Podstatnou časťou úloh kompetenčného centra je výkon posudzovania zhody v kybernetickej bezpečnosti v zmysle nariadenia (EÚ) č. 2019/881 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií (Nariadenie o kybernetickej bezpečnosti). Neskôr, po jeho prijatí, sa bude Kompetenčné centrum uchádzať aj o akreditáciu v zmysle Nariadenia o kybernetickej odolnosti (Cyber Resilience Act – CRA).

Kompetenčné centrum je v súčasnosti akreditované na certifikáciu audítorov a manažérov kybernetickej bezpečnosti podľa osobitného predpisu a normy STN EN ISO/IEC 17024 a integrovaných systémov manažérstva kvality, manažérstva informačnej bezpečnosti, manažérstva IT služieb a manažérstva kontinuity činností, podľa normy STN EN ISO/IEC 17021.

Počet certifikovaných osôb sa v roku 2023 navýšil o 5 certifikovaných audítorov a 7 certifikovaných manažérov.

Ministerstvo spravodlivosti v legislatívnom procese 2022/806 akceptovalo návrh Národného bezpečnostného úradu na rozšírenie znaleckých odvetví o nové odvetvie kybernetická bezpečnosť. V zmysle tohto návrhu bola novelizovaná vyhláška Ministerstva spravodlivosti Slovenskej republiky č. 228/2018, ktorou sa vykonáva zákon č. 382/2004

o znalcoch, tlmočníkoch a prekladateľoch a kompetenčné centrum má ambíciu byť prvou znaleckou organizáciou, ktorá bude vykonávať znalecké činnosti v novom znaleckom odvetví kybernetická bezpečnosť.

Kompetenčné centrum bolo úspešné aj v oblasti vzdelávania dospelých. V roku 2023 sa podľa zákona č. 568/2009 o celoživotnom vzdelávaní podarilo získať od Akreditačnej komisie Ministerstva školstva, vedy a výskumu a športu SR, vedy a výskumu a športu akreditáciu vzdelávacích programov ďalšieho vzdelávania pre školenia Manažér kybernetickej bezpečnosti a Audítor kybernetickej bezpečnosti. Vydaná bola aj aktualizovaná vzdelávacia schéma. Do portfólia vzdelávania pribudol nový špecializovaný kurz a workshop Riadenie kontinuity a kurz Riadenie informačnej bezpečnosti. Aktualizované boli sylaby viacerých existujúcich kurzov.

Za rok 2023 bolo realizovaných celkovo 65 školení, z toho 8 kurzov „Prehľad KB“, 10 kurzov „Základy KB“, 20 kurzov „Manažér KB“, 3 kurzy „Audítor KB“, 9 špecializačných kurzov a workshopov, 1 kurz manažérstva informačnej bezpečnosti podľa ISO/IEC 27001:2022 a 14 bezplatných webinárov zvyšovania povedomia o kybernetickej bezpečnosti. Celkovo sa na uvedených vzdelávacích aktivitách počas roku 2023 zúčastnilo 1 033 účastníkov.

Kompetenčné centrum zorganizovalo úspešnú akciu zameranú na zvyšovanie povedomia o kybernetickej bezpečnosti „Cybersecurity Roadshow 2023“. Realizované boli viaceré odborné prednášky na konferenciách a pre študentov vybraných vysokých škôl v SR.

Kompetenčné centrum vydalo každý mesiac jeden leták na účely zvyšovania bezpečnostného povedomia.

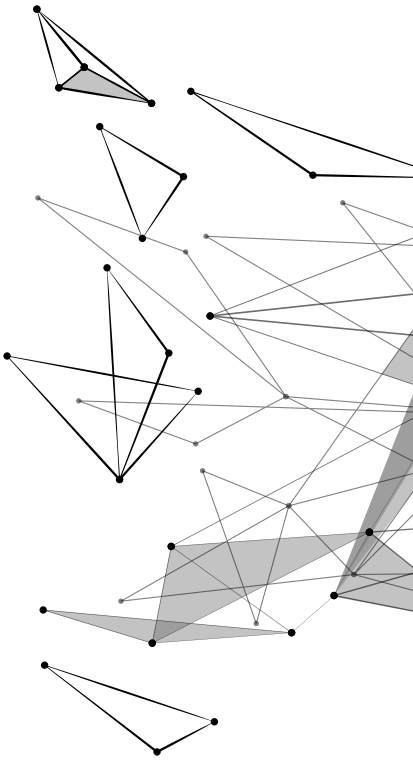
Každoročne sú na základe zadania KCCKB spracované prieskumy stavu kybernetickej bezpečnosti, vydané následne aj vo forme verejného dokumentu. Ide najmä o výsledky prieskumu medzi verejnosťou a výsledky prieskumu realizovaného medzi malými a strednými podnikmi.

Aj v roku 2023 kompetenčné centrum ďalej rozširovalo okruh organizácií, s ktorými uzatvorilo spoluprácu formou podpisu memoranda.

V spolupráci s NCKB SK-CERT postavilo kompetenčné centrum tím mladých ľudí, ktorí Slovensko reprezentovali na podujatí European CyberSecurity Challenge. Aktivitu zastrešuje Európska agentúra pre kybernetickú bezpečnosť (ENISA). Prítomných bolo 34 národných tímov – k tímom z 28 členských krajín EÚ sa pripojili aj hosťujúce tímy z USA, Kanady, Kostariky, Srbska, Gruzínska a Spojených arabských emirátov.

Súťaž trvala od 24. do 27. októbra v nórskom v Hamare. Slovenský tím reprezentovalo desať mladých talentov – deväť chlapcov a jedno dievča. Na súťaž sa tím pripravoval niekoľko mesiacov. V júni sa zúčastnili na medzinárodnom bootcampe vo Viedni a následne niekoľkých bootcampoch v Bratislave pod vedením technických koučov z SK-CERT.

MEDZINÁRODNÁ SPOLUPRÁCA



Príslušníci úradu rozvíjajú vzťahy so zahraničnými partnermi na dennej báze naprieč desiatkami organizácií, platforiem aj formátov. NBÚ v roku 2023 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

Naši príslušníci participovali prezenčne aj virtuálne na pravidelných zasadnutiach Bezpečnostného výboru Rady EÚ (CSC), Skupiny expertov Európskej komisie (EK) pre bezpečnostnú politiku (ComSEG), Bezpečnostného výboru Európskej služby pre vonkajšiu činnosť (EEAS), Bezpečnostného výboru Agentúry Európskej únie pre vesmírny program (EUSPA), Implementačnej pracovnej skupiny pre TEMPEST (ITTF) a Agentúry Európskej únie pre kybernetickú bezpečnosť (ENISA).

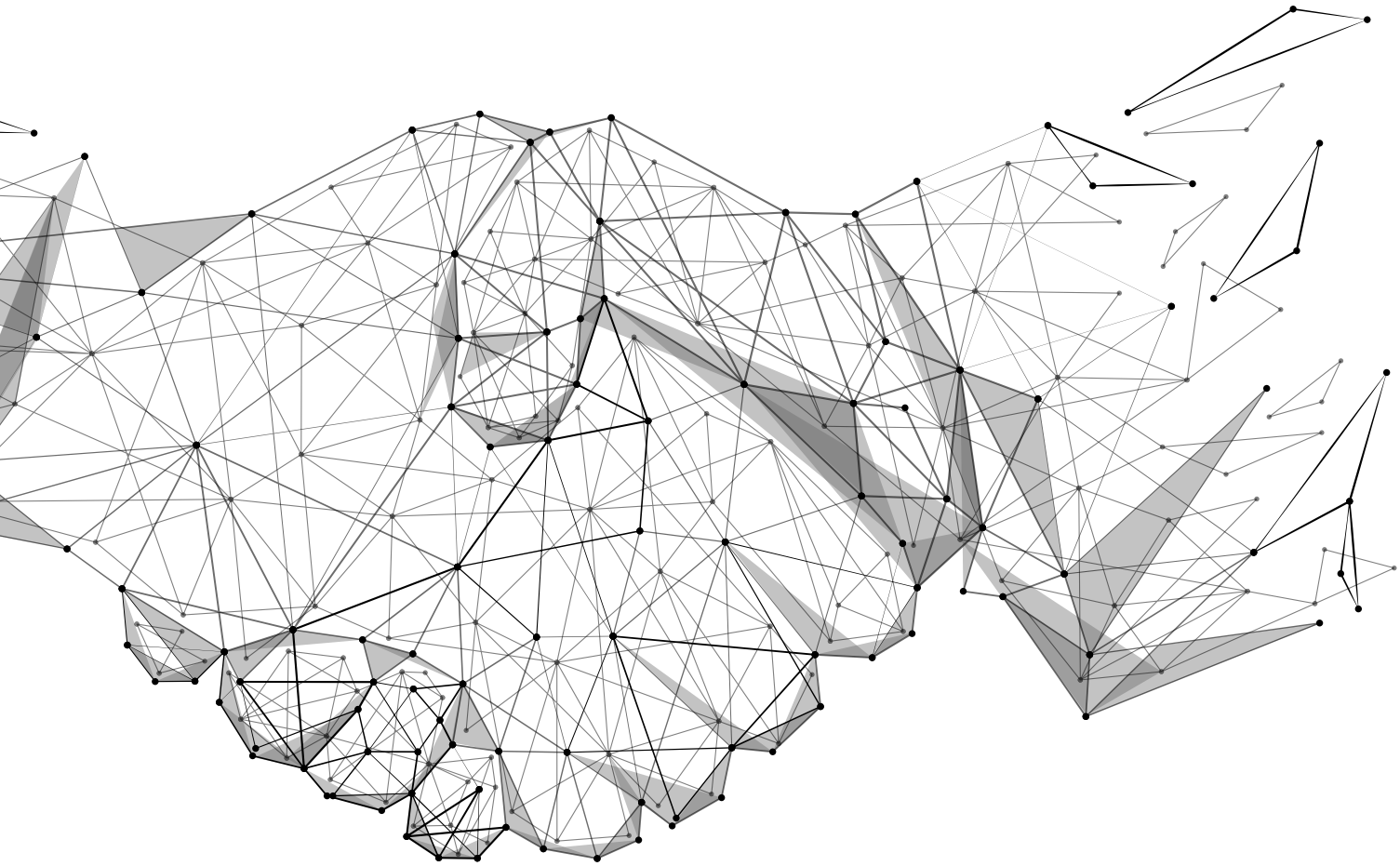
Na pôde Rady EÚ revidovali bezpečnostné pravidlá s cieľom odstrániť nedostatky identifikované v aplikačnej praxi. V uvedených pracovných formátoch sa úrad aktívne zapájal či už do prípravy bezpečnostných noriem tak, aby bola zabezpečená ochrana utajovaných skutočností ale aj do procesu revízie bezpečnostných pravidiel.

Pokračovala revízia bezpečnostných pravidiel Rady pre ochranu utajovaných skutočností EÚ[1] (EUCI) najmä v oblastiach personálnej a priemyselnej bezpečnosti, manažmentu bezpečnostných rizík, hodnotiacich bezpečnostných návštev, porušovania bezpečnostných pravidiel a neoprávnených manipulácií s EUCI, ich zdieľania, ale aj pri mimoriadnom či ad hoc prístupe k EUCI pokračovala revízia bezpečnostných pravidiel Rady pre ochranu utajovaných skutočností EÚ1 (EUCI).

Proces revízie bol zameraný na prílohy obsahujúce konkrétne opatrenia v jednotlivých oblastiach bezpečnosti informácií. Bezpečnostný výbor Rady koncom roka 2023 pripomienkoval návrh nariadenia Európskeho parlamentu (EP) a Rady o informačnej bezpečnosti v inštitúciách, orgánoch, úradoch a agentúrach Únie v časti týkajúcej sa neutajovaných informácií. Pokračovala aj diskusia k návrhu dohody medzi EÚ a USA, ktorou sa stanovujú bezpečnostné postupy pri vypúšťaní satelitov Galileo z územia Spojených štátov.

Rok 2023 bol mimoriadne bohatý na legislatívnu aktivitu v Európskej rade (Rada) a Európskom parlamente. Počas švédskeho a španielskeho predsedníctva sa na úrovni prí-

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



pravných a politických orgánov Rady – najmä v Horizontálnej pracovnej skupine pre kybernetické záležitosti – po právnej stránke dokončili tri spisy.

Prvým bol návrh nariadenia EP a Rady 2023/2841, ktorým sa stanovujú opatrenia na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v inštitúciách, orgánoch, úradoch a agentúrach Únie (KB EUIBAs).

Druhým spisom bol návrh nariadenia EP a Rady o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami a o zmene nariadenia (EÚ) 2019/1020 (CRA).

Posledným bol návrh nariadenia EP a Rady, ktorým sa mení nariadenie eIDAS, pokiaľ ide o stanovenie rámca pre európsku digitálnu identitu (eIDAS2). Publikácia v Úradnom Vestníku EÚ sa očakáva v prvom štvrťroku 2024.

Slovensko aktívne podporovalo ciele zmieňovaných spisov. V priebehu ich negociácií zaslala množstvo pozitívne prijatých pripomienok a komentárov. Schválením uvedenej

legislatívy sa posilní úroveň kybernetickej bezpečnosti v európskych inštitúciách, zvýši sa spotrebiteľská ochrana pri kúpe a využívaní rozličných softvérových a hardvérových produktov s digitálnymi prvkami a vytvorí sa aj predpoklad pre jednoduché a celoúniové overovanie identity občanov EÚ využívajúcich elektronické služby.

Európska komisia v apríli 2023 zverejnila kybernetický balíček, ktorý pozostával z dvoch nových legislatívnych a jedného nelegislatívneho spisu.

Išlo o návrh nariadenia EP a Rady, ktorým sa stanovujú opatrenia na posilnenie solidarity a kapacít v Únii na odhaľovanie kybernetických hrozieb a incidentov, prípravu a reakciu na ne (CySOLa), o návrh nariadenia EP a Rady, ktorým sa mení nariadenie (EÚ) 2019/881, pokiaľ ide o riadené bezpečnostné služby, (CSA+) a o oznámenie k vytvoreniu Akadémie zručností v oblasti kybernetickej bezpečnosti.

S prihliadnutím na potrebu rýchleho napredovania s cieľom dosiahnuť politickú dohodu inštitúcií pred ukončením legislatívneho cyklu začiatkom roka 2024, Horizontálna pracovná skupina pre kybernetické záležitosti počas intenzívnych diskusií prerokovala predmetné spisy.

Výbor stálych zástupcov tak mohol pre CSA+ a CySOLa udeliť predsedníctvu mandát na záverečnú diskusiu s EP a EK. Politická dohoda k obom spisom sa očakáva v prvom štvrťroku 2024. Je potrebné spomenúť, že kým Slovenská republika podporovala hlavné myšlienky a ciele návrhu k solidarite pod podmienkou zásadného dopracovania daného návrhu, čo sa aj podarilo, zdržala sa pri hlasovaní o návrhu CSA+, ktorý považuje za duplicitný k existujúcej právnej úprave.

Je nutné tiež doplniť, že na úrovni komitologických výborov v zmysle už prijatej sekundárnej legislatívy EÚ, najmä revidovanej smernice o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii (smernica NIS2), aktu o kybernetickej bezpečnosti (CSA), či inej relevantnej legislatívy, sa úrad zúčastňoval na technických diskusiách o implementácii jednotlivých opatrení.

Osobitnú pozornosť si však zaslúži príprava kandidátskych schém kybernetickej bezpečnosti EUCC (spoločné kritériá) a EUCS (cloudové schémy), ktoré by mali byť publikované v Úradnom vestníku EÚ v prvom štvrťroku 2024.

Horizontálna pracovná skupina pre kybernetické záležitosti (HWPCI) vo svojich nelegislatívnych aktivitách venovala pozornosť aj ostatným strategickým prvkom v oblasti kybernetickej diplomacie. V roku 2023 sa jej podarilo aktualizovať rámec pre súbor nástrojov kybernetickej diplomacie (Cyber Diplomatic Toolbox), na základe ktorého bude môcť Rada prijať efektívnejšie reakcie voči škodlivým kybernetickým aktivitám vrátane sankcií.

Súčasťou tohto rámca boli aj rozšírené implementačné usmernenia, ktoré zohľadnili prebiehajúci konflikt na Ukrajine, vplyvy nových technológií aj zhoršenú geopolitickú bezpečnostnú situáciu. Okrem uvedeného Rada v máji 2023 na základe práce HWPCI prijala závery k európskej politike kybernetickej obrany a v júni 2023 závery k digitálnej diplomacii. NBÚ participoval pri tvorbe a vyvažovaní spomínaných strategických dokumentov.

Zástupcovia úradu sa zúčastnili aj na zasadaní pracovnej skupiny Certifikačná skupina Európskej únie pre kybernetickú bezpečnosť (ECCG). Hlavnou témou bola príprava finálneho znenia nariadenia EK ohľadom implementácie horizontálnej certifikačnej schémy pre produkty kybernetickej bezpečnosti a pre samotné ochranné dokumen-

ty, pridanie referencií na existujúce národné schémy, ale aj dohoda, že akceptácia a vzájomné uznanie medzi jednotlivými členskými štátmi má byť plnohodnotná.

Príslušník úradu a Národného centra kybernetickej bezpečnosti SK-CERT v roku 2023 pôsobili v pracovných formátoch EK ako Skupina pre spoluprácu – NIS a Pracovná skupina pre hodnotenie národných stratégií. Ich hlavnou úlohou bolo zabezpečovať a zintenzívňovať vzájomnú strategickú a analytickú spoluprácu a zdieľať informácie medzi orgánmi zodpovednými za kybernetickú bezpečnosť členských štátov a ich jednotkami.

Medzi kľúčové priority Skupiny pre spoluprácu – NIS patrila príprava na implementáciu Smernice Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Európskej únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS2), a s tým súvisiaca aplikácia jednotlivých nových nástrojov.

K otázkam riešenia národnej implementácie smernice NIS2 pribudli v súvislosti s hodnotením rizík a rizikových scenárov aj témy súvisiace s prijatými závermi Rady o vývoji prístupu EÚ ku kybernetickej bezpečnosti.

Boli vytvorené nové subplatformy v Skupine pre spoluprácu ako Work Stream on Risk Evaluation, Work stream Supervision a Work Stream WHOIS s cieľom uchopiť témy hodnotenia rizík, dohľadu, kontroly a podpory bezpečnosti a stability internetu.

V druhom polroku sa Skupina pre spoluprácu – NIS z dôvodu incidentov, ktoré sa stali v Baltickom mori, zamerala aj na diskusiu o podmorskej infraštruktúre (dátové káble, potrubia a miesta ich vyústenia).

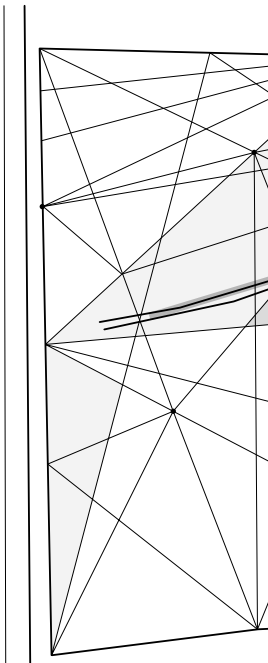
Súčasne rezonoval rozvoj vzťahov medzi Skupinou pre spoluprácu a Skupinou pre budovanie odolnosti kritickej infraštruktúry – obe platformy prvý raz spoločne rokovali.

ENISA realizovala cestovnú mapu potrieb pre cvičenia pre oblasť kybernetickej bezpečnosti. Štáty si zdieľali svoje skúsenosti, pokiaľ išlo o najzávažnejšie incidenty a hrozby v oblasti kybernetickej bezpečnosti, ktoré ich počas roka zasiahli (dominoval opäť ransomvér). Okrem toho ENISA pripravila prezentáciu, v ktorej sa zamerala na svoje nové povinnosti, najmä tie, ktoré sa týkali členských štátov v súvislosti s plnením notifikačných opatrení. NBÚ pôsobil aj v nasledujúcich Work Stream skupinách pre spoluprácu:

- Work Stream – Skupina zameraná na notifikačné povinnosti prevádzkovateľov základných služieb
- Work Stream – Skupina pre riešenie kybernetických bezpečnostných incidentov veľkého rozsahu
- Work Stream - Skupina pre digitálnu infraštruktúru
- Work Stream 5G – Skupina zabezpečenie a ochranu 5G sietí
- Work Stream – Skupina pre sektor zdravotníctva
- Work Stream – Skupina pre voľby

Vo svojom rozvoji pokračovala aj komunita zainteresovaných subjektov EU CyberNet, ktorá združuje národné orgány a inštitúcie pôsobiace v oblasti kybernetickej bezpečnosti, expertné skupiny pre danú oblasť, think-tanky a akademické inštitúcie so sídlom v členských štátoch EÚ.

EU CyberNet organizovala počas roka množstvo workshopov a konferencií, ktoré boli venované aktuálnym témam kybernetickej bezpečnosti; príslušníci úradu si zvyšovali svoju odbornosť a rozširovali poznatky účasťou na týchto aktivitách.



Pravidelné zasadanie Bezpečnostného výboru Európskej služby pre vonkajšiu činnosť (SC EEAS) prinieslo revíziu a implementáciu programu bezpečnostného povedomia a zintenzívnilo školenia personálu o možných kybernetických rizikách.

SC EEAS súčasne finalizoval práce na príručke, ktorá má pomôcť nielen nováčikom pri práci s utajovanými skutočnosťami EÚ (EUCI). Pokračoval s revíziou usmernení k tvorbe a manipulácií s EUCI a k havarijnému plánu pri evakuácii a deštrukcii EUCI. Zamestnanci SC EEAS prispeli k budovaniu odolnosti a bezpečnostného povedomia zahraničných delegácií EÚ pomocou školení, workshopov a podporných programov.

V írskom Dubline sa v novembri konala medzinárodná konferencia Európskych partnerov proti korupcii a Európskej siete kontaktných miest proti korupcii (EPAC/EACN). Zameraná bola na posilnenie medzinárodnej spolupráce a výmenu informácií v oblasti prevencie korupcie a policajného dohľadu, ako aj na postupy na vymáhanie majetku z trestnej činnosti.

Najväčším prínosom podujatia bolo nadviazanie komunikácie, odborná diskusia, osobná výmena poznatkov a praktických postupov pri prevencii, odhaľovaní a vyšetrovaní trestných činov korupcie, sprostredkovanie skúseností partnerských útvarov členov EPAC/EACN a zefektívnenie operatívnej spolupráce protikorupčných a inšpekčných úradov organizovaných v medzinárodnej EPAC/EACN sieti.

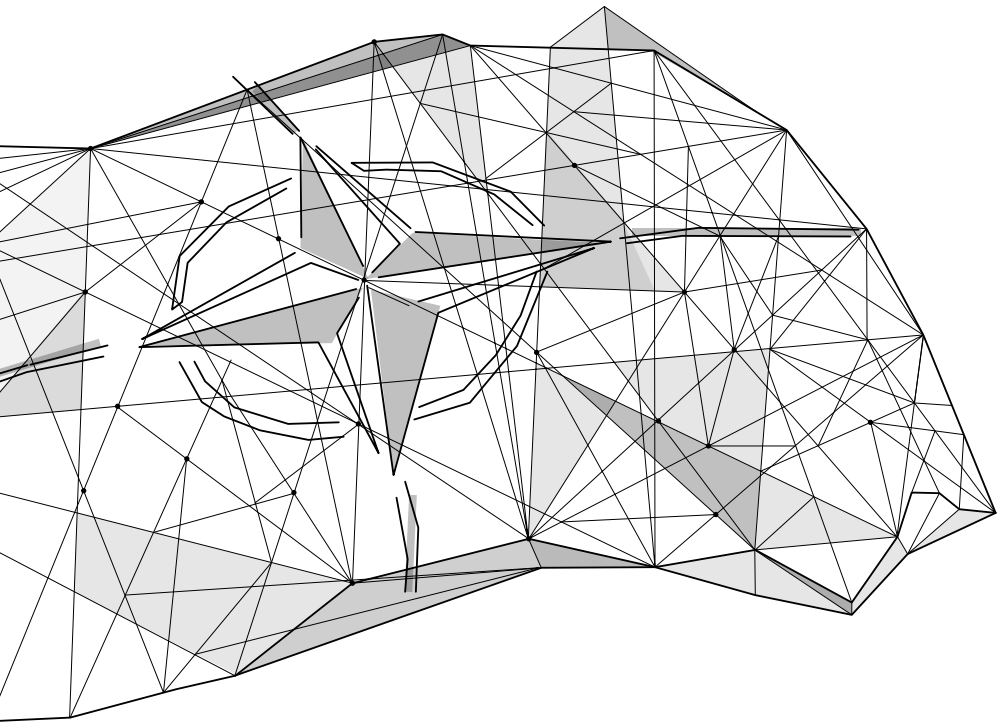
Pokračovali aj aktivity a práce súvisiace s inštitucionalizáciou Európskeho centra odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti a sieť národných koordinačných centier (ECCC).

Hlavnou úlohou tohto centra je strategický záujem EÚ zachovávať a rozvíjať kapacity kybernetickej bezpečnosti s cieľom zabezpečiť jednotný digitálny trh, chrániť kritické siete a informačné systémy a poskytovať kľúčové služby v tejto oblasti. KCCKB aktívne zastupovalo úrad v správnej rade ECCC, pričom súčasne plnilo sprostredkované úlohy ako národné koordinačné centrum.

Veľmi pozitívne je potrebné vnímať i predstavenie a zaslanie nominácie úradu za Slovenskú republiku na neobsadenú funkciu výkonného riaditeľa ECCC, ktorého vyberie EK a zvolí správnou radou.

V roku 2023 sa príslušníci úradu zúčastňovali na pravidelných zasadaniach Bezpečnostného výboru pre Vesmírne programy EÚ v Agentúre Európskej únie pre vesmírny program (EUSPA). V hlavnom Bezpečnostnom výbore EUSPA bolo primárnym bodom diskusie vypracovanie základných bezpečnostných požiadaviek (GSR) a 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. Má byť využitá v súvislosti s programom GOVSATCOM a má zabezpečiť vysokú mieru šifrovania, odolnosti, teda aj bezpečnosti – sieť má byť prispôsobená aj na prenos utajovaných skutočností.



NATO

Bezpečnostný výbor NATO (SC) zasadol vo všetkých svojich formátoch (bezpečnostné politiky, bezpečnosť komunikačných a informačných systémov a na úrovni riaditeľov bezpečnostných úradov).

Z pohľadu ochrany utajovaných skutočností NATO pokračovali rozsiahle revízie bezpečnostných pravidiel. Revízie sa zamerali predovšetkým na podporné dokumenty k hlavnej bezpečnostnej politike NATO C-M(2002)49-REV1.

Hlavnou témou bola Smernica o priemyselnej bezpečnosti a utajovaných kontraktoch. Výbor vytvoril pracovnú skupinu expertov členských štátov na prípravu revidovanej Smernice o bezpečnostných projektoch a priemyselnej bezpečnosti.

Bola vytvorená pracovná skupina pozostávajúca z členov Archívneho výboru a SC, ktorej úlohou bude riešiť problematiku hromadného rušenia utajenia utajovaných skutočností NATO. Rovnako aj v NATO sa revidujú základné smernice a podporné dokumenty bezpečnostných politík NATO, najmä usmernenia o personálnej, fyzickej, objektovej či administratívnej bezpečnosti alebo o bezpečnostnej ochrane utajovaných informácií NATO stupňa Restricted (Vyhradené).

V máji zasadol Archívny výbor (NATO AC). Predstavil iniciatívu vytvorenia nových postupov na hromadné odtajnenie dokumentov z obdobia vojny v Juhoslávii. V súvislosti s týmto cieľom budú zasadania spojenej pracovnej skupiny medzi zástupcami NATO AC a SC vo formáte bezpečnostných politík.

Počas októbrového zasadania v najvyššom formáte (Principals) bol predostretý účastníkom program na rok 2024, ktorý bol rozšírený o dva nové podporné dokumenty. Prvý z nich sa bude zaoberať teleprácou a druhý zahraničným vlastníctvom, kontrolou a vplyvom na firmy zúčastňujúce sa na NATO kontraktoch (FOCI).

Za hlavný míľnik v oblasti kybernetickej bezpečnosti aj obrany možno považovať júlový summit vo Vilniuse. Testoval sa na ňom pilotný mechanizmus Virtual Cyber Incident Support Capability (VCISC).

VCISC predstavuje virtuálnu spôsobilosť, ktorú môžu spojenci využiť v prípade neschopnosti vyriešiť následky škodlivej kybernetickej aktivity vlastnými silami. Členské štáty môžu cez NATO požiadať o poskytnutie pomoci.

Slovensko sa ešte pred konaním summitu stalo dobrovoľným prispievateľom do VCISC a príslušníci úradu aj aktívne participovali na jeho pilotnom testovaní. Ponaučenia z cvičenia budú pretransformované aj do stanovenia cieľov mechanizmu a budovania VCISC komunity.

V novembri hostil Berlín prvú výročnú konferenciu o kybernetickej obrane NATO. Spojila všetky tri úrovne nielen v štruktúrach NATO, ale aj u 31 spojencov. Slovensko bolo zastúpené na politickej, technickej a vojenskej úrovni predstaviteľmi Ministerstva zahraničných vecí a európskych záležitostí Slovenskej republiky, NBÚ a Centra kybernetickej obrany.

Hlavnými posolstvami konferencie boli nevyhnutnosť spolupráce všetkých úrovní so súkromným sektorom, potreba budovania spoločného situačného povedomia, včasné zdieľanie informácií pre rýchlu reakciu na škodlivé kybernetické aktivity, budovanie partnerstiev a spolupráca (primárne EÚ), udržiavanie tempa pri implementovaní nových technológií, väčšia proaktivita a prípadná spoločná atribúcia.

Na bilaterálnej úrovni príslušníci úradu rokovali so zástupcami NATO v dvoch oblastiach. Zástupcovia oddelenia bezpečnostných previerok NOS chceli vedieť detaily priebehu bezpečnostných previerok a vydávania osvedčení a certifikátov, pretože potrebovali tieto informácie na prípravu príručky NATO Personnel Security. V nej presne vysvetľujú postupy získania osvedčenia/certifikátu pre ľudí pracujúcich v štruktúrach NATO.

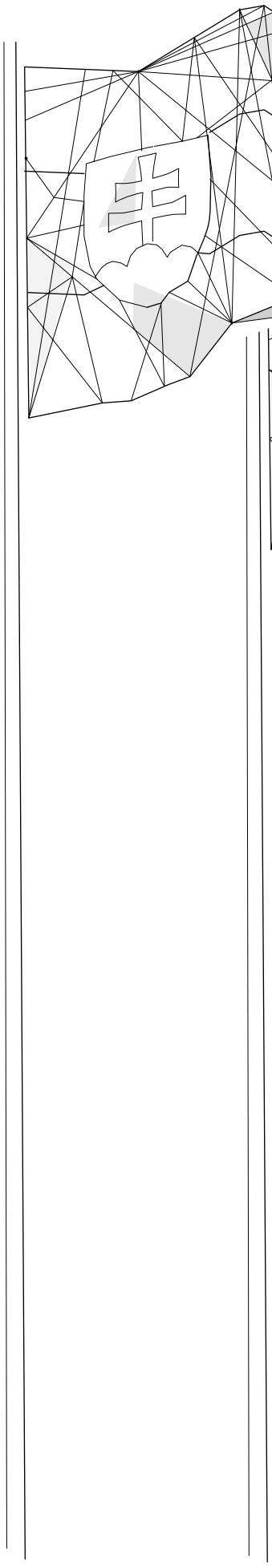
Naši príslušníci navštívili v lete 2023 centrálu NATO v Bruseli, kde im vysvetlili detaily fyzickej a objektovej bezpečnosti. Poznatky využijú pri projekte obnovy fyzickej bezpečnosti a objektovej bezpečnosti úradu.

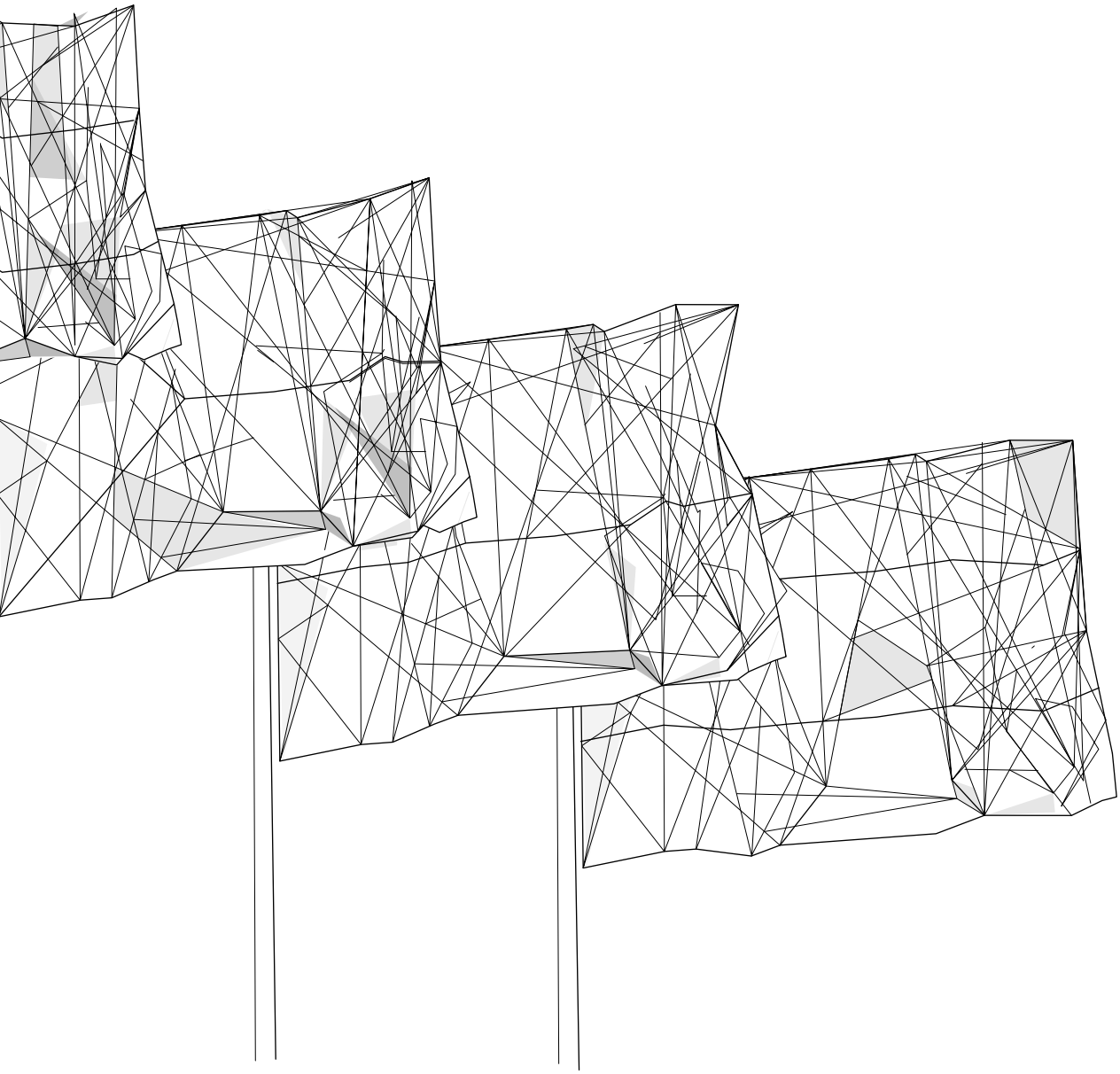
Úrad participoval aj na spoločnom aliančnom cvičení NATO Able Staff 2023 v novembri 2023. Malo preveriť komunikačné procedúry súvisiace s jadrovým plánovaním, precvičiť použiteľné opatrenia systému krízovej odozvy aliancie, priniesť zdokonalenie v konzultačnej oblasti, realizovať praktický výcvik personálu v centrále NATO, v Hlavnom veliteľstve spojeneckých síl v Európe (SHAPE) a v národných ústrediach.

REGIONÁLNA SPOLUPRÁCA

V roku 2023 predsedal Stredoeurópskej platforme pre kybernetickú bezpečnosť český NÚKIB. Zástupcovia úradu sa zúčastnili na rokovaniach platformy s ďalšími kolegami z Maďarska, Poľska a Rakúska.

Predmetom rokovaní boli aktuálne témy na úrovni EÚ, vzájomné prieniky a skúsenosti v daných témach. Zástupcovia jednotlivých krajín sa venovali napríklad transpozícii NIS2; výskumu, vývoju a regionálnej spolupráci, kde česká strana prezentovala svoj prístup k cvičeniam v kybernetickej bezpečnosti alebo úlohy právnych poradcov.





MEDZINÁRODNÉ AKTIVITY

V septembri 2023 sa konalo 37. plenárne zasadanie Multinational Industrial Security Working Group (MISWG). Pracovná skupina je uznávaným orgánom pre spoluprácu týkajúcu sa oblasti najlepších postupov v oblasti medzinárodnej priemyselnej bezpečnosti, kde je zastúpených takmer 40 krajín sveta vrátane Slovenska.

Hlavným cieľom stretnutia bolo podporovať, zlepšovať 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.

Na stretnutí absolvovali zástupcovia úradu viacero bilaterálnych rozhovorov so zámerom prehĺbiť spoluprácu s partnermi v oblastiach ochrany utajovaných skutočností a kybernetickej bezpečnosti (Holandsko, Taliansko, Dánsko, Japonsko, Luxembursko, Španielsko, Maďarsko, Rumunsko, Austrália a Macedónsko).

Príslušníci úradu pôsobili aj v skupine CCRA – Common Criteria Recognition Arrangement Group.

BILATERÁLNE VZŤAHY

Národné centrum kybernetickej bezpečnosti si pravidelne vymieňalo informácie o aktuálnych právnych predpisoch na národnej úrovni, zraniteľnostiach, hrozbách a incidentoch a zdieľalo si informácie o osvedčených postupoch či dobrej praxi so svojimi zahraničnými partnermi aj mimo EÚ.

V marci 2023 schválila vláda medzinárodnú zmluvu s Európskou vesmírnou agentúrou o výmene a vzájomnej ochrane utajovaných skutočností.

V priebehu jari odštartovali rokovania o zmluve o ochrane utajovaných skutočností s Holandskom, ktoré na jeseň pokračovali medzirezortným pripomienkovým konaním.

Riaditeľ úradu Roman Konečný sa počas roka stretol s českými partnermi z GIBS, NBÚ (ČR) a NÚKIB. S poslednou menovanou inštitúciou podpísal aj memorandum o spolupráci. Obe inštitúcie potvrdili aktívnu a dlhodobú kooperáciu v bezpečnostných otázkach. Naši kolegovia sa stretli s odborníkmi z NÚKIB aj pri inovácii vybavenia národného laboratória TEMPEST za účelom testovania a získavania zručností pri práci s novou meracou aparatúrou.

České NBÚ sme naopak privítali na pôde úradu a hovorili o zosúladení postupov pri uznávaní bezpečnostných previerok. Oba úrady následne zverejnili príslušné metodiky na svojich stránkach. V júni sa recipročne stretli zástupcovia centrálnych registrov oboch krajín.

Zástupcovia úradu participovali aj na rokovaniach k návrhu zmluvy medzi vládou a Organizáciou pre spoluprácu v spoločnom vyzbrojovaní (OCCAR). Dohoda umožní slovenským subjektom participáciu na európskych projektoch v oblasti zbrojného priemyslu.

V marci a auguste sme prijali zástupcov z Indonézie. Cieľom bolo ďalšie prehlbovanie spolupráce v oblasti bezpečnosti, regionálnych bezpečnostných výziev a rozvoji bezpečnostnej spolupráce medzi Indonézskou a Slovenskou republikou.

Hlavným bodom bolo podpísanie memoranda o porozumení medzi oboma stranami (marec 2023). V memorande bolo identifikovaných 17 oblastí spolupráce – medzi najdôležitejšie možno zahrnúť ochranu pred aktívnymi kybernetickými hrozbami, podporu zodpovedného správania sa štátu v kyberpriestore, cyber threat intelligence (CTI) a strategické analýzy; bezpečnosť dodávateľského reťazca informačných a komunikačných technológií; budovanie kapacít a ďalšie.

V novembri prijali príslušníci NBÚ na pôde úradu historicky prvú delegáciu z afrického kontinentu – z Kene. Tvorili ju najmä zástupcovia silových rezortov a špecialisti na kybernetickú bezpečnosť. Kenská strana vyjadrila záujem o bližšiu spoluprácu. Agenda stretnutia bola orientovaná na otázky z oblasti kybernetickej bezpečnosti.

Záujem o nadviazanie spolupráce prejavili počas roka na krátkych stretnutiach aj Taipejská reprezentačná kancelária v Bratislave, Stálá komise senátu ČR pro sdělovací prostředky, Stále zastúpenie Belgického kráľovstva pri OSN vo Viedni a Francúzsko ohľadom spolupráce pri zavádzaní a tvorbe európskej schémy kybernetickej bezpečnosti pre oblasť cloudových služieb.

V septembri 2023 bolo vytvorené miesto styčného dôstojníka úradu na Zastupiteľskom úrade Slovenskej republiky vo Washingtone D. C., ktorého hlavnou úlohou je vytvorenie úzkej spolupráce v oblasti kybernetickej bezpečnosti a rozvoj spolupráce s príslušnými orgánmi zaoberajúcimi sa ochranou utajovaných skutočností v Spojených štátoch amerických.

VÝMENA ZAHRANIČNÝCH INFORMÁCIÍ

Elektronizácia registrov zahraničných utajovaných skutočností online prepojením s registrami utajovaných skutočností orgánov verejnej moci umožňuje bezpečnú, rýchlejšiu a flexibilnejšiu evidenciu a elektronickú distribúciu utajovaných skutočností.

NBÚ vlani jednotlivým registrom utajovaných skutočností naďalej poskytoval metodickú pomoc pri elektronickej evidencii utajovaných skutočností.

Pracovisko centrálneho registra spracovalo 3 716 utajovaných skutočností NATO a 2 999 utajovaných skutočností EÚ. Úrad sprostredkoval aj výmenu 172 utajovaných skutočností cudzej moci.

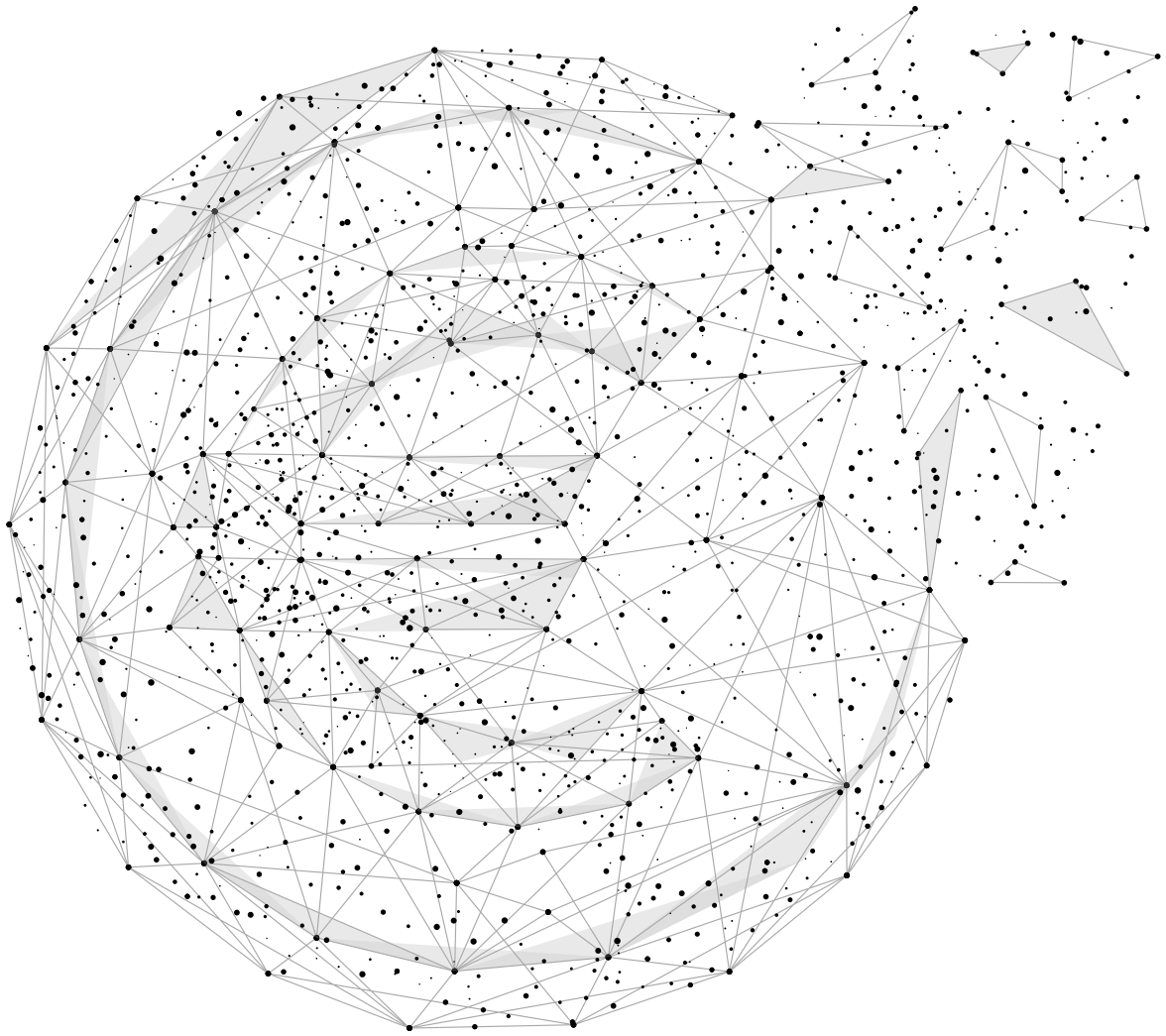
Na úrade od roku 2010 pôsobí register utajovaných skutočností NATO ATOMAL, minulý rok v ňom nebola zaregistrovaná utajovaná písomnosť.

Stupeň utajenia	2022	2023
NATO — RESTRICTED	1833	1863
EU — RESTRICTED	886	1115
CUDZIA MOC — VYHRADENÉ	114	87
NATO — CONFIDENTIAL	565	732
EU — CONFIDENTIAL	750	1117
CUDZIA MOC — DÔVERNÉ	39	59
NATO — SECRET	1770	1121
EU — SECRET	886	767
CUDZIA MOC — TAJNÉ	7	26
NATO — TOP SECRET	0	0
EU — TOP SECRET	0	0
CUDZIA MOC — PRÍSNE TAJNÉ	0	0
NATO – spolu	**4168**	**3716**
EU — spolu	**2522**	**2999**
CUDZIA MOC — spolu	**160**	**172**

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.

HOSPODÁRENIE

Rozpis záväzných ukazovateľov rozpočtu kapitoly 41 – Národný bezpečnostný úrad na rok 2023, vplyv rozpočtových opatrení na výšku upraveného rozpočtu, skutočné čerpanie rozpočtových prostriedkov k 31. decembru 2023 a percentuálne vyhodnotenie plnenia k upravenému rozpočtu:



Záväzné ukazovatele rozpočtu úradu pre rok 2023 schválené zákonom č. č. 526/2022 Z. z. o štátnom rozpočte na rok 2023 zo dňa 22. decembra 2022 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 Z. z. o rozpočtových pravidlách verejnej správy, zákona č. 357/2015 Z. z. o finančnej kontrole a audite, zákona č. 343/2015 Z. z. 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 2023 (v eurách)

*evidenčný počet zamestnancov k 31.12.2022 (bez materských a rodičovských dovoleniek)

UKAZOVATELE	SCHVÁLENÝ ROZPOČET	UPRAVENÝ ROZPOČET	SKUTOČNOSŤ K 31.12.2022	PLNENIE K UPR. ROZPOČTU
I. Príjmy kapitoly	**20 000,00**	**20 000,00**	**32 680,43**	**163,40%**
A. Záväzný ukazovateľ	20 000,00	20 000,00	32 680,43	163,40%
B. Prostriedky Európskej únie	0,00	0,00	0,00	
II. Výdavky kapitoly celkom (A + B+ C + C.1)	**14 612 255,00**	**19 658 606,55**	**19 423 072,86**	**98,80%**
A. Výdavky spolu bez prostriedkov podľa § 17 ods. 4 zákona				
č. 523/2004 Z. z. a prostriedkov Európskej únie	**14 610 255,00**	**19 645 859,10**	**19 410 325,41**	**98,80%**
z toho:				
A.1. rozpočtové prostriedky kapitoly	14 610 255,00	15 296 338,21	15 085 854,44	98,62%
z toho: kód zdroja 111 + 11H + 11UA	14 610 255,00	15 115 288,21	14 906 166,52	98,65%
kód zdroja 131	0,00	181 050,00	179 687,92	99,25%
A.2. prostriedky na spolufinancovanie	0,00	1 099 972,83	1 087 357,54	98,85%
z toho: kód zdroja 1AC2	0,00	52 746,43	52 746,43	100,00%
kód zdroja 1AC3	0,00	78 985,66	77 117,32	97,63%
kód zdroja 3AA2	0,00	520 703,24	514 923,71	98,89%
kód zdroja 3AA3	0,00	447 537,50	442 570,08	98,89%
A.3. mzdy, platy, služ. príj. a ost. os. vyrovnania (610), kód zdroja 111+11H+11UA)	7 542 875,00	7 723 430,64	7 608 964,94	98,52%
toho: mzdy, platy, služ. príjmy a ost. os. vyrovnania aparátu ústred.				
orgánu (kód zdroja 111 + 11H + 11UA)	7 542 875,00	7 723 430,64	7 608 964,94	98,52%
Počet zamestnancov RO podľa prílohy č. 1 k uzneseniu vlády SR č. 577/2021	254 osôb	254 osôb	223 osôb*	87,80%
z toho: aparát ústredného orgánu	254 osôb	254 osôb	223 osôb*	87,80%
administratívne kapacity rozp. organizácií osobitne sledované podľa prílohy č. 1 k uzneseniu vlády SR č. 636/2022	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)	500 000,00	4 661 852,53	4 655 911,94	99,87%
z toho: kód zdroja 111	500 000,00	739 552,40	734 973,89	99,38%
kód zdroja 131L	0,00	181 050,00	179 687,92	99,25%
kód zdroja 1AA1	0,00	1 414 883,84	1 414 883,84	100,00%
kód zdroja 3AA1	0,00	1 402 015,62	1 402 015,62	100,00%
kód zdroja 3AA2	0,00	497 099,91	497 099,91	100,00%
kód zdroja 3AA3	0,00	427 250,76	427 250,76	100,00%
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**	**12 747,45**	**12 747,45**	**100,00%**
C. Prostriedky Európskej únie	**0,00**	**3 249 548,06**	**3 237 113,43**	**99,62%**
z toho: kód zdroja 3AA1	0,00	1 486 507,24	1 486 507,24	100,00%
kód zdroja 1AC1	0,00	298 896,42	298 896,42	100,00%
kód zdroja 3AA1	0,00	1 464 144,40	1 451 709,77	99,15%
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	**14 612 255,00**	**19 658 606,55**	**19 423 072,86**	**98,80%**
0D9 Bezpečnosť informácií	14 477 770,00	15 596 990,67	15 402 034,64	98,75%
0EK0U Informačné technológie financované zo štátneho rozpočtu – NBÚ	134 485,00	142 723,48	125 327,42	87,81%
0EJ0P Informačná spoločnosť 2014-2020 - MF SR - NBÚ	0,00	3 918 892,40	3 895 710,82	99,41%
E. Systemizácia policajtov v štátnej službe	**232 osôb**	**232 osôb**	**206 osôb***	**88,79%**
	6 875 982,00	**7 042 723,72**	**7 030 330,49**	**99,82%**

ROZPOČET NA ROK 2024

Zákonom č. 534/2023 o štátnom rozpočte na rok 2024 boli schválené a oznámené záväzné ukazovatele štátneho rozpočtu jednotlivých kapitol na rok 2024.

Výdavky úradu pre rok 2024 sú rozpočtované v rámci programu 0D9 – Bezpečnosť informácií a medzirezortného podprogramu 0EK0U – Informačné technológie financované zo štátneho rozpočtu – NBÚ v celkovej sume 15 881 633 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.

V projekte Elektronické služby spracovania bezpečnostných spisov NBÚ – malé zlepšenie eGov služieb, ktorý je realizovaný v operačnom programe Integrovaná infraštruktúra prebiehali v roku 2023 hlavné aktivity v realizačnej fáze projektu v súlade s vyhláškou Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 85/2020 o riadení projektov.

Cieľom projektu je zavedenie plne elektronických služieb NBÚ v oblasti bezpečnostných previerok pre občanov a podnikateľov a vybudovanie Informačného systému spracovávania bezpečnostných spisov NBÚ.

V štvrtom kvartáli roku 2023 začal úrad s realizáciou ďalších dvoch projektov priamo financovaných Európskou úniou v rámci programu Digitálna Európa:
- projekt NIS2 Implementácia v Slovenskej republike
- projekt Testovacie a certifikačné kapacity na Slovensku

Efektívna verejná správa – model CAF

Po dvojročnej intenzívnej realizácii projektu bol po úspešnom obhájení realizovanej externej spätnej väzby udelený Národnému bezpečnostnému úradu významný a medzinárodne uznávaný titul Efektívny používateľ modelu CAF

V rebríčku kategórie „Ústredné orgány štátnej správy“ sa Národný bezpečnostný úrad umiestnil na 1. mieste.

VEREJNÉ OBSTARÁVANIE

Analytici z portálu Transparex.sk zostavili rebríček „Zodpovedných verejných obstarávateľov“. V roku 2023 v ňom figurovali všetky štátne organizácie, samosprávy, ústredné orgány štátnej správy, vrátane nemocníc, podnikov vo vlastníctve štátu, materské škôlky a školy.

Národný bezpečnostný úrad si obhájil titul veľmi zodpovedný obstarávateľ s výslednou známkou A+ a hodnotením 77,6 bodov. Z hodnotenia vyplýva, že verejné obstarávanie sa realizuje profesionálne, rýchlo, s dôrazom na vysokú hospodárnosť a zabezpečenie čestnej hospodárskej súťaže.

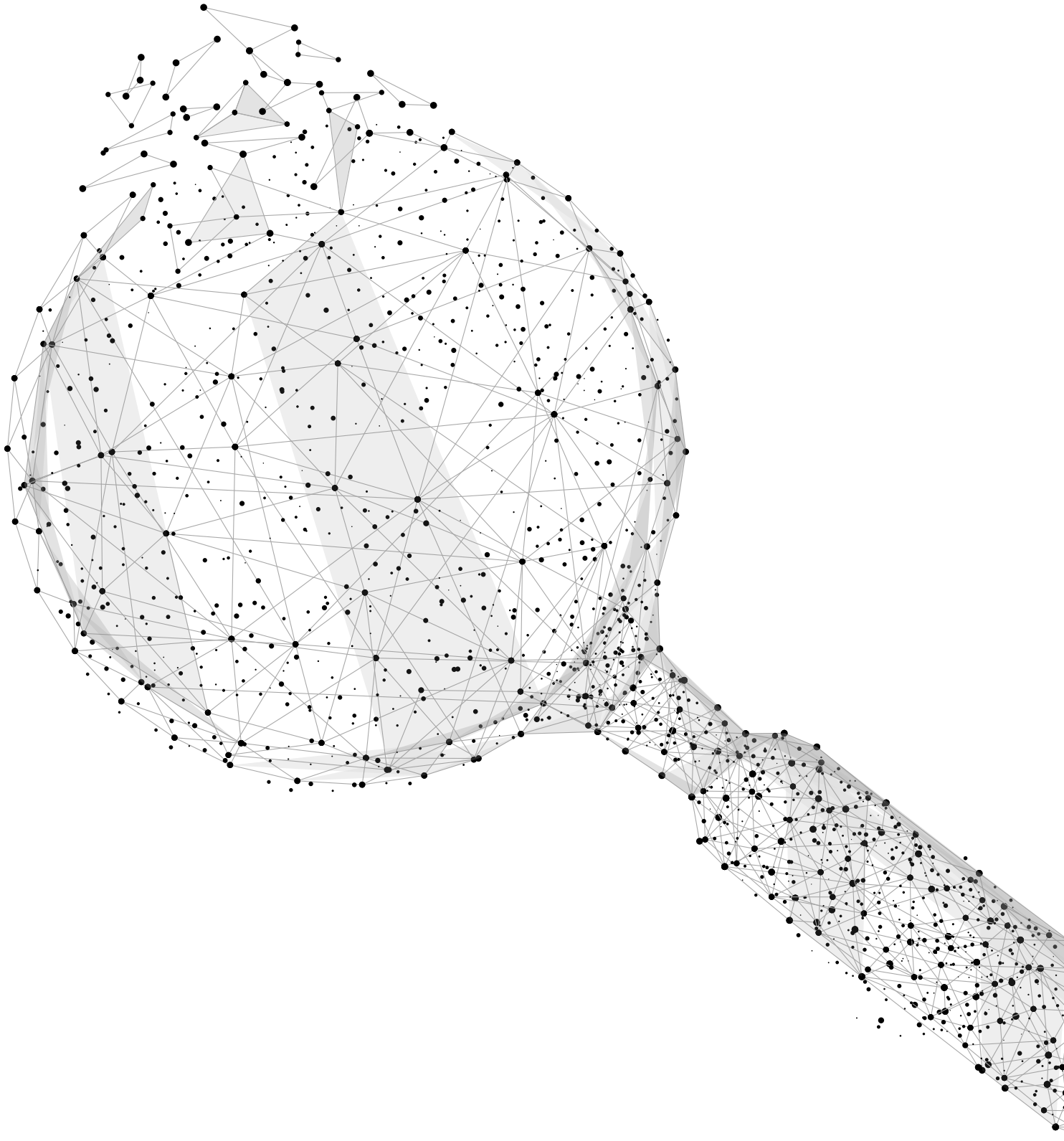
NÁRODNÁ KULTÚRNA PAMIATKA – KAŠTIEĽ BRUNOVCE

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.

Vzhľadom na nevyhovujúci technický stav tejto národnej kultúrnej pamiatky, úrad ešte 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.

Minulý rok boli zrealizované reštaurátorský výskum a architektonicko-historický výskum kaštieľa. Na základe vypracovanej správy bolo vydané rozhodnutie, v ktorom Krajský pamiatkový úrad v Trenčíne schválil návrh na reštaurovanie. V súčasnosti je v procese realizácie vypracovanie projektovej dokumentácie a následne budú vykonané aktivity súvisiace so stavebno-technickou obnovou a implementáciou zelených opatrení s predĺžením životnosti a možnosti širšieho využitia tejto národnej kultúrnej pamiatky.

KONTROLA A AUDIT



KONTROLNÁ ČINNOSŤ

Národný bezpečnostný úrad vykonal kontrolu naprieč všetkými úsekmi pôsobnosti zverenej zákonmi v 37 subjektoch. Kontroly boli vykonané v štátnych orgánoch, u podnikateľov a v jednej medzinárodnej organizácii:

- kontroly podľa zákona č. 215/2004 o ochrane utajovaných skutočností **14 subjektov** (8 štátnych orgánov a 6 držiteľov potvrdenia o priemyselnej bezpečnosti)
- kontrola podľa zákona 272/2016 o dôveryhodných službách **4 subjekty**
- kontrola podľa zákona 69/2018 o kybernetickej bezpečnosti **18 subjektov**
- kontrola plnenia záväzkov z členstva v NATO **1 subjekt**

Kontrolné skupiny sa zamerali najmä na komplexnosť prijatých opatrení a ich koordináciu naprieč jednotlivými oblasťami bezpečnosti.
Nedostatky = v 25 kontrolovaných subjektoch.
Kontrolné skupiny zaznamenali 83 kontrolných zistení:

- 15 na úseku ochrany utajovaných skutočností,
- 67 na úseku kybernetickej bezpečnosti,
- 1 na úseku dôveryhodných služieb.

DOHĽADOVÁ ČINNOSŤ

Úrad vykonával činnosti dohľadu s cieľom zaručiť prostredníctvom *ex ante a ex post* dohľadu, aby kvalifikovaní poskytovatelia dôveryhodných služieb a nimi poskytované kvalifikované dôveryhodné služby, spĺňali požiadavky stanovené v nariadení eIDAS.

Činnosti dohľadu sa týkali najmä analýzy správ o posúdení zhody v prípade pravidelných 24 mesačných auditov a procesu udeľovania kvalifikovaných štatútov, ohlasovacích povinností kvalifikovaných poskytovateľov dôveryhodných služieb pri zmenách pri poskytovaní kvalifikovaných služieb, dohľadu vykonaného na základe podnetov od externých subjektov, kontroly či neposkytujú služby, pre ktoré im nebol udelený kvalifikovaný štatút a kontroly dodržiavania národnej legislatívy pre oblasť dôveryhodných služieb.

Pri predbežnom dohľade boli analyzované správy o posúdení zhody od štyroch kvalifikovaných poskytovateľov dôveryhodných služieb. Bolo udelených osem kvalifikovaných štatútov na kvalifikovanú dôveryhodnú službu.

Zastavené konanie bolo u jedného kvalifikovaného poskytovateľa dôveryhodných služieb na udelenie dvoch kvalifikovaných štatútov z dôvodu nesplnenia požiadaviek nariadenia eIDAS.

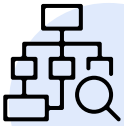
Pri následnom dohľade boli analyzované správy o posúdení zhody, teda doručené správy z pravidelného 24-mesačného auditu od piatich kvalifikovaných poskytovateľov dôveryhodných služieb.

METODICKÁ ČINNOSŤ

Z dôvodu vymenovania historicky prvej úradníckej vlády v ére samostatného Slovenska v máji 2023 boli na základe rozhodnutia riaditeľa úradu jej jednotlivým členom poskytnuté informácie k vybraným aspektom ochrany utajovaných skutočností vo forme prezentácie, prehľadných grafických manuálov so zoznamom opatrení na zachovanie bezpečnosti štátu a predchádzanie krízových situácií.

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. NBÚ ich následne anonymizuje a zverejňuje na svojom webovom sídle. Úrad vydal 175 metodických usmernení a odborných stanovísk:

V OBLASTI OCHRANY UTAJOVANÝCH SKUTOČNOSTÍ	**85**
PERSONÁLNA BEZPEČNOSŤ	32
ADMINISTRATÍVNA BEZPEČNOSŤ	13
PRIEMYSELNÁ BEZPEČNOSŤ	17
FYZICKÁ BEZPEČNOSŤ A OBJEKTOVÁ BEZPEČNOSŤ	10
BEZPEČNOSŤ TECHNICKÝCH PROSTRIEDKOV	4
BEZPEČNOSTNÍ ZAMESTNANCI	1
LETECKÉ SNÍMKOVANIE	3
CUDZIA MOC	**9**
V OBLASTI ŠIFROVEJ OCHRANY INFORMÁCIÍ	2
V OBLASTI KYBERNETICKEJ BEZPEČNOSTI	47
V OBLASTI DÔVERYHODNÝCH SLUŽIEB	22
PRIEREZOVÉ STANOVISKÁ	24



VNÚTORNÁ KONTROLA

NBÚ rozvíjal odborné spôsobilosti pracovníkov vnútornej kontroly ich vyslaním na vzdelávanie v Inštitúte pre verejnú správu. Sekcia vnútornej bezpečnosti v súčinnosti s ďalšími útvarmi vykonala 8 vnútorných kontrol podľa zákona č. 10/1996 o kontrole v štátnej správe.

Kontroly boli zamerané na dodržiavanie času služby príslušníkov a zamestnancov úradu, prideľovanie a evidovanie služobných zbraní a streliva, kontrolu služobných preukazov, vyšetrenia na zistenie alkoholu v krvi príslušníkov a zamestnancov úradu, kontrolu dodržiavania povinnosti vyplývajúcich zo zákona č. 278/1993 o správe majetku štátu a kontrolu za vybranú oblasť administratívnej bezpečnosti ochrany utajovaných skutočností.

Okrem nepatrných formálnych administratívnych nedostatkov nebolo pri kontrolách zistené porušenie všeobecne záväzných právnych predpisov.

VNÚTORNÝ AUDIT

Útvarom vnútorného auditu boli vykonané 4 plánované vnútorné audity, ktorých cieľom bolo overiť a hodnotiť:

- dodržiavanie zákona č. 10/1996 o kontrole v štátnej správe za rok 2022 v povinnej osobe NBÚ,
- hospodárnosť, efektívnosť, účinnosť a účelnosť pri hospodárení s verejnými financiami za rok 2022 a do 9. 8. 2023 v povinnej osobe NBÚ,
- hospodárnosť, efektívnosť, účinnosť a účelnosť pri hospodárení s verejnými financiami za rok 2022 v povinnej osobe Kompetenčné a certifikačné centrum kybernetickej bezpečnosti.

Vykonanými vnútornými auditmi bolo zistených 9 nedostatkov:
1 nedostatok nízkej závažnosti, nesystémový – finančne nevyčísliteľný,
4 nedostatky strednej závažnosti, systémové – finančne nevyčísliteľné,
4 nedostatky strednej závažnosti, nesystémové – finančne nevyčísliteľné.

Povinným osobám 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.

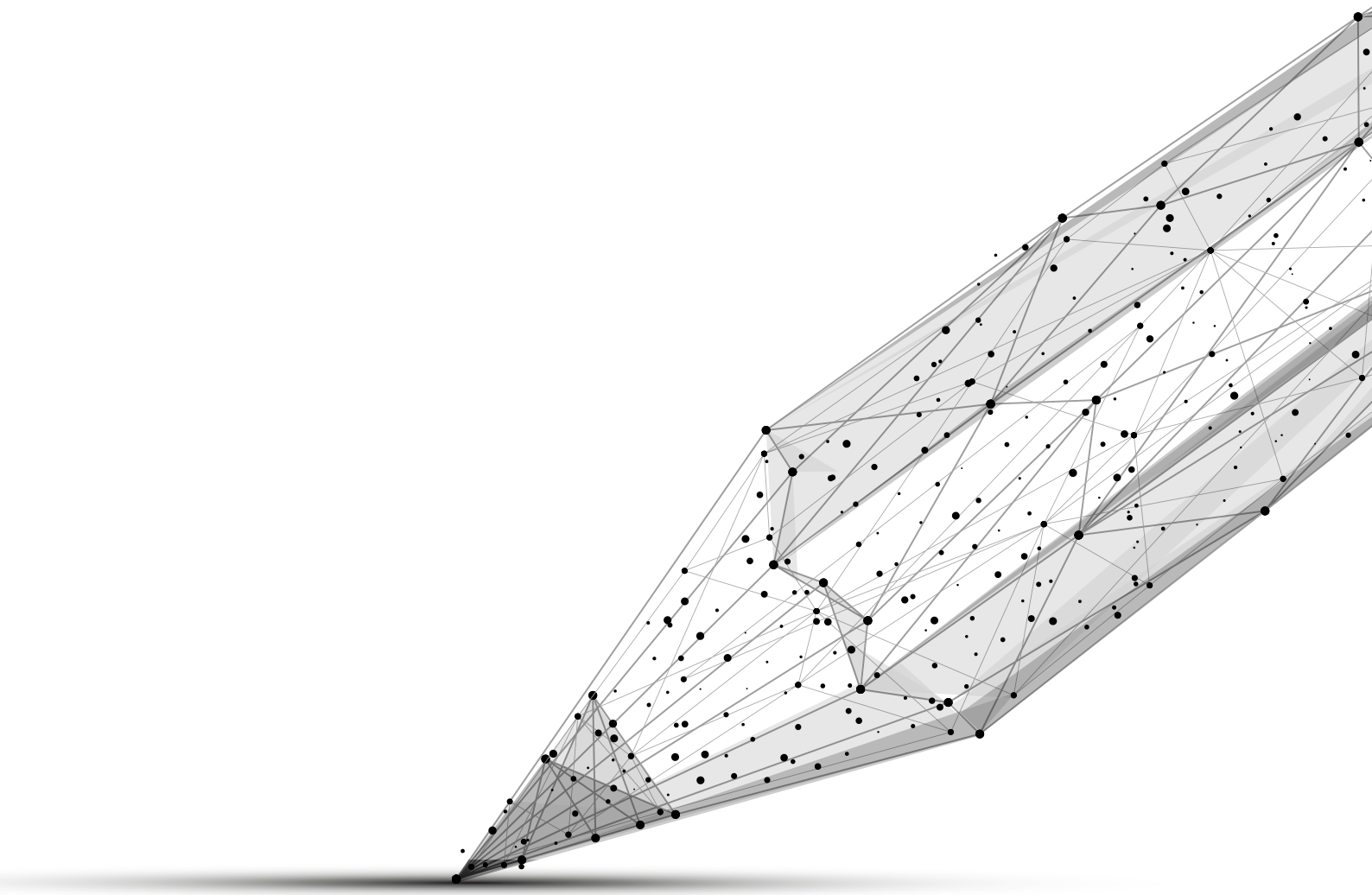
BEZPEČNOSTNÉ RIZIKÁ

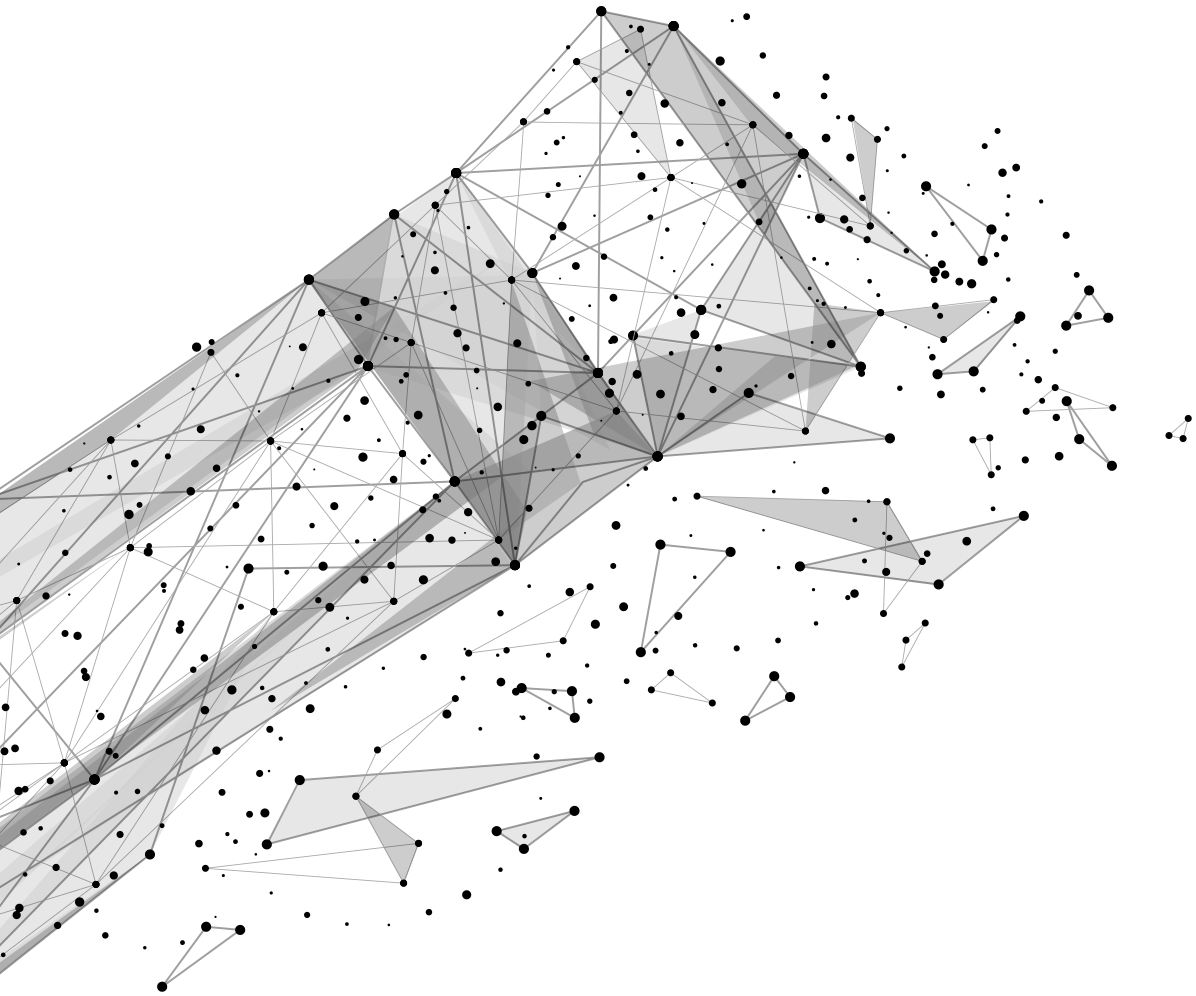
Národný bezpečnostný úrad vykonával svoju pôsobnosť na úseku vnútornej ochrany a získaval, sústreďoval, analyzoval a preveroval informácie o bezpečnostných rizikách týkajúcich sa pôsobnosti úradu a jeho príslušníkov a zamestnancov.

SŤAŽNOSTI A PETÍCIE

Úradu boli doručené 3 sťažnosti, ktoré úrad prešetrením/prekontrolovaním vyhodnotil ako neopodstatnené a 1 podanie označené ako sťažnosť, ktoré však podľa obsahu nebolo sťažnosťou v zmysle zákona č. 9/2010 o sťažnostiach. V roku 2023 nebola úradu doručená žiadna petícia.

PRIORITY
NA ROK 2024





Finalizujeme projekty:

Elektronické služby spracovania bezpečnostných spisov NBÚ – malé zlepšenie eGov služieb a intenzívne pracujeme na ďalších troch projektoch

Zvyšovanie efektívnosti riadenia verejných politík v oblasti kybernetickej bezpečnosti 2023 – 2024

Intenzívne pracujeme na projektoch:

Vybudovanie fyzickej a objektovej bezpečnosti
Implementácia NIS2 v Slovenskej republike
Testovacie a certifikačné kapacity na Slovensku

V priebehu roka bude novelizovaný registratúrny poriadok aj registratúrny plán úradu. Jednou z priorít úradu je aj spustenie integrácie vonkajšieho prostredia s elektronickým informačným systémom pre správu registratúry a naďalej k prioritám úradu patrí spustenie integrácie elektronického informačného systému pre správu registratúry s vonkajším prostredím.