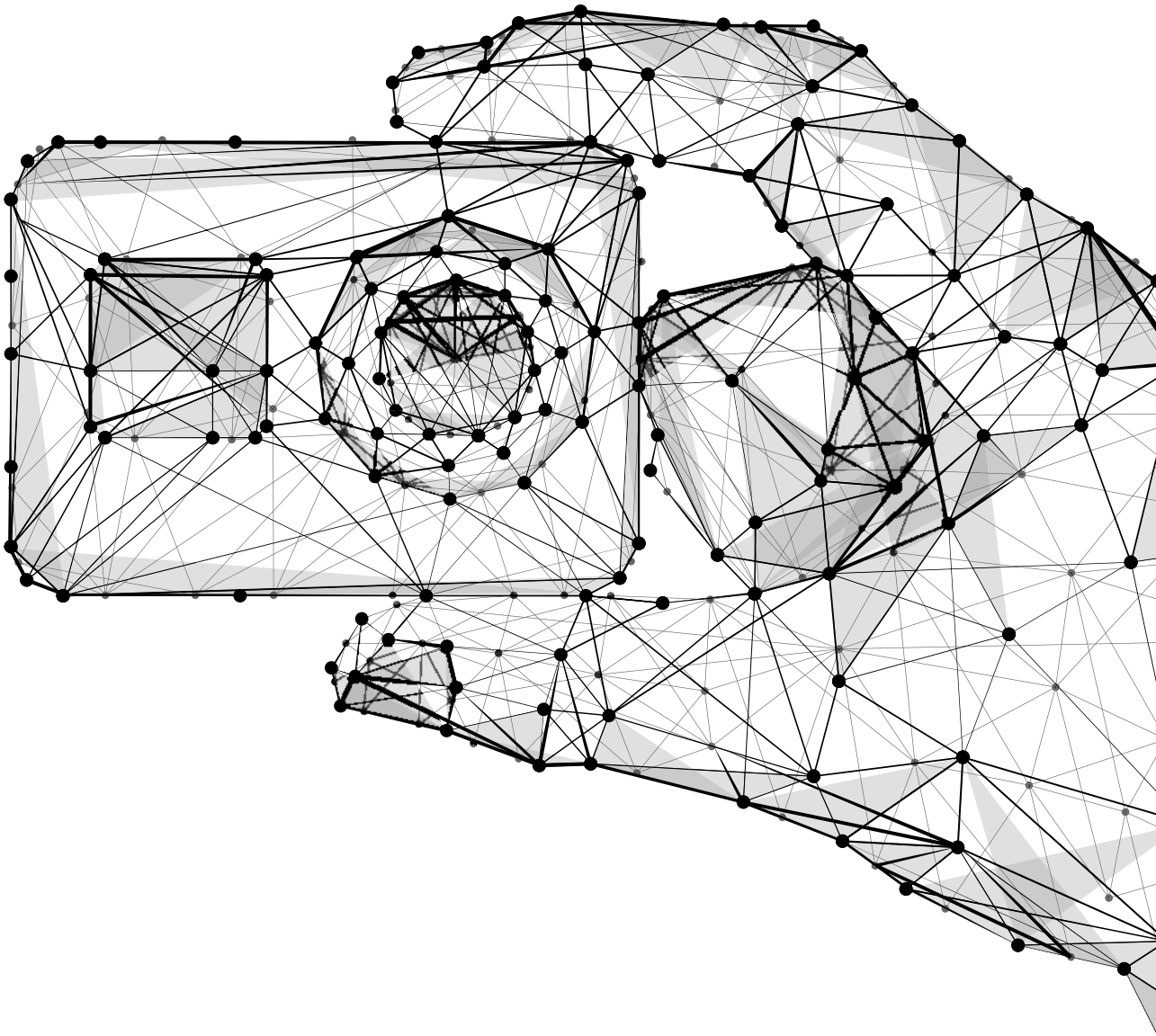
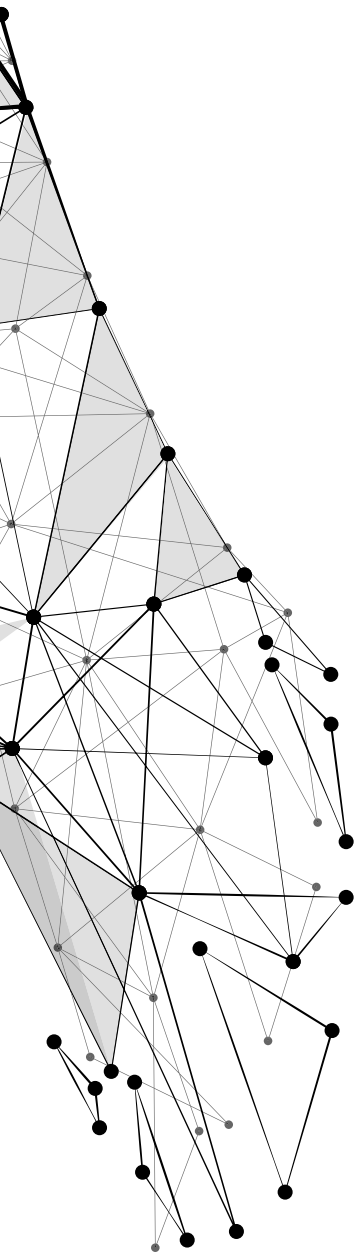
NÁRODNÝ
BEZPEČNOSTNÝ
ÚRAD

SPRÁVA O ČINNOSTI V ROKU 2022

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 neposled-

nom 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.

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 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

Úrad sa pri plnení stanovených úloh riadi Ústavou Slovenskej republiky, ústavnými zákonmi, právne záväznými aktmi Európskej únie, medzinárodnými zmluvami, zákonmi a ďalšími všeobecne záväznými právnymi predpismi, uzneseniami vlády Slovenskej republiky, svojím štatútom, organizačným poriadkom a ostatnými internými právnymi predpismi upravujúcimi vnútorné procesy úradu.

Pri plnení úloh v oblasti ochrany utajovaných skutočností a šifrovej ochrany informácií sa úrad riadi zákonom č. 215/2004 o ochrane utajovaných, súvisiacimi vykonávacími predpismi a platnými štandardmi.

V oblasti certifikácie produktov pre dôveryhodné služby úrad postupuje podľa nariadenia eIDAS (nariadenie Európskeho parlamentu a Rady EÚ č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu), jeho vykonávacích rozhodnutí a podľa zákona č. 272/2016 o dôveryhodných službách pre elektronické transakcie na vnútornom trhu.

Pri plnení úloh v oblasti kybernetickej bezpečnosti a akreditácie jednotiek CSIRT postupuje úrad podľa zákona o kybernetickej bezpečnosti č. 69/2018 a podľa príslušných vyhlášok vydaných na vykonanie zákona.

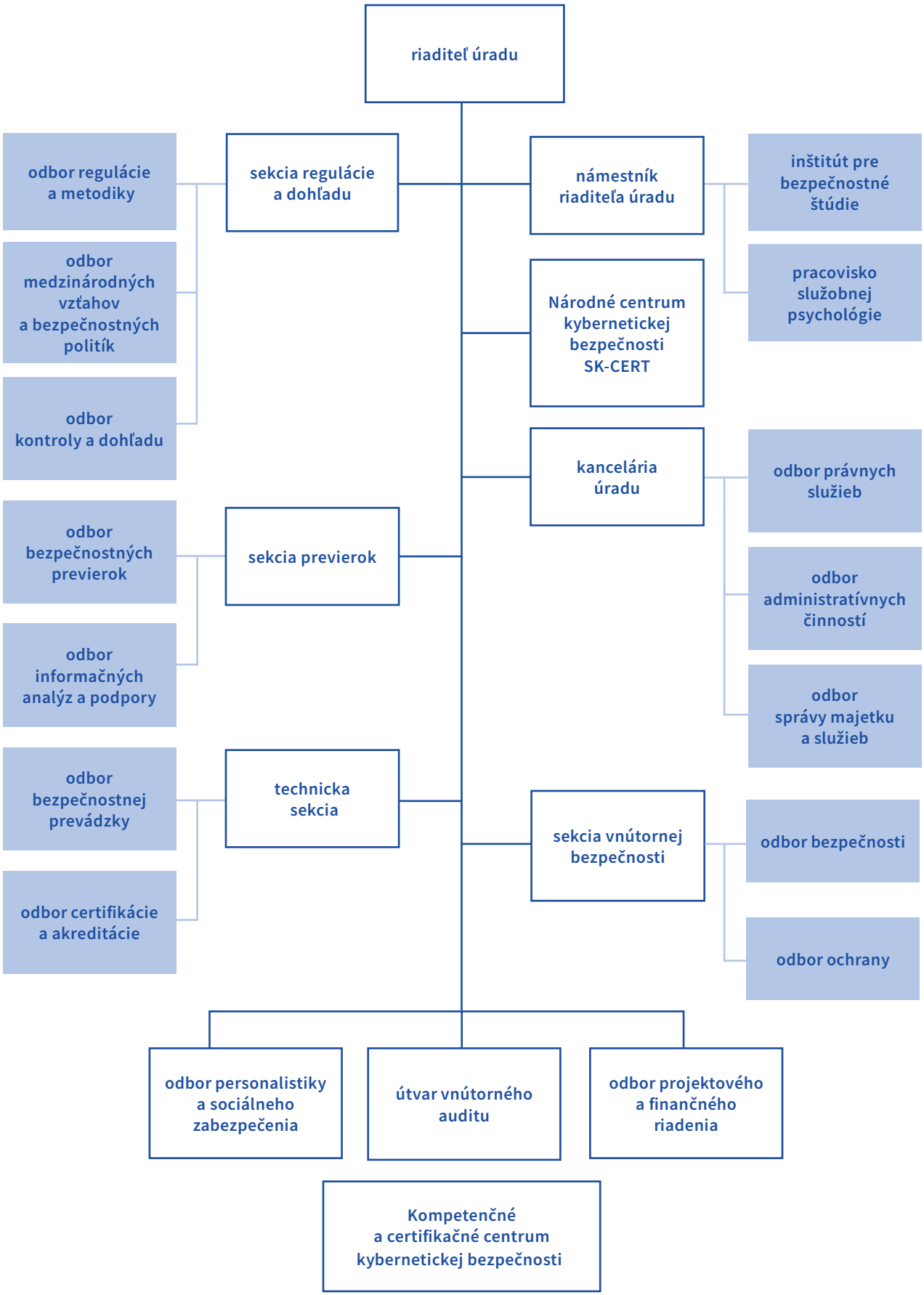
VEDENIE ÚRADU

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

Organizačne sa úrad člení na útvary – sekcie a priamo riadené odbory, sekcie sa ďalej členia na odbory.



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

v oblasti personálnej bezpečnosti a priemyselnej bezpečnosti vykonáva činnosti súvisiace s realizáciou bezpečnostných previerok fyzických osôb a podnikateľov.

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, politiku správania sa v kybernetickom priestore, zásady predchádzania kybernetickým bezpečnostným incidentom a zásady ich riešenia. 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.

Prostredníctvom styčných dôstojníkov, vyslaných k zastupiteľskému úradu SR pri EÚ a k stálej delegácii NATO, plní úlohy pri rozvíjaní a budovaní medzinárodných vzťahov a spolupráce úradu v zahraničí. Styční dôstojníci zabezpečujú komunikáciu medzi úradom a zahraničnými partnermi, zastupujú záujmy Slovenskej republiky v oblastiach zverených do právomoci úradu v NATO, v európskych inštitúciách a agentúrach a realizujú bilaterálnu a multilaterálnu spoluprácu úradu v zahraničí.

Národné centrum kybernetickej bezpečnosti SK-CERT

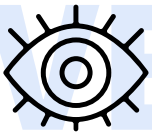
plní úlohy národnej jednotky CSIRT. Zabezpečuje služby spojené s riadením bezpečnostných incidentov, odstraňovaním ich následkov a následnou obnovou činnosti informačných systémov v spolupráci s ich vlastníkmi a prevádzkovateľmi, ale aj výkon analytických činností, výskumu, rozširovania bezpečnostného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

Technická sekcia

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 systémov utajovaného vládneho a utajovaného zahraničného spojenia a taktiež vykonáva bezpečnostný dohľad sieťových a aplikačných parametrov komunikačných a informačných systémov na ochranu utajovaných skutočností.

Odbor personalistiky a sociálneho zabezpečenia

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



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 a finančnú 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 a ochrany pred požiarmi a zabezpečuje telesnú prípravu príslušníkov.

Odbor projektového a finančného riadenia

zabezpečuje projektové a programové riadenie v podmienkach úradu.

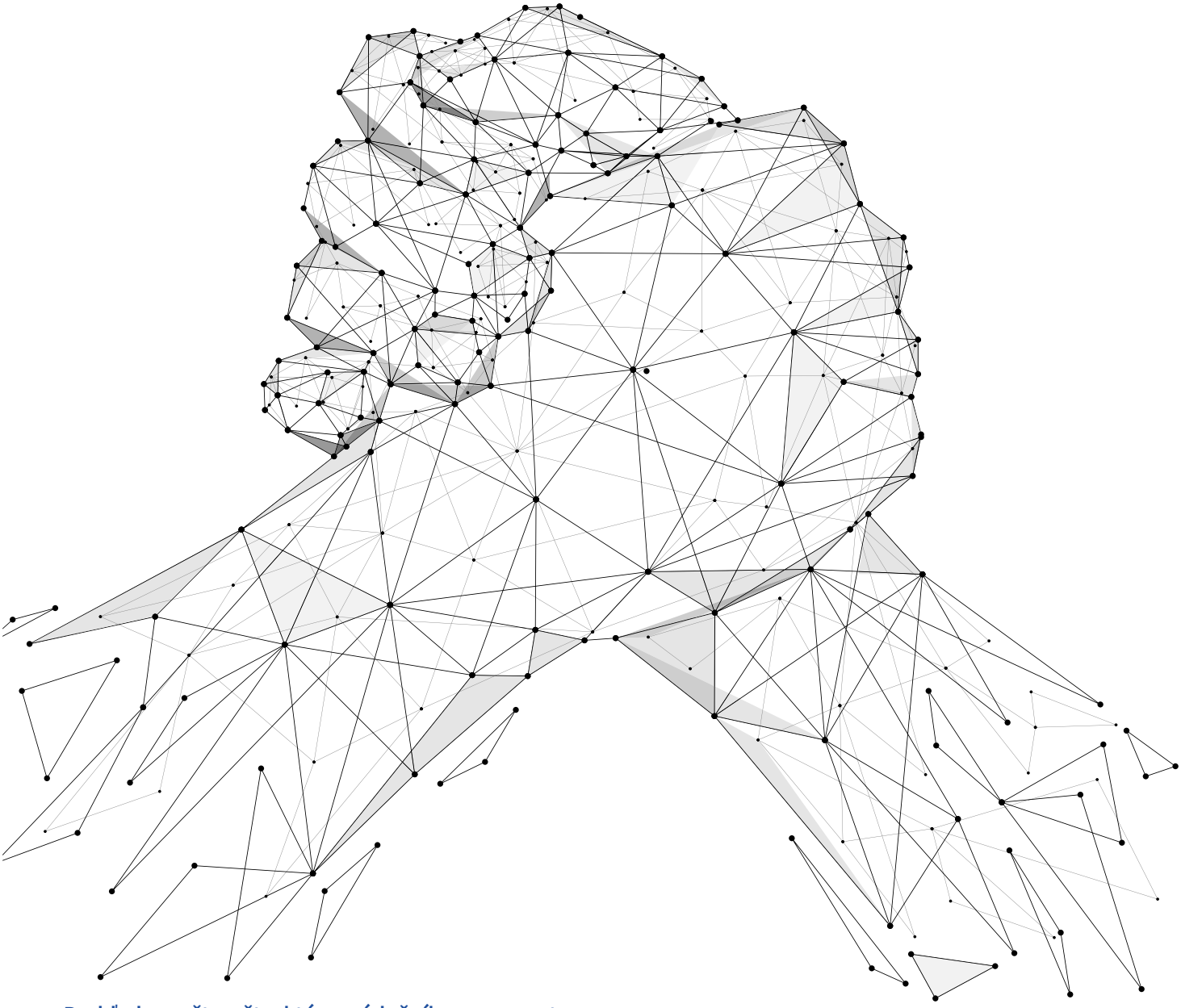
Útvar vnútorného auditu

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.

ĽUDSKÉ ZDROJE



Prehľad o počte a štruktúre príslušníkov a zamestnancov

	Štátna služba		Zamestanci		Príslušníci a zamestanci	
Prípravná štátna služba	**34**	16,35%				
Stála štátna služba	**172**	82,69%				
Dočasná štátna služba	**2**	0,96%				
Spolu	**208**	90,43%	**22**	9,57%	**230**	100%

Veková štruktúra príslušníkov a zamestnancov

	Príslušníci		Zamestanci		Príslušníci a zamestanci	
do 34 rokov	40	19,23%	4	18,8%	44	19,13%
35 — 49 rokov	125	60,1%	9	40,91%	134	58,26%
50 — 59 rokov	39	18,75%	5	22,73%	44	19,13%
60 a viac rokov	4	1,92%	4	18,18%	8	3,48%
Spolu	208	90,43%	22	9,57%	230	100%

Ženy a muži v NBÚ

	Príslušníci		Zamestanci		Príslušníci a zamestanci	
ženy	107	51,44%	12	54,54%	119	51,73%
muži	101	48,56%	10	45,46%	111	48,27%
Spolu	208	90,43%	22	9,57%	230	100%

Vzdelanostná štruktúra príslušníkov a zamestnancov

Príslušníci			Zamestanci	
0	0%	Základné vzdelanie	0	0%
33	15,87%	Úplné stredné vzdelanie	10	44,45%
7	3,37%	Vysokoškolské vzdelanie I.st.	0	0%
160	76,92%	Vysokoškolské vzdelanie II.st.	11	50%
8	3,85%	Vysokoškolské vzdelanie III.st.	1	4,55%
208	90,43%	Spolu	22	100%

PREHLBOVANIE KVALIFIKÁCIE A ZVYŠOVANIE ZRUČNOSTÍ

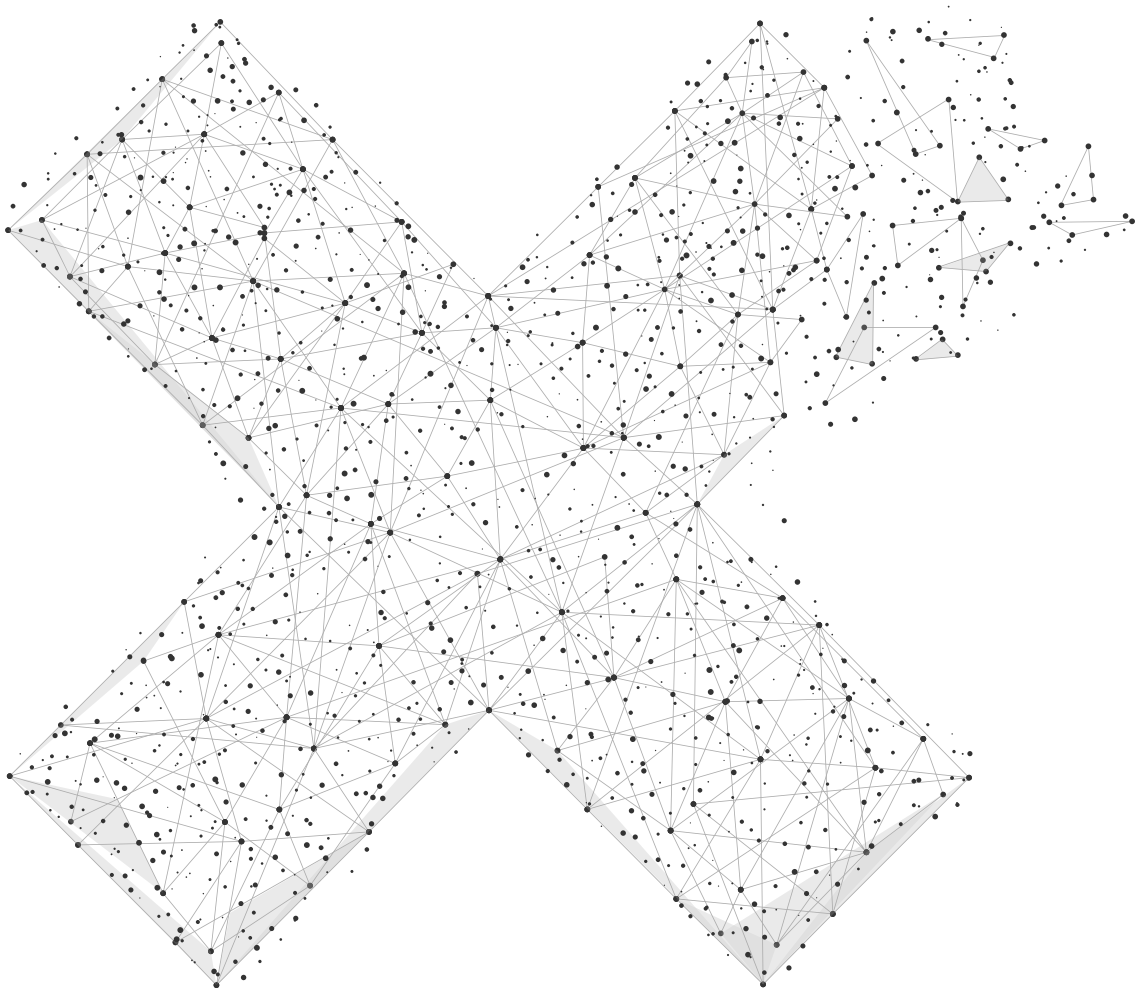
Úrad sa snažil nepretržite zefektívňovať proces vzdelávania so zámerom prispieť k posilneniu odborného a kvalitného personálneho zázemia úradu, k podpore osobnostného a profesionálneho rastu a vnútornej motivácii príslušníkov a zamestnancov úradu.

V podmienkach úradu je príslušníkom a zamestnancom umožnené udržiavať si odbornú pripravenosť, nadobúdať nové vedomosti, zručnosti a prehlbovať kvalifikáciu na odborných kurzoch, seminároch a školeniach doma i v zahraničí. V prípade potreby im umožňuje zvýšiť si kvalifikáciu na vysokých školách.

Príslušníci aj zamestnanci štandardne absolvovali vstupné školenia a sú pravidelne preškoľovaní v oblasti bezpečnosti a ochrany zdravia pri práci a takisto ochrany pred požiarmi.

Pre novoprijatých príslušníkov každoročne realizuje špecializované policajné vzdelávanie, ktoré je podmienkou pre zaradenie novoprijatých príslušníkov do stálej štátnej služby.

Príslušníci a zamestnanci úradu majú vytvorené vhodné podmienky na zvyšovanie fyzickej kondície. Najmä príslušníci sekcie vnútornej bezpečnosti pravidelne absolvujú cvičné streľby, taktické cvičenia aj simulované bezpečnostné scenáre vo viacerých objektoch ministerstva vnútra a ministerstva obrany.



BOJ PROTI KORUPCII

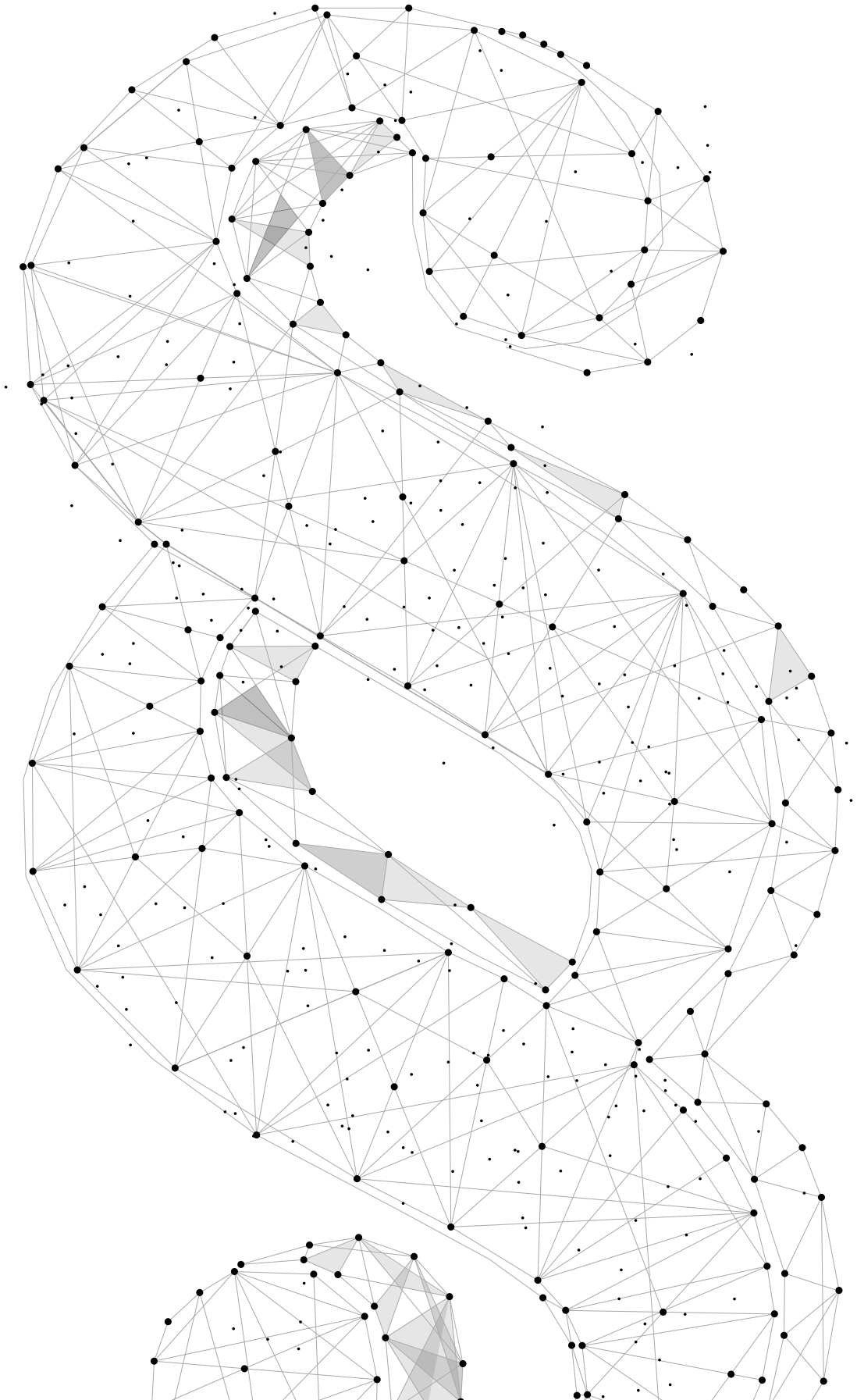
Protikorupčný program úradu je nástrojom na posilňovanie a presadzovanie protikorupčnej kultúry a zdokonaľovanie riadenia a rozpoznávania korupčných rizík v podmienkach úradu.

Vo svojom protikorupčnom programe úrad posudzuje a vyhodnocuje existujúce korupčné riziká a zavádza konkrétne systémové opatrenia zamerané na prevenciu korupcie a podporu protikorupčného správania na úrade.

Úrad v roku 2022 aktualizoval existujúci Protikorupčný program úradu, ktorý má 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. Národný bezpečnostný úrad nedostal v roku 2022 žiadne oznámenie o protispoločenskej činnosti vo vzťahu ku svojim príslušníkom.

LEGISLATÍVA



Rok 2022 zásadne ovplyvnila ruská vojenská invázia na Ukrajinu. Konflikt v blízkosti hraníc Slovenskej republiky ako členského štátu Organizácie Severoatlantickej zmluvy (NATO) a nové hybridné hrozby z Ruskej federácie upriamujú pozornosť na nevyhnutnosť zabezpečenia a zefektívnenia ochrany utajovaných skutočností.

Úrad v súvislosti s vojenským konfliktom na Ukrajine pristúpil v marci 2022 k **mimoriadnej novelizácii vyhlášky Národného bezpečnostného úradu č. 336/2004 o fyzickej bezpečnosti a objektovej bezpečnosti v znení vyhlášky č. 315/2006.** Opatrenie pomohlo Ministerstvu obrany Slovenskej republiky, ktoré malo interpretačné a aplikačné problémy v súvislosti s jej aplikáciou vo vzťahu k ochrane výrobkov obranného priemyslu, zbraní, zbraňových systémov alebo streliva, ktoré sú postupované Slovenskej republike zo zahraničia a sú utajovanými skutočnosťami alebo takéto utajované skutočnosti obsahujú.

Vláda navrhla balík mimoriadnych opatrení v zákone č. 55/2022 o niektorých opatreniach prijatých v súvislosti so situáciou na Ukrajine. Reagovala v ňom aj na narastajúci počet aktérov dezinformačnej legislatívnou zmenou **zákona č. 69/2018 o kybernetickej bezpečnosti.**

Ustanovila sa povinnosť úradu rozhodnúť o blokovaní škodlivého obsahu alebo škodlivej aktivity smerujúcej do alebo z kybernetického priestoru SR a zabezpečiť aj samotné vykonanie blokovania s platnosťou do 30. júna 2022. Zákonom č. 231/2022, ktorým sa mení a dopĺňa zákon č. 69/2018 sa neskôr predĺžila táto lehota do 30. septembra 2022.

Ešte v máji 2022 bol predložený do medzirezortného pripomienkového konania návrh zákona, ktorým sa mení a dopĺňa zákon č. 69/2018, ktorého cieľom bolo reflektovať na niektoré otázky aplikačnej praxe v súvislosti s výkonom blokovania, zodpovednosti, procesného postupu pri vydávaní rozhodnutia a jeho realizácii a úprava zverejňovania rozhodnutí na webovom sídle úradu. V novembri 2022 bol vládny návrh zákona predložený na rokovanie Národnej rady Slovenskej republiky (I. čítanie).

Ďalej úrad v roku 2022 zrealizoval legislatívny proces dvoch vykonávacích predpisov zákona č. 69/2018 o kybernetickej bezpečnosti. Pôvodný **návrh novely vyhlášky Národného bezpečnostného úradu č. 436/2019 o audite kybernetickej bezpečnosti a znalostnom štandarde audítora** sa v priebehu legislatívneho procesu transformoval na návrh novej vyhlášky o audite kybernetickej bezpečnosti s cieľom aktualizovať pravidlá výkonu auditu kybernetickej bezpečnosti, jeho časový rozsah trvania, periodicitu a stanovenie náležitosti záverečnej správy o výsledkoch auditu. Nová vyhláška Národného bezpečnostného úradu č. 493/2022 o audite kybernetickej bezpečnosti nadobudla účinnosť 1. januára 2023.

Vyhláška Národného bezpečnostného úradu č. 492/2022, ktorou sa ustanovujú znalostné štandardy v oblasti kybernetickej bezpečnosti má za cieľ určiť minimálne odborné znalosti pre jednotlivých používateľov sietí a informačných systémov vykonávajúcich činnosti a úlohy v oblasti kybernetickej bezpečnosti.

Znalostné štandardy rovnako tvoria rámec pre vytvorenie vzdelávacích programov na vzdelávacích inštitúciách, čím sa vypĺňa priestor nielen pre budovanie kvalitného bezpečnostného povedomia v oblasti kybernetickej bezpečnosti, ale aj pre zvyšovanie kvality vzdelávacích procesov. Prínosom bude teda aj kvalita pracovníkov vykonávajúcich činnosti v oblasti kybernetickej bezpečnosti v štátnych a v súkromných organizáciách.

Zavedenie a definovanie znalostných štandardov a ich aplikovanie v oblasti kybernetickej bezpečnosti

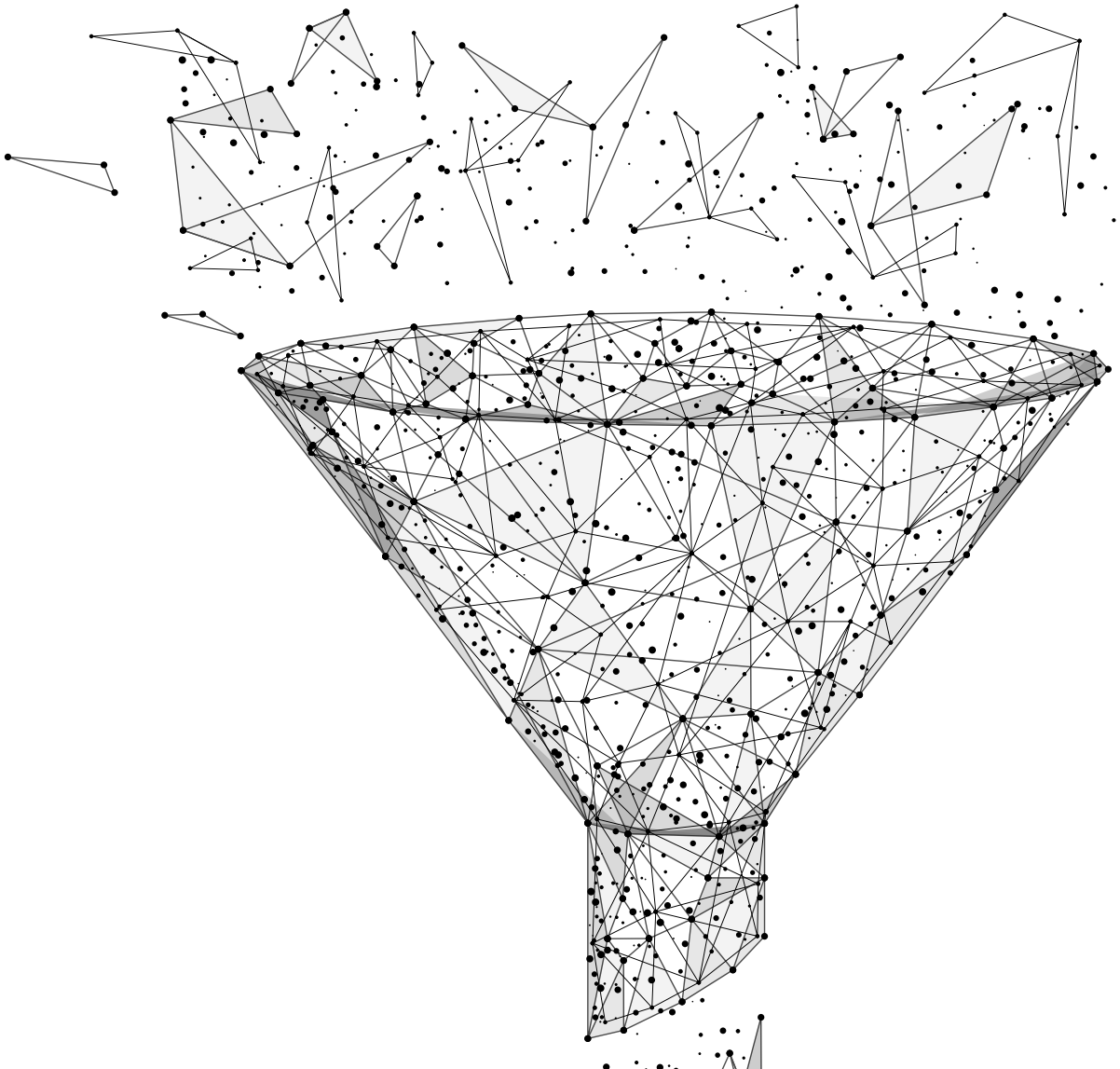
je základným prvkom budovania stabilného a predvídateľného bezpečnostného prostredia. Aj táto vyhláška nadobudla účinnosť 1. januára 2023.

Pri aplikácii **zákona č. 215/2004 o ochrane utajovaných skutočností** v praxi sa ako najproblematickejší javí fakt, že právna úprava na úrovni EÚ a NATO nepredstavuje jednotnú právnu úpravu v oblasti utajovaných skutočností pre členské štáty, ale vzťahuje sa len na ochranu pri manipulácii s utajovanými skutočnosťami, ktorých pôvodcom sú EÚ a/alebo NATO.

Rôznorodosť vnútroštátnej právnej úpravy členských štátov v oblasti utajovaných skutočností v medzinárodnej spolupráci viacerých štátov spôsobuje následne aplikačné problémy naprieč všetkými oblasťami bezpečnosti. Aj v tejto súvislosti mal úrad v roku 2022 snahu o priblíženie sa právnej úprave EÚ a NATO v tom zmysle, že pri pripomienkovaní relevantných právnych predpisov chcel viac uvoľniť ochranu utajovaných skutočností stupňa utajenia Vyhradené, no táto aktivita úradu nenašla pochopenie u iných orgánov verejnej moci, ktoré paradoxne požadujú skôr sprísnenie ochrany utajovaných skutočností stupňa utajenia Vyhradené.

Úrad sa napríklad snažil upraviť skutkovú podstatu v § 353 Trestného zákona tak, aby sa táto skutková podstata týkala iba utajovaných skutočností stupňa utajenia Dôverné. Ohrozenie alebo vyzradenie utajovanej skutočnosti stupňa utajenia Vyhradené by teda už nebolo trestným činom, ale iba priestupkom.

Úrad sa v Trestnom zákone snažil precizovať ustanovenia trestných činov týkajúcich sa ochrany utajovaných skutočností tak, aby uplatňovanie týchto ustanovení v praxi nekončilo na čisto formálnych nedostatkoch v podobe napríklad absentujúceho označenia utajovanej skutočnosti. Snahou úradu bolo viac previazať definície skutkových podstát trestných činov v oblasti utajovaných skutočností s definíciami stupňov utajenia v § 3 zákona č. 215/2004 najmä vo vzťahu k ujme na záujmoch Slovenskej republiky.



INTERNÉ PREDPISY

V roku 2022 vydala kancelária úradu **10 nariadení** riaditeľa úradu, **50 rozkazov** riaditeľa úradu a **2 štatúty** riaditeľa, ktoré majú zefektívniť vnútorné procesy a implementovať všeobecne záväzné právne predpisy.

Úrad vydal nové nariadenie, ktorým sa vymedzuje zodpovednosť riaditeľov útvarov pri plnení úloh vedúceho vyplývajúcich zo zákona č. 215/2004 o ochrane utajovaných skutočností; nariadenie, ktorým sa upravuje proces schválenia zriadenia registra utajovaných skutočností a koncového registra utajovaných skutočností; nariadenie o vykonaní psychofyziologického overenia pravdovravnosti; nariadenie o poskytovaní psychologickej starostlivosti a tiež boli novelizované nariadenie o tuzemských cestách, zahraničných cestách a prijatiach zahraničných delegácií a nariadenie o finančnom riadení a finančnej kontrole.

Nové štatúty boli vydané pre útvar inštitútu pre bezpečnostné štúdie a pracovisko služobnej psychológie.

Rozkazy riaditeľa úradu slúžili na určenie nositeľov konkrétnych úloh – napr. pri zriaďovaní projektových tímov, menovaní členov do rôznych komisií alebo inventarizácii majetku, či výkone špeciálnej a streleckej prípravy príslušníkov.

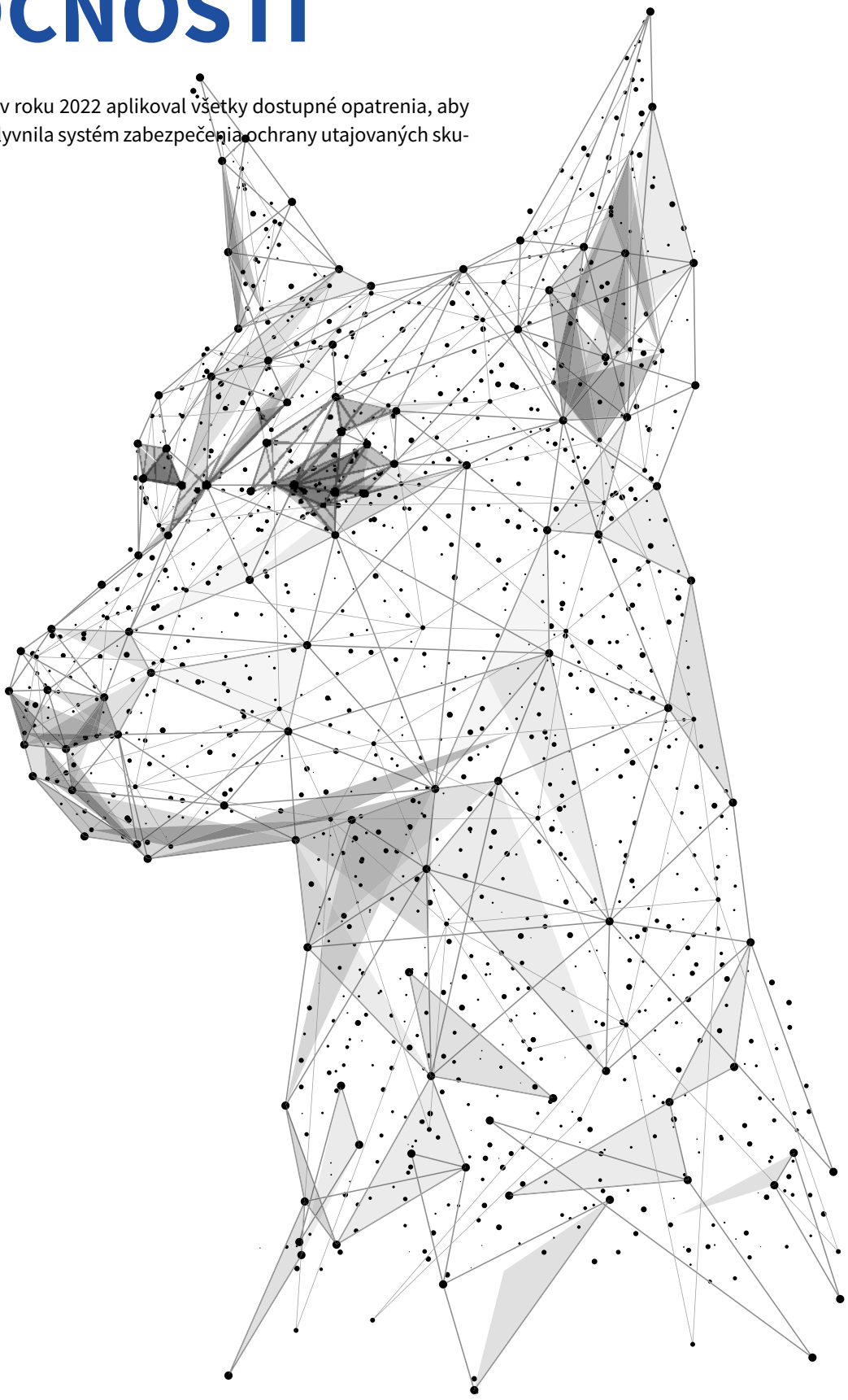
SPRÁVNE A PRIESTUPKOVÉ KONANIE

V roku 2022 úrad evidoval **17 podaní** vo veci podozrenia zo spáchania priestupku na úseku ochrany utajovaných skutočností podľa zákona č. 215/2004, z toho 14 podaní bolo vyhodnotených a evidovaných ako neoprávnená manipulácia s utajovanou skutočnosťou. Jedno podanie bolo odstúpené na prešetrenie príslušnému orgánu činnému v trestnom konaní.

Úrad uložil pokuty za spáchanie priestupku na úseku ochrany utajovaných skutočností v súhrnnej sume 150 eur a za spáchanie správneho deliktu na úseku ochrany utajovaných skutočností v súhrnnej sume 5 600 eur a na úseku kybernetickej bezpečnosti v sume 26 000 eur.

OCHRANA UTAJOVANÝCH SKUTOČNOSTÍ

Národný bezpečnostný úrad aj v roku 2022 aplikoval všetky dostupné opatrenia, aby pretrvávajúca pandémia neovplyvnila systém zabezpečenia ochrany utajovaných skutočností

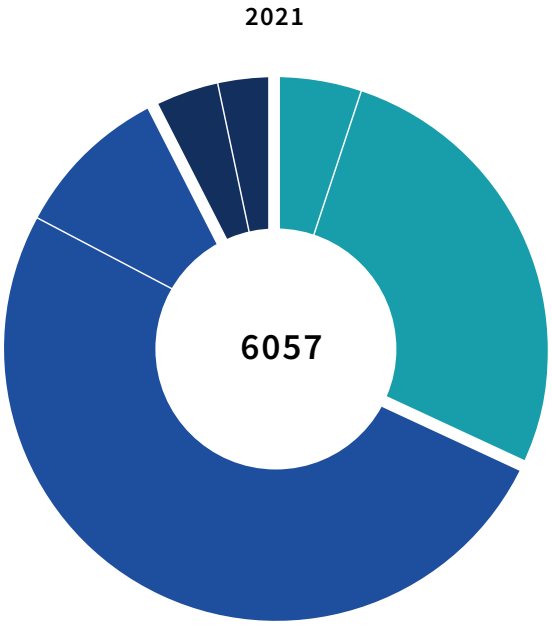


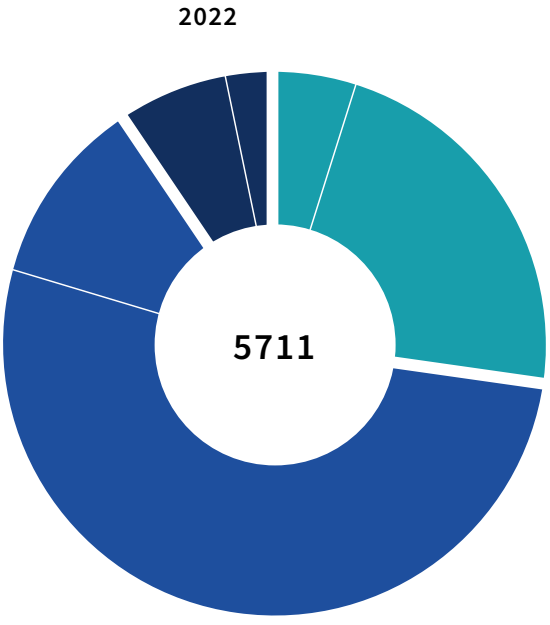
PERSONÁLNA BEZPEČNOSŤ

Vykonávanie bezpečnostných previerok fyzických osôb patrí ku kľúčovým činnostiam úradu. Úrad v roku 2022 vydal **5 711 osvedčení na oboznamovanie sa s utajovanými skutočnosťami,** z toho 3619 pre ministerstvo obrany.

Prehľad osvedčení vydaných v rokoch 2021 a 2022

Stupeň utajenia	2021	2022
DÔVERNÉ	**1947**	**1570**
z toho Dôverné pre MO SR	318	279
TAJNÉ	**3662**	**3614**
z toho Tajné pre MO SR	3034	2985
PRÍSNE TAJNÉ	**448**	**527**
z toho Prísne Tajné pre MO SR	278	355
Spolu	**6057**	**5711**





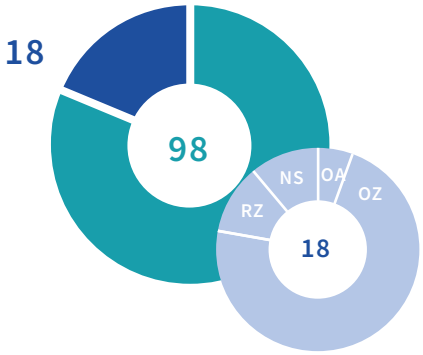
V roku 2022 úrad vydal 47 rozhodnutí. Proti rozhodnutiu úradu podali fyzické osoby 16 odvolaní.

Úrad rozhodol o 2 odvolaniach autoremedúrou.

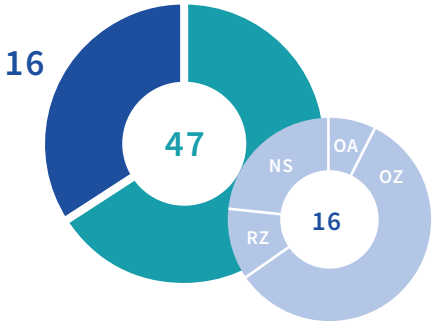
Výbor Národnej rady Slovenskej republiky na preskúmavanie rozhodnutí Národného bezpečnostného úradu rozhodol o **18 odvolaniach;** 15 z nich zamietol a 3 rozhodnutia zrušil. K 31.12.2022 bolo v odvolacom procese jedno odvolanie.

Proti rozhodnutiu výboru bolo na Najvyššom súde Slovenskej republiky podaných šesť žalôb. Prehľad informácií o rozhodnutiach úradu, odvolaniach a žalobách podaných na najvyšší súd sa nachádza v tabuľke č. 2.

2021



2022



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

	2021	2022
ROZHODNUTIA ÚRADU	**98**	**47**
ODVOLANIA	**18**	**16**
Odvolania – autoremedúra (OA)	1	2
Odvolania zamietnuté výborom (OZ)	13	15
Rozhodnutia zrušené výborom (RZ)	2	3
Podané žaloby na najvyššom súde (NS)	2	6

Vo vzťahu k **utajovaným skutočnostiam postupovaným NATO a EÚ** bolo navrhovaným osobám v roku 2022 vydaných **7 410 certifikátov**, z toho bolo vydaných 3 703 certifikátov NATO a 3707 certifikátov EÚ.

Z celkového počtu certifikátov NATO úrad vydal 18 certifikátov NATO ATOMAL, ktoré oprávňujú na prístup k informáciám o strategickom jadrovom odstrašovaní NATO a vydávajú sa úzkemu okruhu osôb.

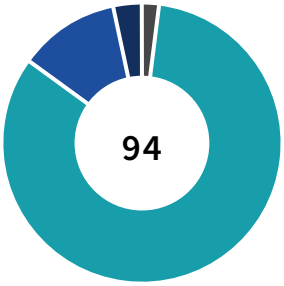
PRIEMYSELNÁ BEZPEČNOSŤ

V oblasti priemyselnej bezpečnosti úrad vykonáva **bezpečnostné previerky podnikateľov.** Bezpečnostná previerka podnikateľa sa zameriava na získavanie informácií o podnikateľoch, u ktorých vzniká odôvodnený predpoklad, že ich štátny orgán požiada o vytvorenie utajovanej skutočnosti, alebo im bude utajovaná skutočnosť postúpená.

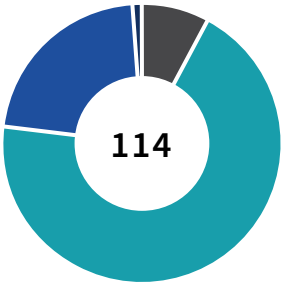
Povinnosťou štatutárneho orgánu podnikateľa je v takomto prípade požiadať úrad o vykonanie bezpečnostnej previerky pre získanie **potvrdenia o priemyselnej bezpečnosti.**

V roku 2022 úrad vydal **114 potvrdení o priemyselnej bezpečnosti,** z toho 9 potvrdení stupňa utajenia Vyhradené, 79 potvrdení stupňa utajenia Dôverné, 25 potvrdení stupňa utajenia Tajné a 1 potvrdenie stupňa utajenia Prísne tajné. Prehľad uvádzaných údajov sa nachádza v tabuľke č. 3.

2021



2022



Prehľad potvrdení o priemyselnej bezpečnosti vydaných v rokoch 2021 a 2022

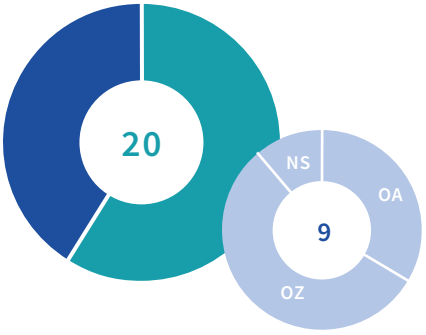
Stupeň utajenia	2021	2022
VYHRADENÉ	2	9
DÔVERNÉ	78	79
TAJNÉ	11	25
PRÍSNE TAJNÉ	3	1
Spolu	94	114

V roku 2022 úrad vydal 13 rozhodnutí. Proti rozhodnutiu úradu podali podnikatelia **4** odvolania.

Úrad rozhodol o dvoch odvolaniach autoremedúrou. Výbor rozhodol o dvoch odvolaniach, ktoré zamietol. K 31. decembru 2022 nebolo v odvolacom procese žiadne odvolanie.

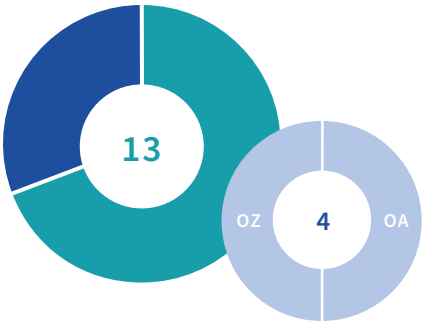
2021

9



2022

4



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

	2021	2022
ROZHODNUTIA ÚRADU	20	13
ODVOLANIA	9	4
Odvolania – autoremedúra (OA)	3	2
Odvolania zamietnuté výborom (OZ)	5	2
Rozhodnutia zrušené výborom (RZ)	0	0
Podané žaloby na najvyššom súde (NS)	1	0

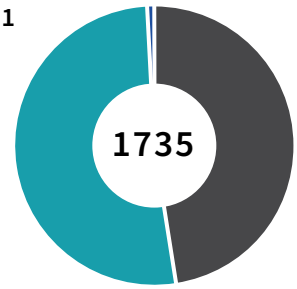
Vo vzťahu k utajovaným skutočnostiam NATO a EÚ bolo v roku 2022 podnikateľom vydaných **6 certifikátov NATO a 3 certifikáty EÚ**, ktoré oprávňujú podnikateľov oboznamovať sa v utajovanými skutočnosťami NATO, resp. EÚ.

ADMINISTRATÍVNA BEZPEČNOSŤ

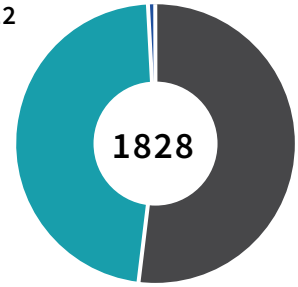
V roku 2022 úrad prijal a odoslal **1 828 utajovaných skutočností**.

Údaje o vymieňaných utajovaných skutočnostiach v internom prostredí – interná komunikácia medzi útvarmi – v celkovom počte 1 828 nie je uvedená. Od roku 2022 elektronický informačný systém pre správu registratúry umožňuje vytvárať utajované skutočnosti stupňa utajenia Vyhradené aj obsahovo.

2021



2022



Stupne utajenia vydaných certifikátov

Stupeň utajenia	2021	2022
VYHRADENÉ	826	950
DÔVERNÉ	898	867
TAJNÉ	11	11
PRÍSNE TAJNÉ	0	0
Spolu	1735	1828

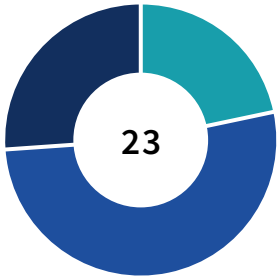
FYZICKÁ BEZPEČNOSŤ A OBJEKTOVÁ BEZPEČNOSŤ

Za rok 2022 úrad vydal **37 certifikátov** mechanických zábranných a technických zabezpečovacích prostriedkov.

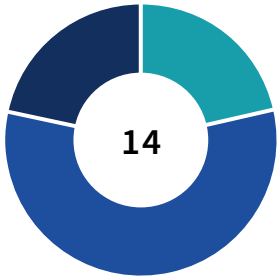
Stupne utajenia vydaných certifikátov

Stupeň utajenia	MZP	TZP	MZP a TZP
VYHRADENÉ	0	0	0
DÔVERNÉ	5	3	8
TAJNÉ	12	8	20
PRÍSNE TAJNÉ	6	3	9
Spolu	23	14	37

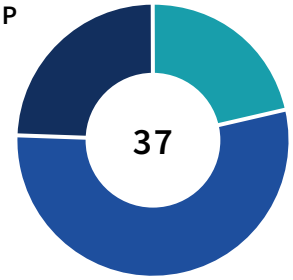
MZP



TZP



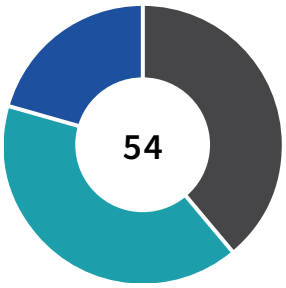
MZP a TZP



BEZPEČNOSŤ TECHNICKÝCH PROSTRIEDKOV

Za rok 2022 úrad vydal **54 certifikátov** technických prostriedkov a **20 dodatkov** k už vydaným certifikátom technických prostriedkov.

2021



Stupne utajenia vydaných certifikátov

Stupeň utajenia	TP
VYHRADENÉ	21
DÔVERNÉ	22
TAJNÉ	11
PRÍSNE TAJNÉ	0
Spolu	54

AKREDITÁCIA KOMUNIKAČNÝCH A INFORMAČNÝCH SYSTÉMOV

V roku 2022 úrad vykonal **3 akreditácie** komunikačných a informačných systémov v súlade s Bezpečnostnou politikou NATO C-(2002)49-REV1 a **2 akreditácie** komunikačných a informačných systémov v súlade s Rozhodnutím rady (2013/488/EÚ).

OCHRANA PRED NEŽIADUCIM ELEKTROMAGNETICKÝM VYŽAROVANÍM

Na zabezpečenie ochrany utajovaných skutočností pred únikom cez nežiaduce elektromagnetické vyžarovanie technická sekcia vykonávala v roku 2022 zónové merania chránených priestorov (mobilnou meracou aparatúrou) a merania technických prostriedkov a prostriedkov šifrovej ochrany informácií v špecializovanom TEMPEST laboratóriu.

V roku 2022 bolo na **základe 35 doručených žiadostí vykonaných 268 meraní** zariadení (TP a PŠOI) a 52 zónových meraní priestorov na základe, ktorých bolo kategorizovaných **46 komponentov zariadení technických prostriedkov a 51 miestností.**

V danom období boli prijaté taktiež:

- 2 žiadosti o vykonanie merania útlmu tienených komôr, na základe ktorých bolo vykonaných 5 meraní a posúdené 2 tienené komory,
- 2 žiadosti o vykonanie merania útlmu tienených kontajnerov, na základe ktorých boli vykonané 4 merania a posúdené 3 kontajnery,
- 1 žiadosť o vykonanie technických bezpečnostných prehliadok priestorov, na základe ktorej bola vykonaná prehliadka 12 miestností a 16 služobných motorových vozidiel.

BUDOVANIE BEZPEČNOSTNÉHO POVEDOMIA

Na na úseku ochrany utajovaných skutočností vykonáva úrad skúšky bezpečnostného zamestnanca a preškolenia osôb. Skúšky a preškolenia sa vykonávajú v rôznych oblastiach bezpečnosti najmä formou online testu v prostredí samostatnej webovej aplikácie, komunikácia počas skúšky a preškolenia prebieha vo virtuálnej videokonferenčnej miestnosti.

Na skúšky bolo v roku 2022 **pozvaných 431 uchádzačov**. Z uvedeného počtu pozvaných skúšku úspešne vykonalo 284 uchádzačov (z nich 31 prezenčnou formou a 34 v rámci Ministerstva vnútra SR) a 78 uchádzačov bolo neúspešných (z nich 4 v rámci Ministerstva vnútra SR). Zvyšný počet uchádzačov sa na skúške nezúčastnil.

Na preškolenia bolo v hodnotenom období pozvaných 131 uchádzačov. Z uvedeného počtu pozvaných preškolenie úspešne absolvovalo 113 uchádzačov (z nich 12 prezenčnou formou a 14 v rámci Ministerstva vnútra SR) a 2 uchádzači boli neúspešní. Zostávajúci počet uchádzačov sa na preškolení nezúčastnil.

Okrem uvedených činností, úrad v roku 2022 vydal aj 4 potvrdenia o absolvovaní skúšky (duplikáty).

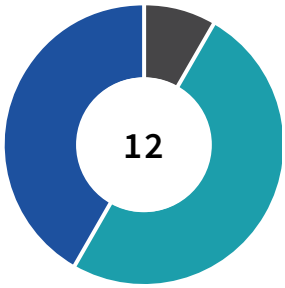
ŠIFROVÁ OCHRANA INFORMÁCIÍ

PERSONÁLNA BEZPEČNOSŤ

Systém šifrovej ochrany je založený na overenej štruktúre rezortných šifrových orgánov a ich úzkej spolupráci s úradom, ktorý plní rolu ústredného šifrového orgánu. Predmetom komunikácie v roku 2022 boli najmä oblasti certifikácie prostriedkov šifrovej ochrany informácií, vydávanie dodatkov k pravidlám na používanie prostriedkov šifrovej ochrany informácií a otázky ohľadom možností uznávania a preberania zahraničných certifikátov.

Za rok 2022 úrad vydal **12 certifikátov** prostriedkov šifrovej ochrany informácií a **7 dodatkov** k už vydanému certifikátu.

2022



Stupne utajenia vydaných certifikátov

Stupeň utajenia	TP
VYHRADENÉ	1
DÔVERNÉ	6
TAJNÉ	5
PRÍSNE TAJNÉ	0
Spolu	12

ZABEZPEČENÁ INFRAŠTRUKTÚRA

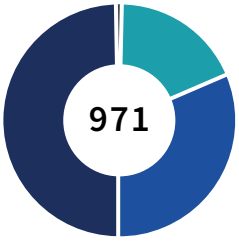
Úrad pokračoval v distribúcii prostriedkov určených na bezpečnú výmenu informácií medzi vládnymi inštitúciami v režime stupňa utajenia Vyhradené, Dôverné a Tajné. Zabezpečoval ochranu videokonferencií a prenosu informácií pre členov vlády Slovenskej republiky.

Napredovanie digitálnej transformácie v podmienkach orgánov verejnej moci a samospráv spolu s aktuálnou bezpečnostnou situáciou spôsobujú neustály nárast požiadaviek na služby a podporu poskytovanú úradom v operačnom prostredí systémov zabezpečenia obrany a bezpečnosti Slovenskej republiky.

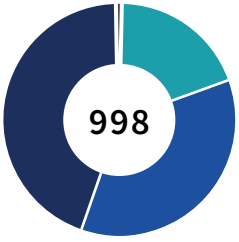
V priebehu roku 2022 sa podarilo zvýšiť bezpečnosť a prevádzkovú spoľahlivosti týchto systémov použitím nových technológií prostriedkov šifrovej ochrany informácií. Pre udržateľnosť plnenia stanovených cieľov sme realizovali výcvik personálu zameraný na získanie a rozvoj odborných spôsobilostí pre správu informačných systémov, spôsobilostí zabezpečujúcich ochranu informačných systémov, webových služieb, technických prostriedkov a prostriedkov šifrovej ochrany informácií v správe NBÚ.

V roku 2022 úrad v podmienkach zabezpečenej infraštruktúry Slovenskej republiky priamo prevádzkoval 6 systémov so šifrovou ochranou informácií, prevádzkoval alebo poskytoval podporu pre 433 koncových zariadení a poskytoval služby a podporu pre 805 používateľov, pričom v hodnotenom období celkovo evidujeme 998 vybavených požiadaviek od týchto používateľov. NBÚ priebežne zabezpečoval operatívne požiadavky rezortov a poskytoval podporu pri výrobe a distribúcii šifrového materiálu.

2021



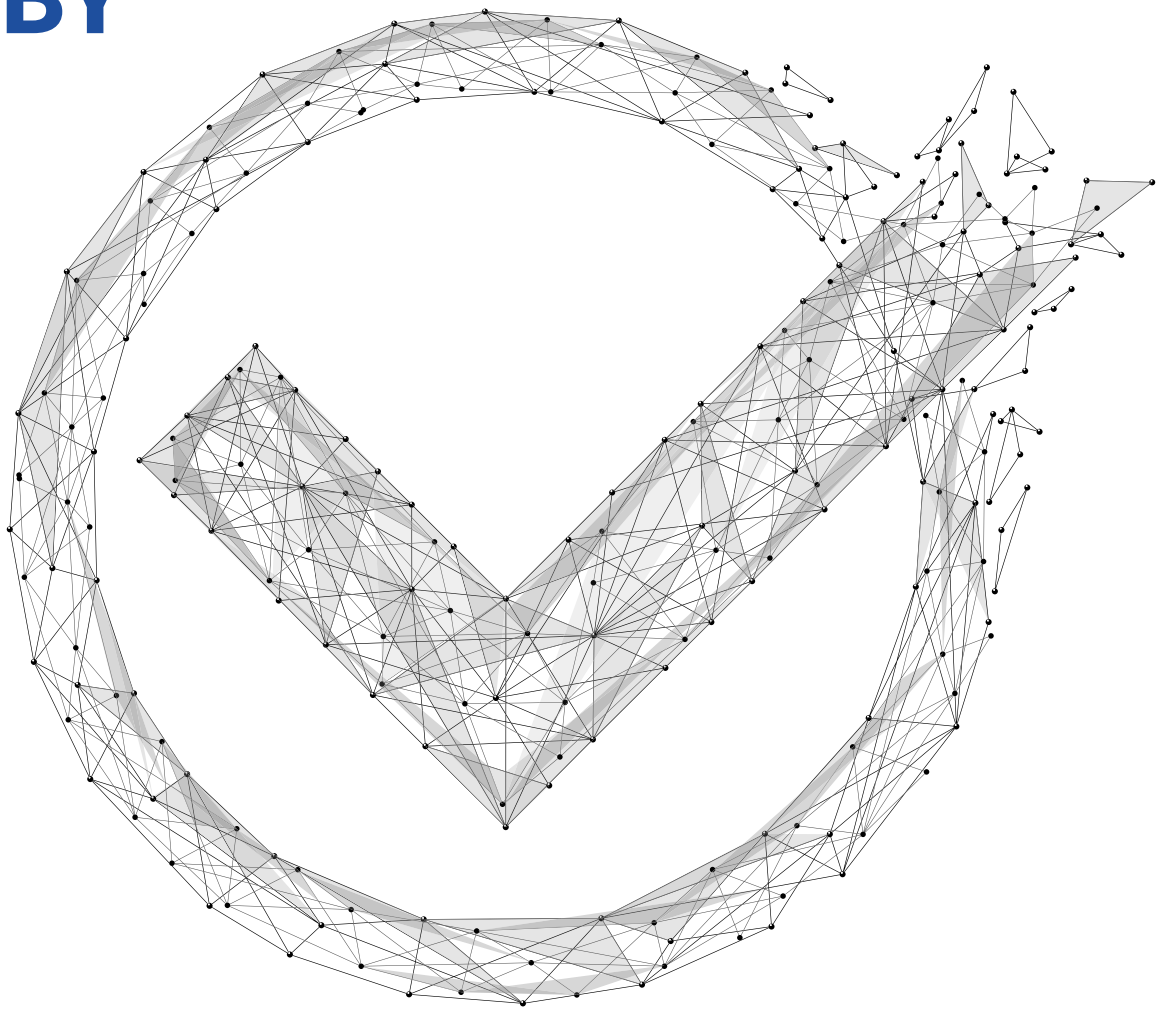
2022



Stupne utajenia vydaných certifikátov

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

DÔVERYHODNÉ SLUŽBY



V priebehu roka 2022 Rada 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 bezpečnostnej a dôveryhodnej elektronickej identifikácii a autentifikácii prostredníctvom európskej peňaženky 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 zadefinujú postupy aj podľa článku 45d, kedy členské štáty zabezpečia, aby sa prijali opatrenia, ktoré kvalifikovaným poskytovateľom elektronických osvedčení atribútov umožnia na žiadosť používateľa elektronickými prostriedkami overiť pravosť týchto atribútov na základe príslušného autentického zdroja na vnútroštátnej úrovni alebo prostredníctvom 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.

CERTIFIKÁCIA

V roku 2022 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.

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 úrad publikoval dôveryhodné zoznamy č. 85 až 99.

ZOZNAM OPRÁVNENÍ

Zoznam oprávnení, ktorý je informačným zdrojom pre kvalifikovaných poskytovateľov dôveryhodných služieb pre vydávanie mandátnych certifikátov, zverejňuje úrad na svojom webovom sídle. Na základe žiadostí štátnych orgánov a orgánov územnej samosprávy bolo do zoznamu zapísaných 18 nových oprávnení. V priebehu roka úrad publikoval 9 verzií zoznamu oprávnení. Jeho aktuálna verzia bola vždy doplnená archívom predchádzajúcich verzií.

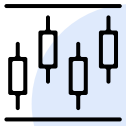
NOVÉ DÔVERYHODNÉ SLUŽBY

Úrad prijal oznámenie piatich kvalifikovaných poskytovateľov o zámere poskytovať kvalifikovanú dôveryhodnú službu. Celkovo bolo udelených štrnásť kvalifikovaných štatútov na kvalifikovanú dôveryhodnú službu.

V roku 2022 boli kvalifikovanými poskytovateľmi dôveryhodných služieb predložené orgánu dohľadu dve správy o posúdení zhody vykonaných orgánom posudzovania zhody do 24 mesiacov od vykonania posledného auditu. Potvrdzujú, že kvalifikovaní poskytovatelia dôveryhodných služieb a kvalifikované dôveryhodné služby, ktoré poskytujú, spĺňajú požiadavky stanovené v nariadení eIDAS. NBÚ nezaznamenal narušenia bezpečnosti alebo integrity poskytovania dôveryhodných služieb.

DÔVERYHODNÁ INFRAŠTRUKTÚRA

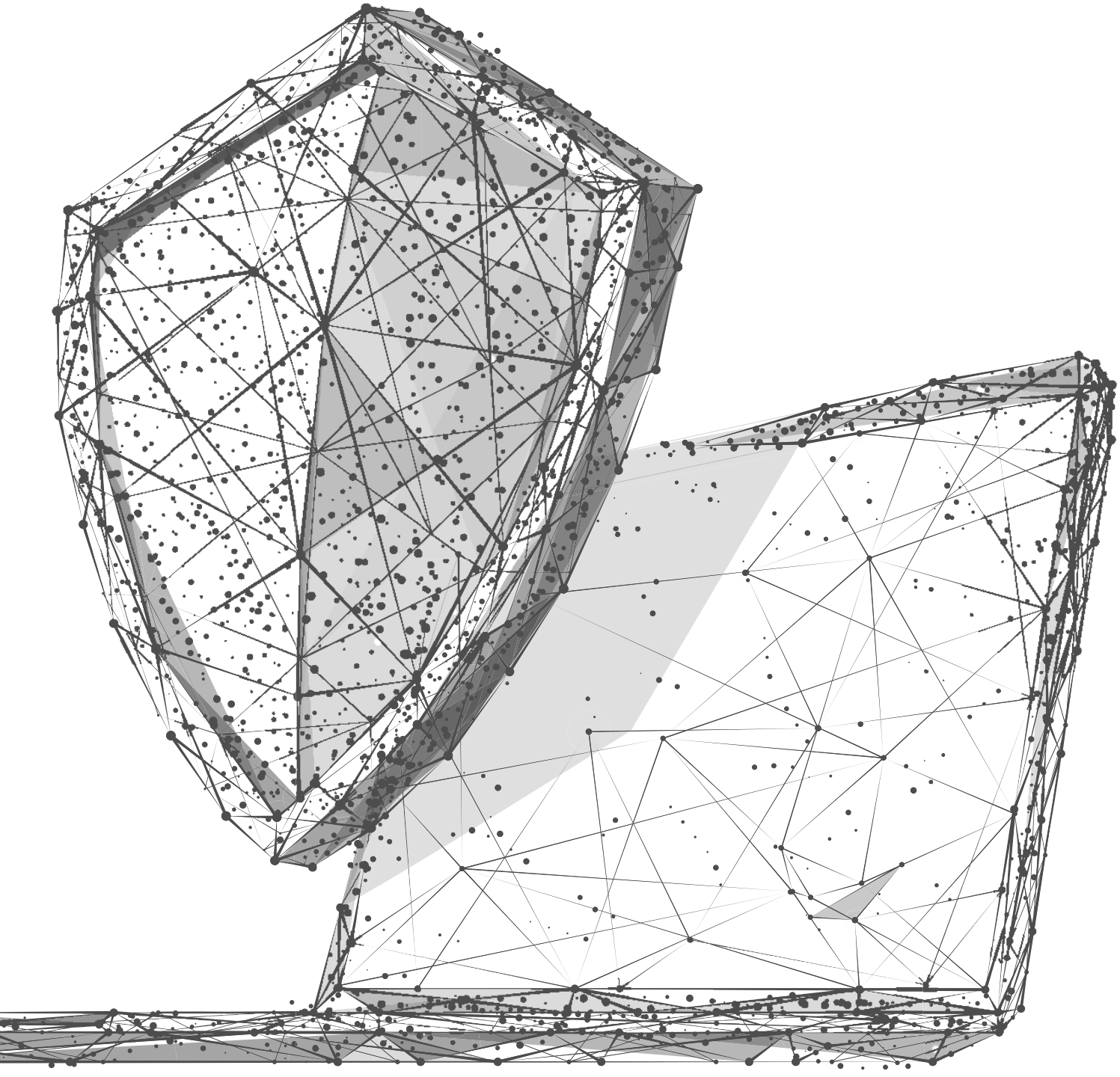
Úrad prevádzkuje v dôveryhodnej infraštruktúre koreňovú certifikačnú autoritu Slovenskej republiky, ktorá vydáva certifikáty verejných kľúčov a vedie dlhodobú databázu vydaných kvalifikovaných certifikátov s ich stavom platnosti, vydaných poskytovateľmi, ktorým úrad udelil kvalifikovaný štatút. Za rok 2022 evidujeme celkovo 122 357 certifikátov.



TVORBA MEDZINÁRODNÝCH NORIEM

Pri tvorbe medzinárodných technických noriem použiteľných pre implementáciu nariadenia eIDAS bol príslušník úradu projektovým vedúcim pre ISO 14533-1 v ISO TC 154. Práce na revízii ISO 14533-1 sa zavŕšili jej vydaním v polovici roka 2022.

KYBERNETICKÁ BEZPEČNOSŤ



Národný bezpečnostný úrad prostredníctvom Národného centra kybernetickej bezpečnosti SK-CERT prijíma hlásenia o kybernetických bezpečnostných incidentoch, analyzuje ich, vyhodnocuje, vykonáva dohľad a koordinuje ich riešenie.

Svoje aktivity vykonáva tak, aby pri vzniku kybernetických bezpečnostných incidentov došlo k náprave a minimalizácii škôd. Zároveň distribuuje varovania a zvyšuje tým úroveň prevencie.

Činnosť SK-CERT sa na operatívnej úrovni v roku 2022 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 KBI Národnému bezpečnostnému úradu za rok 2022 podľa sektorov

	Jan	Feb	Mar	Apr	Máj	Jún	Jul	Aug	Sep	Okt	Nov	Dec
Bankovníctvo	10	24	19	9	16	13	13	6	10	5	2	4
Doprava	0	1	1	0	1	0	3	0	0	0	2	0
Digitálna infraštruktúra	0	2	1	0	0	1	1	0	0	0	1	1
Elektronické komunikácie	1	0	3	2	1	1	0	1	0	2	0	3
Energetika	1	1	0	1	0	2	1	0	0	0	0	0
Infraštruktúra finančných trhov	0	0	0	0	0	0	0	0	0	0	0	0
Pošta	1	6	8	7	5	1	1	0	0	0	2	1
Priemysel	0	0	2	0	0	3	0	0	1	1	1	0
Voda a atmosféra	0	0	0	0	0	0	0	0	0	0	0	0
Verejná správa	27	35	23	25	21	26	19	19	39	30	23	41
Zdravotníctvo	9	3	1	5	4	10	4	2	7	3	3	1
Iné	51	37	42	125	47	46	28	27	51	45	43	42
CELKOM	**100**	**109**	**100**	**174**	**95**	**103**	**70**	**55**	**108**	**86**	**77**	**93**

NBÚ evidoval v roku 2022 celkovo **1170 hlásení o kybernetických bezpečnostných incidentoch**, z toho **20 hlásení** o závažných kybernetických bezpečnostných **incidentoch I. stupňa, 8 hlásení** o závažnom kybernetickom bezpečnostnom **incidente II. stupňa, 7 hlásení** o závažných kybernetických bezpečnostných **incidentoch III. stupňa.**

SK-CERT evidoval aj 1135 dobrovoľných hlásení.

Znamená to medziročný nárast hlásení o 28%, nárast však bol zaznamenaný hlavne v oblasti dobrovoľných hlásení.

Slovenský kybernetický priestor v roku 2022 významne ovplyvnila vojna Ruska proti Ukrajine. Na začiatku konfliktu aj počas roka bola pozorovaná zvýšená aktivita rôznych hackerských skupín, podporujúcich a vykonávajúcich škodlivé aktivity v mene Ruskej federácie.

Skupiny sa koordinovali cez sociálne médiá najmä na komunikačnej platforme Telegram, čo prispelo aj k zapojeniu sympatizujúcej verejnosti do útokov.

Najviditeľnejšie boli DDoS útoky zamerané na zneprístupnenie rôznych webových stránok a služieb rôznych verejných inštitúcií, ale aj súkromných spoločností. Tieto útoky boli koordinované a smerovali aj na iné členské štáty EÚ a NATO – ich verejné inštitúcie alebo iné dôležité ciele.

Útoky boli často odpoveďou na vyhlásenia verejných predstaviteľov alebo na schválenie konkrétnych sankcií uvalených na Rusko. Výber cieľov bol najprv nekonzistentný a neefektívny, avšak postupom času bolo spozorované zlepšovanie sa útočníkov v ich taktike, technikách a procedúrach, čo zahŕňalo používanie lepších nástrojov, dôkladnejší výber cieľov, odmeny, vrátane finančných, pre najlepších útočníkov a podobne.

Okrem kybernetických útokov súvisiacich s vojnou boli pozorované rozsiahle phishingové kampane, ktoré zneužívali identitu poštových a doručovateľských služieb. NBÚ pozoruje tento trend už od roku 2020. Útočníci takisto zneužívajú identity bánk a ich útoky sú čím ďalej tým sofistikovanejšie – nevyužívajú len bežné komunikačné nástroje ako napríklad e-mail.

Pri svojich útokoch často využívajú šírenie phishingového obsahu cez SMS, sociálne siete, telefónne hovory či iné komunikačné služby (napr. aplikáciu WhatsApp, Facebook Messenger a podobne).

V roku 2022 boli takisto rozšírené phishingové kampane, zneužívajúce identitu orgánov presadzovania práva (polícia, Interpol, Europol), v ktorých útočníci vyzývali obete na uhradenie financií, aby sa vyhli fiktívnemu trestnému stíhaniu.

Šírenému škodlivému kódu už niekoľko rokov dominuje ransomvér, ktorého účelom už nie je len zašifrovanie dát a následné pýtanie výkupného, ale aj exfiltrácia (krádež dát s cieľom ich následného speňaženia) a následné vydieranie (ak nezaplatíš, zverejním).

Ransomvérové útoky majú často devastačné účinky na dáta a infraštruktúru zasiahnutých organizácií, a to najmä u tých, ktoré podceňujú aplikáciu bezpečnostných opatrení (napríklad správneho zálohovania). V slovenskom kybernetickom priestore sa vyskytovalo hneď niekoľko rôznych typov ransomvéru s rôznou mierou sofistikovanosti či spôsobom šifrovania a exfiltrácie dát. Pri škodlivom kóde však boli pozorované aj iné formy, zamerané na získavanie údajov a informácií, vytváranie botnetových sietí a iné škodlivé aktivity útočníkov.

V roku 2022 pokračoval trend výskytu zraniteľností a zlých nastavení v rôznych systémoch a službách. Tento problém je prítomný v celom slovenskom kybernetickom priestore, bez ohľadu na sektor. Často boli pozorované neaktualizované systémy a služby, ktoré obsahovali aj niekoľko mesiacov či rokov staré zraniteľnosti. Takéto situácie sú zapríčinené nesprávnou alebo žiadnou implementáciou bezpečnostných opatrení, ktoré sú pre prevádzkovateľov základných služieb vrátane prvkov kritickej infraštruktúry povinné.

Národné centrum kybernetickej bezpečnosti SK-CERT vydávalo počas roka 2022 bezpečnostné odporúčania a varovania pred zraniteľnosťami a hrozbami. NCKB SK-CERT celkovo **vydalo 52 súhrnných bezpečnostných bulletinov a 271 bezpečnostných varovaní.**

Spolu upozornilo na **628 zraniteľností a hrozieb.**

CYBERGAME

V roku 2022 zorganizoval NBÚ súťaž v oblasti kybernetickej bezpečnosti pod 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 bola určená pre kohokoľvek – nadšencov, špecialistov, študentov, učiteľov, zamestnancov verejnej správy; bez rozdielu veku, pohlavia, zamestnania alebo vzdelania.

Trvala od 1. marca do 10. mája 2022 a na zapojenie sa stačil obyčajný notebook a voľne dostupné nástroje z internetu. CyberGame kombinovala technické a netechnické úlohy. Celkovo bolo pripravených viac ako 50 úloh. Hra bola rozdelená na 4 vetvy – malvérová analýza, forenzná analýza, obfuskácia a kryptografia a OSINT.

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. Ak hráč použil pomoc, body sa mu zredukovali. Za dokončenie celého scenára bolo bonusové ohodnotenie. Do hry zapojilo **1242 hráčov**.

Celkový víťaz, najlepšia hráčka v ženskej kategórii a najlepší študent vyhrali fakultatívny zájazd do malvérového laboratória v Montreale. Ostatní súťažiaci zo zvyšných kategórií vyhrali vecné ceny. CyberGame v roku 2022 získala ocenenie IT projekt roka, tzv. slovenského IT Oscara.

MEDZINÁRODNÉ VZŤAHY

NBÚ sa aktívne podieľal na národných a nadnárodných aktivitách účasťou na konferenciách, workshopoch, pracovných skupinách a ďalších podujatiach, aby si vymenil skúsenosti a poznatky z praxe.

Pracovné skupiny a rôzne iné medzinárodné formáty na úrovni EÚ, NATO a OBSE boli možnosťou na presadzovanie záujmov SR v oblasti kybernetickej bezpečnosti a participáciou na tvorbe strategických, legislatívnych a metodických dokumentov.

NBÚ je hlavným kontaktným bodom na medzinárodnej úrovni, čo v praxi znamenalo širokú spoluprácu so zahraničnými partnermi a partnerskými organizáciami, a to najmä v pracovných skupinách NIS Cooperation Group, CSIRT Networku, CyCLONe a organizácií Trusted Introducer a FIRST výmenou skúseností, operatívnych informácií pri riešení kybernetických bezpečnostných incidentov a najlepšej praxe.

Najdôležitejšími aktivitami bola výmena informácií a koordinácia v rámci závažných incidentov s medzinárodným presahom. Zástupca NBÚ aktívne pôsobil v ENISA Management Board a ENISA Executive Board. NBÚ zastupuje Slovenskú republiku v oblasti kybernetickej bezpečnosti aj v OBSE.

Na národnej úrovni pokračovalo zdieľanie informácií s relevantnými subjektami, a to najmä medzi NBÚ, SIS, VS, NASES, polícia a MIRRI. Okrem výmeny relevantných informácií, dôležitých na zabezpečenie národného kybernetického priestoru, sme s partnermi komunikovali strategické a koncepčné otázky.

Spoločne sme sa zúčastňovali na medzinárodných cvičeniach, zameraných na kybernetickú bezpečnosť a kybernetickú obranu. Na národnej úrovni NBÚ zastrešoval komunikačnú platformu pre prevádzkovateľov základných služieb. Bola určená na zdieľanie skúseností a výmenu odporúčaní a pripomienkovanie zásadných legislatívnych dokumentov súvisiacich s kybernetickou bezpečnosťou.

NBÚ poskytoval metodickú pomoc, konzultácie a usmernenia pri implementácii zákonných požiadaviek najmä prevádzkovateľom základných služieb a poskytovateľom digitálnych služieb, ale aj ústredným orgánom podľa zákona.

V oblasti kybernetickej bezpečnosti technická sekcia akredituje jednotky CSIRT. V roku 2022 NBÚ nedostal žiadosť o takúto akreditáciu. Technická sekcia spolupracuje s analytickými bezpečnostnými pracoviskami pre účely výmeny a zdieľania informácií o bezpečnostných incidentoch.

KOMPETENČNÉ A CERTIFIKAČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti (KCCKB) je príspevková organizácia a jej základným poslaním je napomáhať vo verejnom záujme k plneniu odborných úloh Národného bezpečnostného úradu ako zriaďovateľa v oblasti kybernetickej bezpečnosti, ochrany utajovaných skutočností, šifrovej ochrany a dôveryhodných služieb.

Vo vymedzenom predmete činností sú to najmä úlohy národného odvetvového, technologického a výskumného centra v oblasti kybernetickej bezpečnosti, posudzovanie zhody pre rôzne typy objektov v oblasti kybernetickej bezpečnosti, realizácia a komplexná implementácia projektov z európskych štrukturálnych a investičných fondov, Kohézneho fondu a iných finančných nástrojov Európskej únie.

KCCKB, ako akreditovaný orgán posudzovania zhody, certifikuje audítorov a manažérov kybernetickej bezpečnosti a integrované systémy manažérstva. V kontexte kybernetickej bezpečnosti je akceptovaná kombinácia systémov manažérstva informačnej bezpečnosti podľa ISO/IEC 27001:2013, spolu so systémami manažérstva IT služieb podľa ISO/IEC 200001:2018, riadenia kontinuity činností podľa ISO 22301:2019 a riadenia kvality podľa ISO 9001:2015.

Pre všetky uvedené systémy manažérstva aj pre posudzovanie odbornej spôsobilosti audítorov a manažérov kybernetickej bezpečnosti má KCCKB udelené akreditačné rozhodnutia od Slovenskej národnej akreditačnej služby. Ako jediný orgán posudzovania zhody na Slovensku pokrýva všetky objekty posudzovania a platné certifikačné schémy relevantné pre kybernetickú bezpečnosť.

Formou posudzovania zhody sú aj aktivity pod značkou Cybersecurity Made in Europe. Oprávnenie udeliť túto obchodnú značku majú iba kvalifikované subjekty autorizované Európskou organizáciou pre kybernetickú bezpečnosť (European Cyber Security Organisation – ECSO). Jedným z oprávnených partnerov, ktorý udeľuje značku v Európe, je aj KCCKB.

Značka buduje povedomie o strategickej hodnote firiem a organizácií v kybernetickej bezpečnosti, ktoré rozvíjajú podnikanie na základe dôveryhodných európskych hodnôt. Ako priemyselný marketingový nástroj zároveň zvyšuje reputáciu u obchodných partnerov, investorov a koncových používateľov.

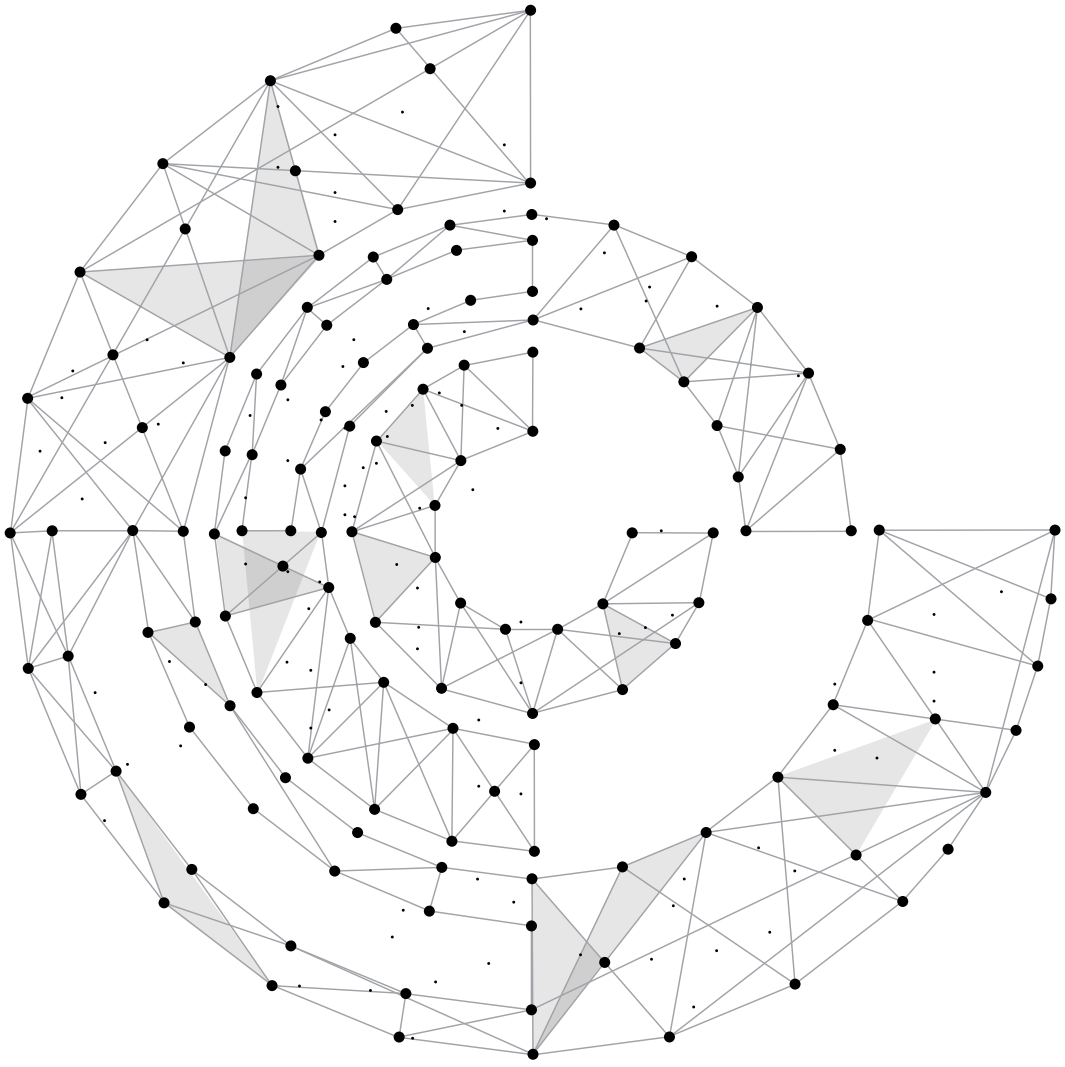
Kompetenčné centrum tiež realizuje audity kybernetickej bezpečnosti u prevádzkovateľov základných služieb s cieľom potvrdiť účinnosť prijatých bezpečnostných opatrení a overiť plnenie požiadaviek stanovených zákonom.

Ako národné odvetvové, technologické centrum však KCCKB pôsobí najmä ako expertná organizácia v dvoch rovinách – konzultačnej a znaleckej. Znalectvo je špecializovaná odborná činnosť vykonávaná znalcami pre zadávateľa, za podmienok ustanovených v zákone. Úkonmi znaleckej činnosti sú najmä znalecký posudok a jeho doplnok, odborné stanovisko alebo potvrdenie, odborné vyjadrenie a vysvetlenie. Znalecká činnosť je vykonávaná podľa Zákona č. 382/2004 o znalcoch, tlmočníkoch a prekladateľoch.

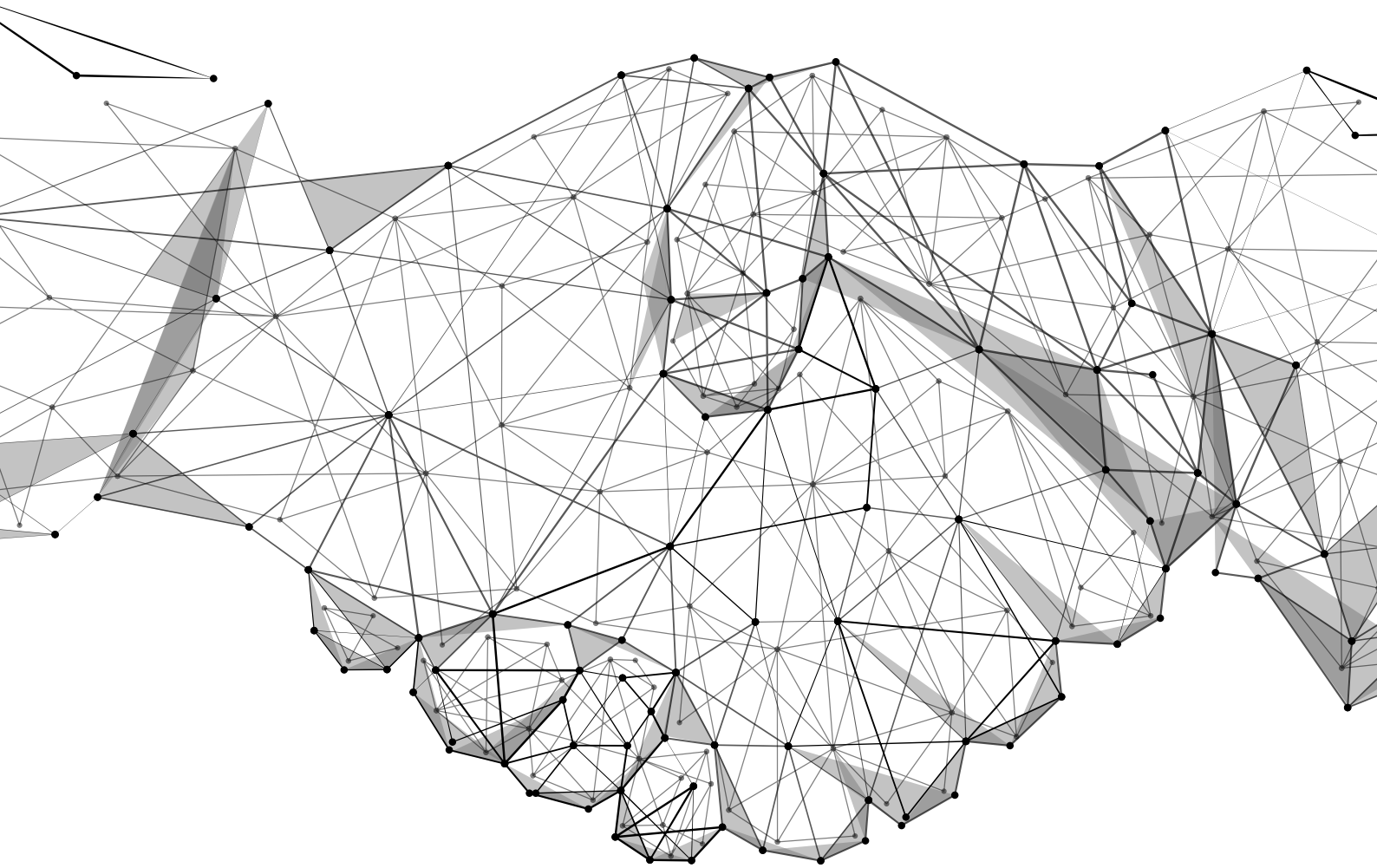
Hlavnou a nezastupiteľnou úlohou Kompetenčného centra bude implementácia relevantných častí programov Digitálna Európa a Európsky Horizont udeľovaním grantov a podporou verejných obstarávaní. O finančných zdrojoch pre kybernetickú bezpečnosť bude rozhodovať Európske kompetenčné centrum v úzkej spolupráci so sieťou národných koordinačných centier a s komunitnými partnermi, ktorými sú výskumné subjekty, dodávateľské a odberateľské odvetvia a verejný sektor.

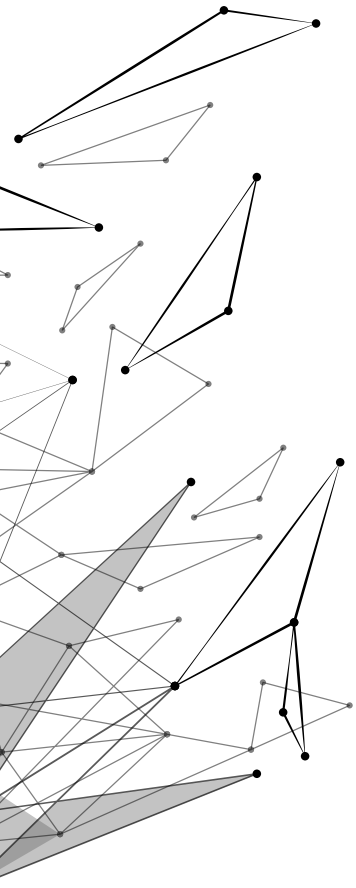
Kompetenčné centrum má podpísané memorandá o spolupráci s absolútnou väčšinou relevantných vysokoškolských pracovísk, ktoré poskytujú študijné programy a odbory v oblasti ochrany informačných.

V neposlednom rade je úlohou KCCKB aj vzdelávanie dospelých v informačnej a kybernetickej bezpečnosti vrátane kampaní na zvyšovanie bezpečnostného povedomia.



MEDZINÁRODNÁ SPOLUPRÁCA





Pandémia ochorenia covid 19 v rokoch 2020 až 2021 a ruská inváziа na Ukrajinu výrazne urýchlili rozvoj digitálnej éry. Digitálne technológie sa stali nevyhnutnou súčasťou bežného i profesionálneho života a osobné kontakty sa značne obmedzili. Situácia výrazne ovplyvnila zavádzanie týchto technológií do praxe a s tým aj riešenie súvisiacich bezpečnostných výziev.

NBÚ vlani 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 Stratégie kybernetickej bezpečnosti EÚ v digitálnej dekáde.

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

Pokiaľ ide o rozvoj medzinárodných vzťahov úradu, príslušníci ich rozvíjali na stálom medzinárodnom zastúpení Slovenskej republiky, kde sa zúčastňovali a podieľali na tvorbe bezpečnostných politík na pôde EÚ a NATO. Takisto rozvíjali medzinárodné aktivity, bilaterálne vzťahy a regionálnu spoluprácu.

EURÓPSKA ÚNIA

Príslušníci úradu sa zúčastňovali, prezenčne alebo virtuálne, na pravidelných zasadnutiach Bezpečnostného výboru Rady EÚ (CSC), Skupiny expertov Európskej komisie pre bezpečnostnú politiku (ComSEG) a Bezpečnostného výboru Európskej služby pre vonkajšiu činnosť (EEAS).

Na pôde Rady EÚ v roku 2022 naďalej prebiehali práce na revízii bezpečnostných pravidiel s cieľom odstrániť nedostatky identifikované v aplikačnej praxi a zvýšiť komfort pre adresátov týchto pravidiel. V uvedených pracovných formátoch sa úrad aktívne zapájal do prípravy bezpečnostných noriem tak, aby bola zvýšená úroveň ochrany utajovaných skutočností a pokračoval aktívnym zapojením v procese revízie bezpečnostných pravidiel.

V súčasnosti pokračuje rozsiahla revízia bezpečnostných pravidiel Rady pre ochranu utajovaných skutočností EÚ (EUCI). Úrad sa preto aktívne zúčastňoval na tvorbe a revízii pravidiel v oblasti personálnej a priemyselnej bezpečnosti. Pokračovala aj diskusia o zmenách pri výmene utajovaných skutočností EÚ s tretími krajinami a medzinárodnými organizáciami, ako aj o Návrhu nariadenia EP a Rady (EÚ), ktorým sa ustanovuje program Únie pre bezpečnú konektivitu na obdobie rokov 2023 – 2027 (EU Secure Connectivity Programme).

Najdiskutovanejšou témou bolo však pripravované nariadenie EK o spoločných jednotných pravidlách ochrany utajovaných skutočností EÚ pre všetky inštitúcie, orgány a agentúry EÚ. Členské štáty sa zhodujú, že právny základ všetkých bezpečnostných pravidiel EÚ je stanovený Radou platnými dokumentmi.

Na pravidelnom zasadaní Bezpečnostného výboru Európskej služby pre vonkajšiu činnosť (SC EEAS) sa EEAS príslušníci participovali na revízii programu bezpečnostného povedomia a zintenzívnenia školenia personálu o možných kybernetických rizikách. V tej-

to súvislosti sa pripravuje príručka, ktorá má pomôcť nielen nováčikom pri práci s EUCI. Zamestnanci EEAS prispeli k budovaniu odolnosti a bezpečnostného povedomia na zahraničných delegáciách EÚ pomocou školení, workshopov a podporných programov.

Úrad mal pravidelné a aktívne zastúpenie na rokovaniach Horizontálnej pracovnej skupiny pre kybernetické záležitosti (HWPCI) počas francúzskeho a českého predsedníctva v Rade EÚ. V legislatívnej oblasti bol rok 2022 dôležitým míľnikom pre posilnenie kybernetickej bezpečnosti EÚ.

Bola prijatá Smernica Európskeho Parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2).

Hlavnou úlohou úradu v tejto súvislosti bude jej transpozícia do národnej legislatívy. Ďalším dôležitým a nadväzujúcim krokom bolo predstavenie návrhu právneho aktu o kybernetickej odolnosti, ktorý stanoví požiadavky kybernetickej bezpečnosti pre produkty s digitálnymi prvkami. Rozhodujúcou úlohou v tomto smere bude jednoznačné nastavenie pravidiel zabezpečenia vysokej úrovne kybernetickej bezpečnosti EÚ s víziou stanovenia štandardov aj pre zvyšok sveta.

Rokovania HWPCI sa zaoberali aj negociovaním nelegislatívnych dokumentov. Za najdôležitejšie z nich možno považovať Strategický kompas, Závery Rady EÚ o kybernetickom postoji únie, Závery Rady o bezpečnosti dodávateľského reťazca IKT a návrh novej politiky kybernetickej obrany predstavenej v tzv. obrannom balíku EK.

Oblasť kybernetickej diplomacie bola vo veľkej miere ovplyvnená udalosťami u východného partnera EÚ. Rokovania HWPCI sa preto sústredili aj na formulovanie textov vyhlásení vysokého predstaviteľa EÚ o odsúdení kybernetických útokov ruských aktérov na Ukrajinu, ktoré predchádzali a naďalej pretrvávali počas invázie Ruska. V tejto súvislosti sa niekoľkokrát otvorila otázka revízie súboru nástrojov kybernetickej diplomacie (CDT).

V Agentúre Európskej únie pre vesmírny program (EUSPA) bolo hlavným bodom diskusie vypracovanie Bezpečnostných pokynov pre jednotlivé programy (PSI). 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 iniciatívy EK. Ide o ad hoc skupinu 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 a v neposlednom rade aj bezpečnosti. Táto sieť má byť prispôsobená aj na prenos utajovaných skutočností.

Medzi kľúčové priority Skupiny pre spoluprácu aj naďalej patrí implementácia Smernice Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Európskej únii (smernica NIS), a s tým súvisiaca aplikácia jednotlivých nástrojov.

V roku 2022 k tejto úlohe pribudli aj ďalšie dôležité témy ako „Hodnotenie rizika a rizikové scenáre“, čo vyplýva aj z úlohy pre Skupinu pre spoluprácu a adresne zo Záverov Rady pre rozvoj pozície EÚ ku kybernetickej bezpečnosti, „Krízové riadenie“, „Organizácia a potenciálne oblasti spolupráce v budúcnosti v Skupine pre spoluprácu“ a „Koordinované zverejňovanie zraniteľnosti“. ENISA realizovala cestovnú mapu potrieb pre cvičenia pre oblasť kybernetickej bezpečnosti a štáty si zdieľali svoje skúsenosti, pokiaľ išlo o najzávažnejšie incidenty a hrozby v oblasti kybernetickej bezpečnosti, ktoré ich počas roka zasiahli (dominoval opäť ransomvér).

Work Stream 3

skupina zameraná na notifikačné povinnosti prevádzkovateľov základných služieb. Skupina sa v rámci svojej činnosti venovala zlepšeniu jednotlivých nástrojov, ktoré slúžia k notifikačným povinnostiam pre členské krajiny.

Work Stream 7

skupina pre riešenie kybernetických bezpečnostných incidentov veľkého rozsahu. Na úrovni tejto skupiny sa pokračovalo v príprave operačných procedúr pri riešení závažných incidentov s medzinárodným presahom a zástupcovia úradu na nich aktívne participovali.

Work Stream 10

skupina pre Digitálnu infraštruktúru. Na platforme sa členské štáty venovali príslušným orgánom a ich povinnosti definovať a dodržiavať spoločný prístup k implementačným požiadavkám pre poskytovateľov digitálnych služieb (PDS). Zámerom smernice NIS bolo definovať maximálny harmonizačný rámec pre PDS, ktorí budú podliehať jurisdikcii jediného kompetentného orgánu (príslušného orgánu v krajine hlavného sídla v EÚ) pre všetky ich činnosti v Únii.

Work Stream 5G

skupina pre zabezpečenie a ochranu 5G sietí. EK uverejnila súbor odporúčaných opatrení na zmiernenie rizík súvisiacich s výstavbou a prevádzkou 5G sietí, tzv. 5G Toolbox. Aplikácia týchto opatrení sa preniesla aj na národnú úroveň najmä v podobe aplikačnej praxe.

Work Stream 12

skupina pre sektor zdravotníctva sa vyrovnávala najmä s aktuálnymi problémami, ktoré so sebou priniesla pandémia v oblasti kybernetickej bezpečnosti. Pracovala aj na návrhu dokumentu o implementácii smernice NIS (sektorové pravidlá a odporúčania, pokiaľ ide o nastavenie kybernetických bezpečnostný opatrení v danom segmente), ktorý nadobúda reálnu podobou. Ďalším zámerom je zvýšenie opatrení v kybernetickej bezpečnosti subjektov, ktoré spadajú do oblasti zdravotníctva.

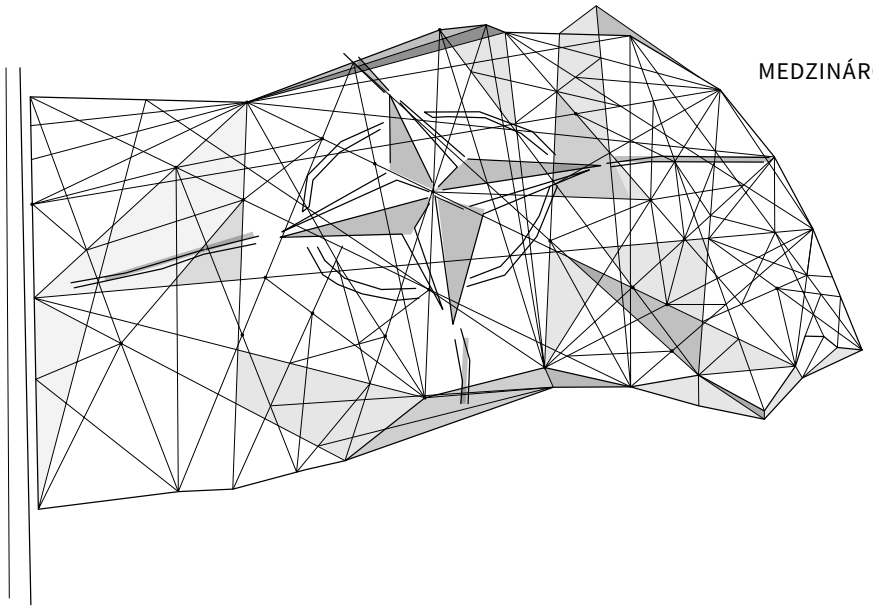
Work Stream 15

Novovzniknutá pracovná platforma Work stream 15 – skupina pre bezpečnosť dodávateľských reťazcov sa počas roka 2022 zameriavala na posilnenie bezpečnosti dodávateľského reťazca IKT a na prvé kroky k riešeniu hrozieb neželaných strategických závislostí v dodávateľských reťazcoch IKT.

EU CyberNet

Počas roka nabrala na vážnosti aj komunita **EU CyberNet** zainteresovaných subjektov, ktorá združuje národné orgány a inštitúcie pôsobiace v oblasti kybernetickej bezpečnosti, expertné skupiny pre danú oblasť, think-thanky 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, pričom príslušníci si zvyšovali svoju odbornosť a poznatky aktívnou účasťou na týchto aktivitách a budovali kapacity úradu.



NATO

Chod NATO bol vo veľkej miere ovplyvnený geopolitickým dianím, a to najmä situáciou na Ukrajine. Kybernetické útoky vykonávané ruskými aktérmi, ktoré predchádzali samotnej nevyprovokovanej invázii a ktoré naďalej pretrvávajú, boli odsúdené generálnym tajomníkom NATO Jensom Stoltenbergom verejnými vyhláseniami.

Výbor kybernetickej obrany (CDC) sa v značnej miere zaoberal poskytnutím pomoci vojnou zasiahnutému partnerovi a urýchlením jeho vstupu do Centra výnimočnosti kybernetickej obrany v Talline.

Vojna na Ukrajine priniesla aj isté ponaučenia z nekoordinovaného postupu pri poskytovaní pomoci a júlový madridský samit v tejto súvislosti vyprodukoval dohodu spojencov na zriadení virtuálnej jednotky rýchlej kybernetickej odozvy, ktorá by dobrovoľne združovala kybernetických expertov spolupracujúcich pri reakciách na závažné škodlivé kybernetické aktivity.

V roku 2022 sa konalo historicky prvé zasadnutie národných kybernetických koordinátorov na pôde Severoatlantickej rady (NAC). Hlavnou témou diskusie boli národné príspevky kybernetickej obrany do celkovej aliančnej zostavy síl pre odstrašenie a obranu v reakcii na dianie na Ukrajine. Za Slovenskú republiku sa na rokovaní zúčastnil riaditeľ Národného centra kybernetickej bezpečnosti SK-CERT.

Pokračovali aj rokovania Bezpečnostného výboru NATO (SC) vo všetkých svojich formátoch – vo formáte bezpečnostných politík, bezpečnosti komunikačných a informačných systémov (CISS) a na najvyššej úrovni – úroveň riaditeľov bezpečnostných úradov členských štátov.

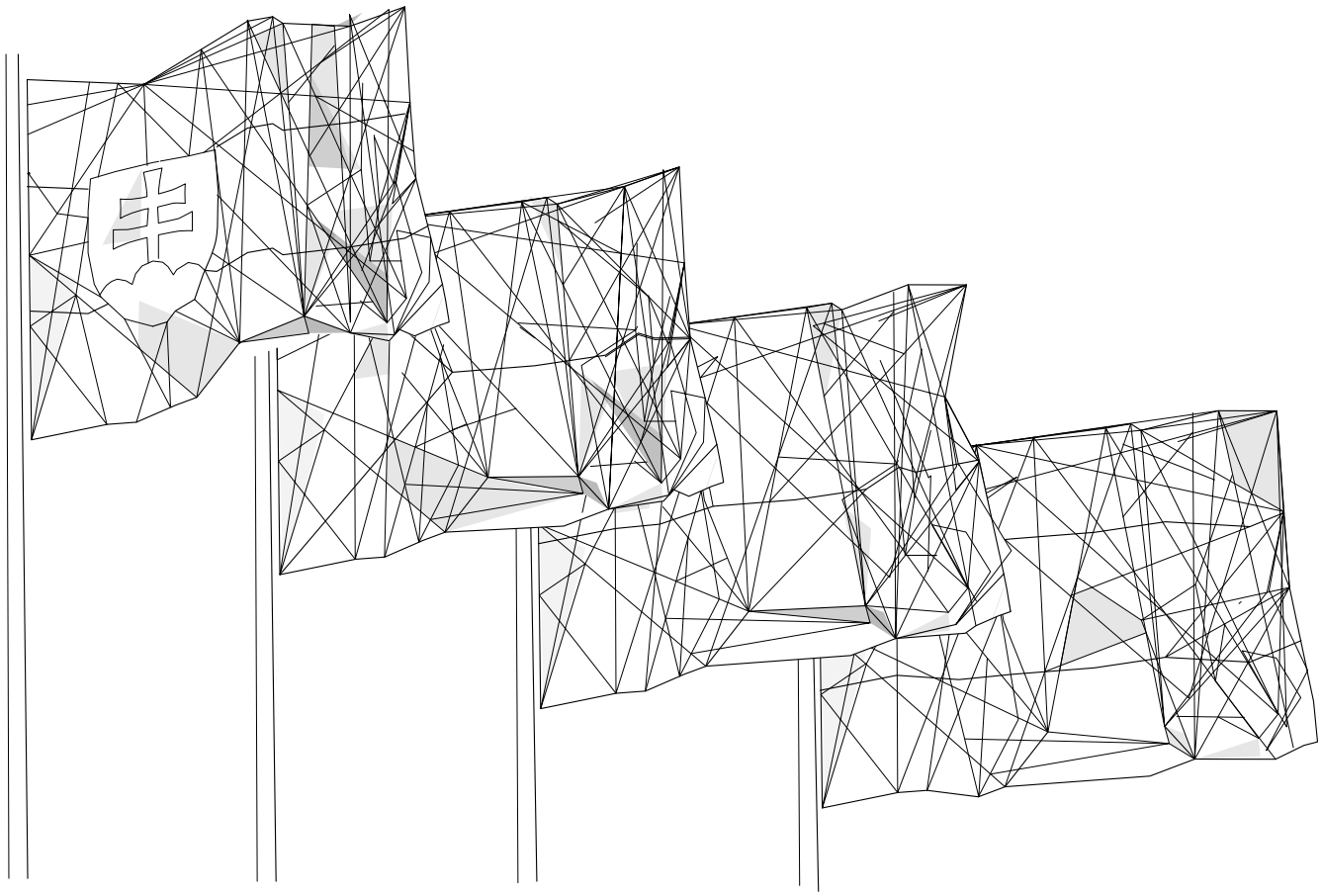
Tento rok bol z pohľadu ochrany utajovaných skutočností v znamení pokračovania v rozsiahlej revízii bezpečnostných pravidiel NATO. Úrad sa zúčastnil aj na zasadaní expertnej skupiny špecialistov z členských štátov na oblasť priemyselnej bezpečnosti (Capability Team) a počas októbrového zasadnutia predostrel Bezpečnostnému úradu NATO (NOS) a delegátom svoje návrhy na zmenu Smernice o utajovaných projektoch a priemyselnej bezpečnosti.

Formát bezpečnosti komunikačných a informačných systémov v NATO SC sa venoval dvom hlavným dokumentom – Smernici o kybernetickej bezpečnosti a NATO Stratégii o umelej inteligencii (AI). Počas októbrového zasadania na najvyššom formáte (Principals level) bol účastníkom predostretý program na rok 2023.

Príslušníci úradu sa v marci zúčastnili na cvičení krízového riadenia NATO CMX (cvičenie na najvyššej strategickej úrovni zamerané na precvičenie a skvalitnenie politických konzultácií a prijímania rozhodnutí). Jeho účelom bolo precvičenie plnenia opatrení Národného systému reakcie na krízové situácie. Úrad sa v národnom riadiacom štábe podieľal na riadení, koordinovaní, kontrole priebehu cvičenia a jeho vyhodnotení.

Úrad participoval aj na spoločnom aliančnom cvičení **NATO Able Staff 2022**, ktoré bolo v decembri 2022 a malo preveriť komunikačné procedúry súvisiace s jadrovým plánovaním, precvičiť použiteľné opatrenia systému krízovej odozvy aliancie, priniesť zdokonalenie v konzultačnej oblasti, realizovať praktický výcvik personálu v centrále NATO, v Hlavnom veliteľstve spojeneckých síl v Európe (SHAPE) a v národných ústrediach.

Úrad sa na cvičení zúčastňoval na distribučnej úrovni, prostredníctvom pracoviska centrálneho registra zabezpečil prijímanie a postupovanie utajovaných skutočností. Komunikácia počas cvičenia prebiehala cez informačný systém NS WAN a NNCCRS (NATO Nuclear Command Control Response System), ktorým prúdil tok informácií medzi zainteresovanými rezortmi, úradom a centrálou NATO.



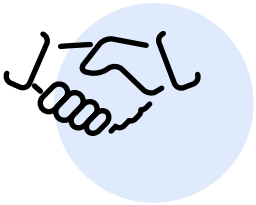
REGIONÁLNA SPOLUPRÁCA

NBÚ zastupoval Slovensko predsedníctvom v Stredoeurópskej platforme pre kybernetickú bezpečnosť (CECSP). Svojich expertov v nej majú krajiny Vyšehradskej štvorky (Česká republika, Maďarsko, Poľsko, Slovenská republika) a Rakúsko.

Úrad zorganizoval partnermi vysoko hodnotené pracovné stretnutie vo fyzickom formáte, ktoré sa bolo 12. septembra 2022 v Bratislave. Venovalo sa aktuálnym témam, ktoré rezonovali na úrovni EÚ. Medzi najdôležitejšie patrili transpozícia NIS 2 a koordinovanie oznamovania zraniteľností.

Slovenská republika sa zviditeľnila prezentáciou venovanou téme umiestnenia kompetenčného centra v systéme regulácie kybernetickej bezpečnosti. Príslušníci NBÚ predstavili aj koncept pre komunitu kybernetickej bezpečnosti.

Komplexnú a ucelenú štúdiu, ktorá sa týkala auditu kybernetickej bezpečnosti na Slovensku prezentoval zástupca KCCKB. Experti si vymenili vzájomné poznatky a uviedli príklady dobrej praxe pri transpozícii smernice NIS 2.



BILATERÁLNE VZŤAHY

Úrad rozvíjal bilaterálne vzťahy naprieč všetkými pracovnými platformami.

Slovensko a Spojené štáty americké podpísali bilaterálnu dohodu o bezpečnostných opatreniach na ochranu utajovaných skutočností. Výrazne prispieva k prehĺbeniu vzťahov a zintenzívneniu spolupráce medzi oboma krajinami.

Počas roka sme odštartovali rokovania o podobnej dohode aj s Holandskom.

Rozširovanie sféry spolupráce sa zameralo aj na Východnú Áziu. Prijali sme dve zahraničné návštevy z Indonézskej republiky. Delegácie sa zaujímali o oblasť ochrany utajovaných skutočností a kybernetickej bezpečnosti.

V oboch segmentoch bola nadviazaná bližšia spolupráca s cieľom uzatvoriť medzinárodnú dohodu o ochrane utajovaných skutočností a memorandum o spolupráci v oblasti kybernetickej bezpečnosti.

V septembri 2022 navštívila Slovensko počas európskeho programu TAIEX delegácia zo Severného Macedónska. Príslušníci úradu pripravili viacero prezentácií a vzdelávacích aktivít najmä k vyžiadanej téme ohľadom fyzickej a objektovej bezpečnosti.

Koncom roka 2022 uzavrela vláda Slovenskej republiky bezpečnostnú dohodu s Európskou vesmírnou agentúrou (ESA).

Zintenzívnili sa aj stretnutia s českým Národným úřadem pro kybernetickou a informační bezpečnost (NÚKIB). Schôdzky boli zamerané najmä na adaptáciu národných certifikačných postupov a legislatívy na pripravovaný celoeurópsky systém certifikačných schém.

VÝMENA ZAHRANIČNÝCH INFORMÁCIÍ

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

V roku 2022 úrad jednotlivým registrom utajovaných skutočností, zriadenými orgánmi verejnej moci, naďalej poskytoval metodickú pomoc pri elektronickej evidencii utajovaných skutočností. Pracovisko centrálneho registra spracovalo **4 218 utajovaných skutočností NATO a 2 522 utajovaných skutočností EÚ.**

Úrad sprostredkoval aj výmenu **160 utajovaných skutočností cudzej moci**. Na úrade od roku 2010 pôsobí register utajovaných skutočností NATO ATOMAL. V roku 2022 v ňom neboli zaevidované žiadne ATOMAL utajované písomnosti.

V súvislosti s nadobudnutím účinnosti zákona č. 364/2020, ktorým sa mení a dopĺňa zákon č. 395/2002 o archívoch a registratúrach, Národný bezpečnostný úrad má od roku 2021 zriadené centrálne úložisko utajovaných skutočností pre dočasné uloženie utajovaných skutočností, ktoré majú trvalú dokumentárnu hodnotu.

Centrálne úložisko utajovaných skutočností je zriadené na detašovanom pracovisku v Topoľčiankach.

K prioritám pre rok 2023 patrí naďalej spustenie integrácie elektronického informačného systému pre správu registratúry s vonkajším prostredím.

Stupeň utajenia	2021	2022
NATO — RESTRICTED	1739	1833
EU — RESTRICTED	693	886
CUDZIA MOC — VYHRADENÉ	48	114
NATO — CONFIDENTIAL	732	568
EU — CONFIDENTIAL	486	750
CUDZIA MOC — DÔVERNÉ	49	39
NATO — SECRET	1209	1770
EU — SECRET	346	886
CUDZIA MOC — TAJNÉ	3	7
NATO — TOP SECRET	0	0
EU — TOP SECRET	0	0
CUDZIA MOC — PRÍSNE TAJNÉ	3	0
NATO – spolu	**3680**	**4218**
EU — spolu	**1525**	**2522**
CUDZIA MOC — spolu	**103**	**160**

HOSPODÁRENIE

Rozpis záväzných ukazovateľov rozpočtu kapitoly 41 – Národný bezpečnostný úrad na rok 2022, vplyv rozpočtových opatrení na výšku upraveného rozpočtu, skutočné čerpanie rozpočtových prostriedkov k 31. decembru 2022 a percentuálne vyhodnotenie plnenia k upravenému rozpočtu je uvedený v tabuľke č. 1

Záväzné ukazovatele rozpočtu úradu pre rok 2022 schválené zákonom č. 534/2021 o štátnom rozpočte na rok 2022 boli úradom dodržané. Pri hospodárení s finančnými prostriedkami úrad postupoval podľa zásad hospodárnosti, efektívnosti a účelnosti pri dodržiavaní legislatívnych predpisov, najmä zákona č. 523/2004 o rozpočtových pravidlách verejnej správy, zákona č. 357/2015 o finančnej kontrole a audite, zákona č. 343/2015 o verejnom obstarávaní, uznesení vlády Slovenskej republiky a metodických pokynov a usmernení Ministerstva financií Slovenskej republiky.

ROZPOČET NA ROK 2023

Zákonom č. 526/2022 o štátnom rozpočte na rok 2023 boli schválené záväzné ukazovatele štátneho rozpočtu jednotlivých kapitol na rok 2023. V nadväznosti na bod C. 1. uznesenia vlády SR č. 636 k návrhu rozpočtu verejnej správy na roky 2023 až 2025 a ustanovenie § 6 ods. 3 zákona č. 523/2004 o rozpočtových pravidlách verejnej správy boli úradu oznámené záväzné ukazovatele štátneho rozpočtu na rok 2023.

Výdavky úradu pre rok 2023 sú rozpočtované v programe 0D9 – Bezpečnosť informácií a medzirezortnom podprograme 0EK0U – Informačné technológie financované zo štátneho rozpočtu – NBÚ v celkovej sume 14 612 255,00 eur. Príjmy úradu ako záväzný ukazovateľ sú rozpočtované v sume 20 000,00 eur, príjmy pod kódom zdroja 72e sú rozpočtované v sume 2 000,00 eur.

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

VEREJNÉ OBSTARÁVANIE

Analytici z portálu **Transparex.sk** zostavili v roku 2022 rebríček „Zodpovedných verejných obstarávateľov za rok 2021“. Rebríček pozostával zo všetkých štátnych organizácií – mestá a obce, kraje, Ústredné orgány štátnej správy, nemocnice, podniky vo vlastníctve štátu, škôlky a školy. Národný bezpečnostný úrad sa v ňom umiestnil na 2. mieste s celkovým hodnotením 87,16 bodov a so známkou A+, čo znamená „veľmi zodpovedný obstarávateľ“.

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

NÁRODNÁ KULTÚRNA PAMIATKA – KAŠTIEĽ BRUNOVCE

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

Do vypuknutia pandémie covidu bol kaštieľ v obmedzenej miere prístupný miestnej komunite aj širokej verejnosti a zároveň bol v uvedenom období využívaný predovšetkým na služobné účely ako školiace stredisko, ale aj na rôzne súkromné akcie pracovníkov úradu a tiež pre ostatných občanov za účelom ubytovania alebo prenájmu priestorov v interiéroch a exteriéroch kaštieľa (napr. svadobné fotenie, oslavy výročia obce a s tým spojená svätá omša v priestoroch spomínanej kaplnky kaštieľa).

Vzhľadom na nevyhovujúci technický stav tejto národnej kultúrnej pamiatky, úrad v roku 2022 pristúpil k zámeru jej kompletnej obnovy. Hlavným cieľom je získať finančné prostriedky z priorít Plánu obnovy a odolnosti Slovenskej republiky pri obnove verejných historických a pamiatkovo chránených budov.

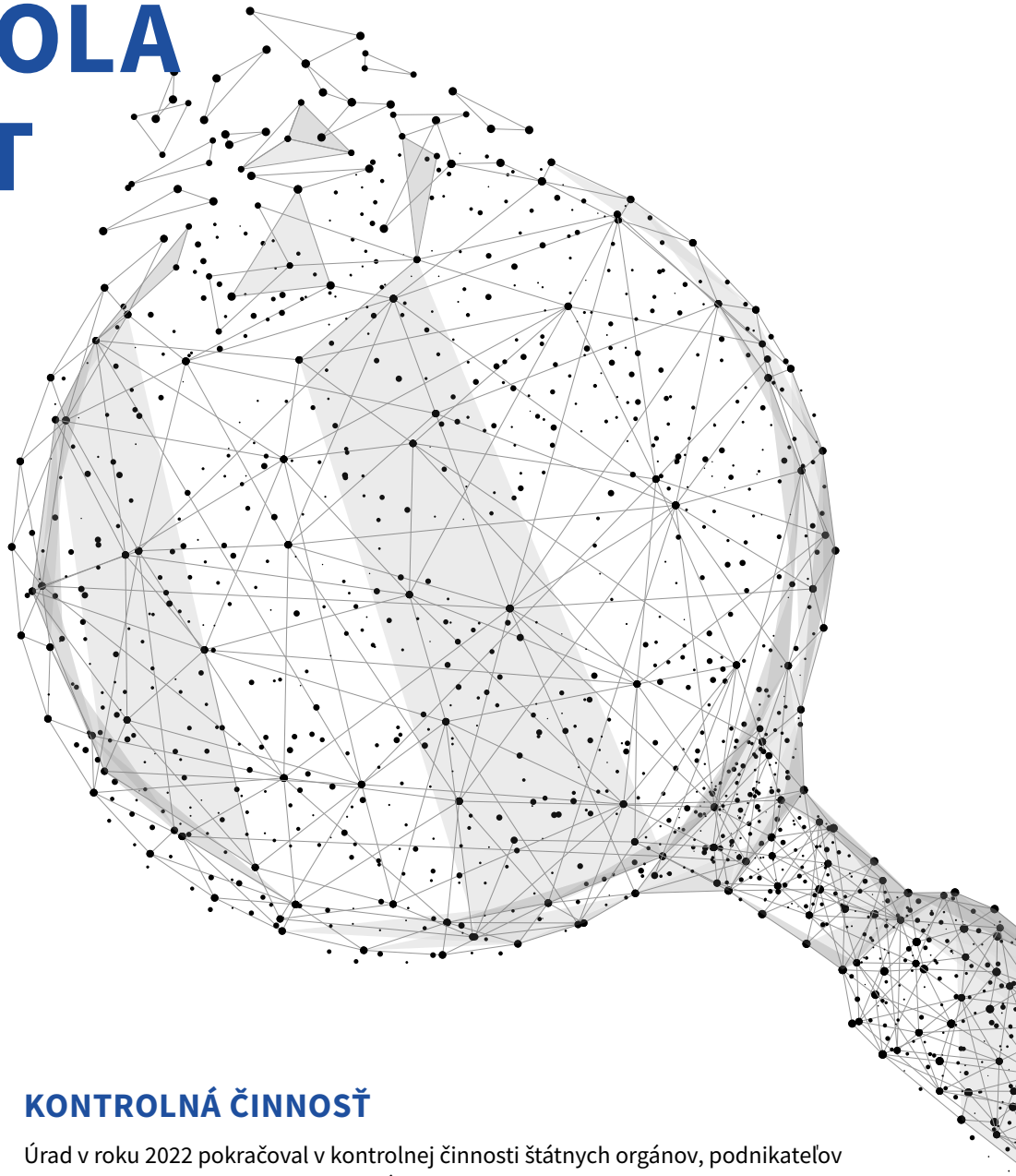
Rekonštrukcia bude zameraná predovšetkým na zlepšenie energetickej hospodárnosti kaštieľa a po schválení príslušným pamiatkovým úradom budú realizované aktivity súvisiace so stavebno-technickou obnovou a implementáciou zelených opatrení s predĺžením životnosti a možnosti širšieho využitia tejto národnej kultúrnej pamiatky.

Tabuľka č. 1: Rozpočet Národného bezpečnostného úradu v roku 2022 (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**	**38 424,22**	**192,12%**
A. Záväzný ukazovateľ	20 000,00	20 000,00	38 424,22	192,12%
B. Prostriedky Európskej únie	0,00	0,00	0,00	
II. Výdavky kapitoly celkom (A + B+ C + C.1)	**12 844 288,00**	**14 474 812,33**	**13 885 343,39**	**95,93%**
A. Výdavky spolu bez prostriedkov podľa § 17 ods. 4 zákona				
č. 523/2004 Z. z. a prostriedkov Európskej únie	**12 842 288,00**	**14 436 307,40**	**13 846 838,46**	**95,92%**
z toho:				
A.1. rozpočtové prostriedky kapitoly	12 842 288,00	14 424 566,63	13 835 097,69	95,91%
z toho: kód zdroja 111 + 11H + 11UA	12 842 288,00	13 353 915,99	13 065 873,33	97,84%
kód zdroja 131	0,00	1 070 650,64	769 224,36	71,85%
A.2. prostriedky na spolufinancovanie	0,00	11 740,77	11 740,77	100,00%
z toho: kód zdroja 3AA2	0,00	6 313,99	6 313,99	100,00%
kód zdroja 3AA3	0,00	5 426,78	5 426,78	100,00%
A.3. mzdy, platy, služ. príj. a ost. os. vyrovnania (610), (kód zdroja 111 + 11H)	6 494 929,00	6 707 686,00	6 491 911,86	96,78%
z toho: mzdy, platy, služ. príjmy a ost. os. vyrovnania aparátu ústred.				
orgánu (kód zdroja 111 + 11H + 11UA)	6 494 929,00	6 707 686,00	6 491 911,86	96,78%
Počet zamestnancov RO podľa prílohy č. 1 k uzneseniu vlády SR č. 577/2021	250 osôb	254 osôb	214 osôb*	84,25%
z toho: aparát ústredného orgánu	250 osôb	254 osôb	214 osôb*	84,25%
administratívne kapacity rozpočtových organizácií osobitne				
sledované podľa prílohy č. 1 k uzneseniu vlády SR č. 577/2021	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)	250 000,00	1 343 795,81	1 042 369,53	77,57%
z toho: kód zdroja 111	250 000,00	273 145,17	273 145,17	100,00%
kód zdroja 131I	0,00	240 665,88	108 665,88	45,15%
kód zdroja 131J	0,00	431 382,36	261 956,08	60,72%
kód zdroja 131K	0,00	368 360,00	368 360,00	100,00%
kód zdroja 131L	0,00	30 242,40	30 242,40	100,00%
A.5. Plán obnovy a odolnosti – prostriedky na úhradu DPH	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 zdôvodu dosiahnutia vyšších ako rozpočt. príjmov.)	**2 000,00**	**2 725,70**	**2 725,70**	**100,00%**
C. Prostriedky Európskej únie	**0,00**	**35 779,23**	**35 779,23**	**100,00%**
z toho: kód zdroja 3AA1	0,00	35 779,23	35 779,23	100,00%
C.1 Prostriedky z plánu obnovy a odolnosti	**0,00**	**0,00**	**0,00**	
D. Výdavky štátneho rozpočtu na realizáciu programov vlády SR a časti programov vlády SR	**12 844 288,00**	**14 474 812,33**	**13 885 343,39**	**95,93%**
0D9 Bezpečnosť informácií	12 657 784,00	14 308 694,33	13 733 505,30	95,98%
0EK0U Informačné technológie financované zo štátneho rozpočtu – NBÚ	186 504,00	166 118,00	151 838,09	91,40%
E. Systemizácia policajtov v štátnej službe	**228 osôb**	**232 osôb**	**192 osôb***	**82,76%**
	5 905 472,00	**6 111 867,00**	**5 963 241,23**	**97,57%**

KONTROLA A AUDIT



KONTROLNÁ ČINNOSŤ

Úrad v roku 2022 pokračoval v kontrolnej činnosti štátnych orgánov, podnikateľov a jednej medzinárodnej organizácie. Úrad celkovo vykonal kontrolu v 22 subjektoch.

Podľa zákona č. 215/2004 o ochrane utajovaných skutočností bolo skontrolovaných 10 subjektov, v ktorých predmetmi kontroly boli rôzne kombinácie oblastí: ochrana utajovaných skutočností (9-krát), šifrová ochrana informácii (2-krát) a kontrola splnenia opatrení (1-krát).

Dohľad plnenia záväzkov vyplývajúcich z členstva v NATO bola realizovaná v jednom subjekte a kontrola v oblasti kybernetickej bezpečnosti bola vykonaná v 11 subjektoch.

Kontrolné skupiny sa zamerali najmä na komplexnosť prijatých opatrení a ich koordináciu naprieč jednotlivými oblasťami bezpečnosti. Nedostatky boli zistené v štrnástich kontrolovaných subjektoch. Kontrolné skupiny v roku 2022 zaznamenali celkovo 62 kontrolných zistení:

- 51 v oblasti kybernetickej bezpečnosti,
- 0 v oblasť fyzickej a objektovej bezpečnosti,
- 3 v oblasti technických prostriedkov,
- 5 v oblasti personálnej bezpečnosti,
- 3 v oblasti administratívnej bezpečnosti.

METODICKÁ ČINNOSŤ

Bezpečnostná rada Slovenskej republiky na svojom 145. zasadnutí 2. februára 2022 prijala k aktuálnej bezpečnostnej situácii (vojna na Ukrajine) súbor návrhov opatrení s cieľom zabezpečiť spoľahlivú koordináciu opatrení na zachovanie bezpečnosti štátu a predchádzania krízovým situáciám. Pre úrad vyplynula úloha koordinovať činnosti na úseku ochrany utajovaných skutočností. V tejto súvislosti úrad spracoval pre dotknuté subjekty zoznam nasledujúcich opatrení aj so spôsobom ich riešenia:

- zvýšiť stupeň vykonanej bezpečnostnej previerky pre kľúčové osoby,
- aktualizovať postupy pri ochrane utajovaných skutočností v prípade mimoriadnej situácie a krízovej situácie,
- zabezpečiť náležitú ochranu utajovaných skutočnosti pri manipulácii a ich ukladaní vedúcim,
- aktualizovať zoznamy utajovaných skutočností,
- zabezpečiť spojenie centrálneho registra utajovaných skutočností s rezortnými registrami formou pohotovostných služieb.

Na úseku **regulácie a metodiky** úrad vydáva stanoviská a metodiky (metodické usmernenia) k všeobecne záväzným právnym predpisom a dokumentom v pôsobnosti úradu, pripravuje návrhy všeobecne záväzných právnych predpisov do legislatívneho procesu, pripomienkuje a vypracúva stanoviská k návrhom legislatívnych materiálov v **medzirezortnom pripomienkovom konaní** (sekcia regulácie a dohľadu eviduje 527 riešených pripomienkových konaní z hľadiska svojej vecnej pôsobnosti, kde nie sú započítané MPK riešené ostatnými útvarmi, a tiež žiadosti o substanoviská adresované sekcii regulácie a dohľadu).

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

Úrad v roku 2022 vydal **157 metodických usmernení**:

V oblasti ochrany utajovaných skutočností	
PERSONÁLNA BEZPEČNOSŤ	**37**
ADMINISTRATÍVNA BEZPEČNOSŤ	**7**
PRIEMYSELNÁ BEZPEČNOSŤ	**18**
FYZICKÁ BEZPEČNOSŤ A OBJEKTOVÁ BEZPEČNOSŤ	**6**
BEZPEČNOSŤ TECHNICKÝCH PROSTRIEDKOV	**2**
BEZPEČNOSTNÍ ZAMESTNANCI	**1**
LETECKÉ SNÍMKOVANIE	**5**
CUDZIA MOC	**9**
V oblasti šifrovej ochrany informácií	1
V oblasti kybernetickej bezpečnosti	21
V oblasti dôveryhodných služieb	15
Prierezové stanoviská	35
Spolu	85

DOHĽADOVÁ ČINNOSŤ

Úrad v roku 2022 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 (EÚ) č. 910/2014.

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.

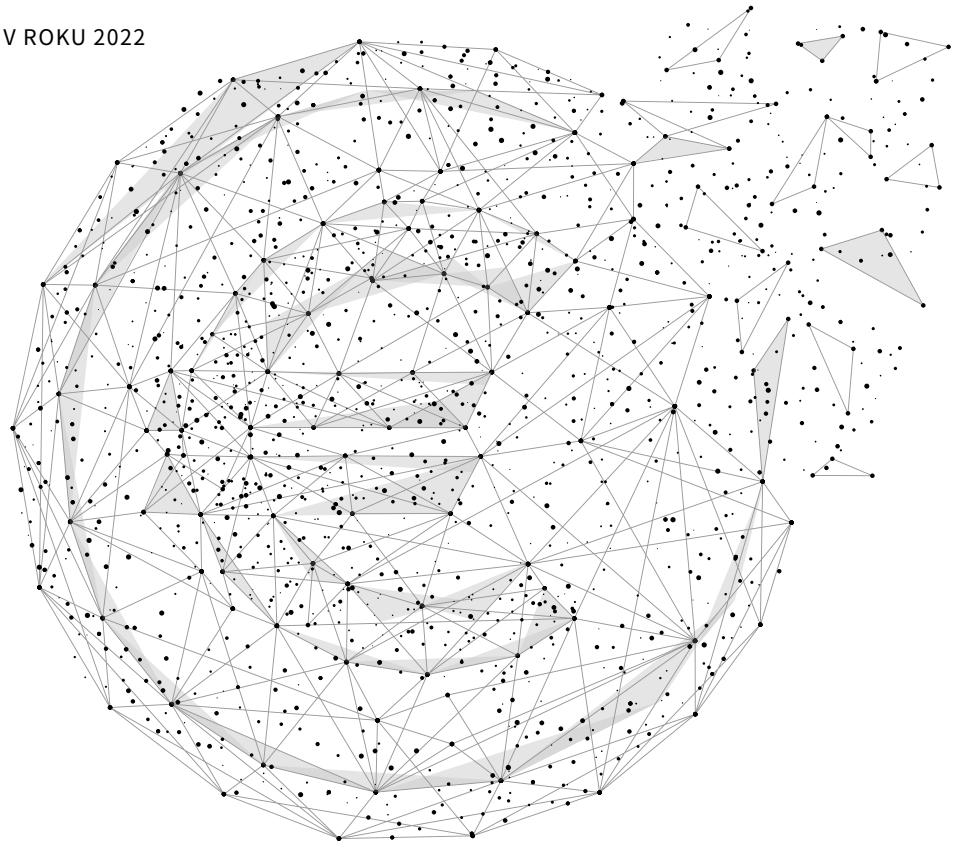
V **predbežnom dohľade** boli analyzované správy o posúdení zhody od štyroch kvalifikovaných poskytovateľov dôveryhodných služieb. Bolo udelených 18 kvalifikovaných štatútov na kvalifikovanú dôveryhodnú službu.

V **následnom dohľade** boli analyzované správy o posúdení zhody, t. j. doručené správy z pravidelného 24-mesačného auditu od troch kvalifikovaných poskytovateľov dôveryhodných služieb a dve správy z kontrolného auditu od dvoch kvalifikovaných poskytovateľov dôveryhodných služieb.

VNÚTORNÁ KONTROLA

Vnútorný kontrolný orgán úradu v roku 2022 vykonal 12 vnútorných kontrol. Štyri vykonané kontroly sa týkali vecného plnenia úloh z uznesení vlády. Ďalšie kontroly boli zamerané najmä na kontrolu dodržiavania času služby príslušníkov a zamestnancov úradu, kontrolu dodržiavania povinností vyplývajúcich z interných predpisov v oblasti prevádzky služobných motorových vozidiel, pridelenia a evidencie služobných zbraní a streliva, iného taktického materiálu, kontroly služobných preukazov, vyšetrenia na zistenie alkoholu v krvi a kontrolu plnenia povinnosti príslušníkov a zamestnancov vyplývajúcich z ich uskutočnených zahraničných ciest a prijatí.

Okrem prípadov malého významu nebolo pri kontrolách zistené porušenie všeobecne záväzných právnych predpisov.



VNÚTORNÝ AUDIT

V roku 2022 boli útvarom vnútorného auditu vykonané 4 plánované vnútorné audity, ktorých cieľom bolo overiť a hodnotiť:.

- dodržiavanie § 8f zákona č. 278/1993 o správe majetku štátu za roky 2020 a 2021 v povinnej osobe NBÚ,
- hospodárnosť, efektívnosť, účinnosť a účelnosť pri hospodárení s verejnými financiami za rok 2021 v povinnej osobe NBÚ,
- dodržiavanie zákona č. 10/1996 o kontrole v štátnej správe za roky 2020 a 2021 v povinnej osobe NBÚ,
- hospodárnosť, efektívnosť, účinnosť a účelnosť pri hospodárení s verejnými financiami za rok 2021 v povinnej osobe Kompetenčné a certifikačné centrum kybernetickej bezpečnosti.

Vykonanými vnútornými auditmi bolo zistených 10 nedostatkov nízkej a strednej závažnosti, ktoré ale nemali finančné dôsledky.

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.

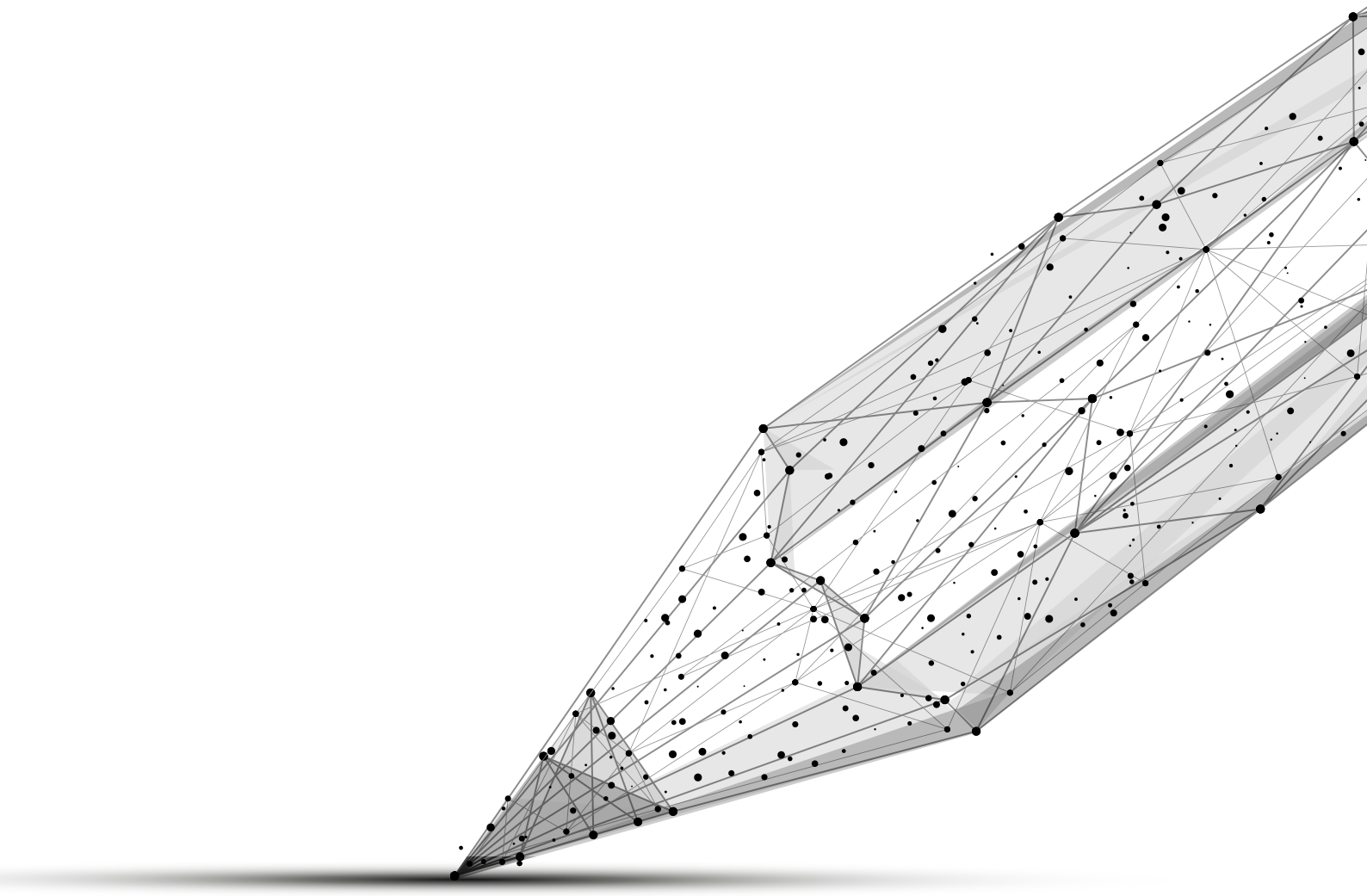
BEZPEČNOSTNÉ RIZIKÁ

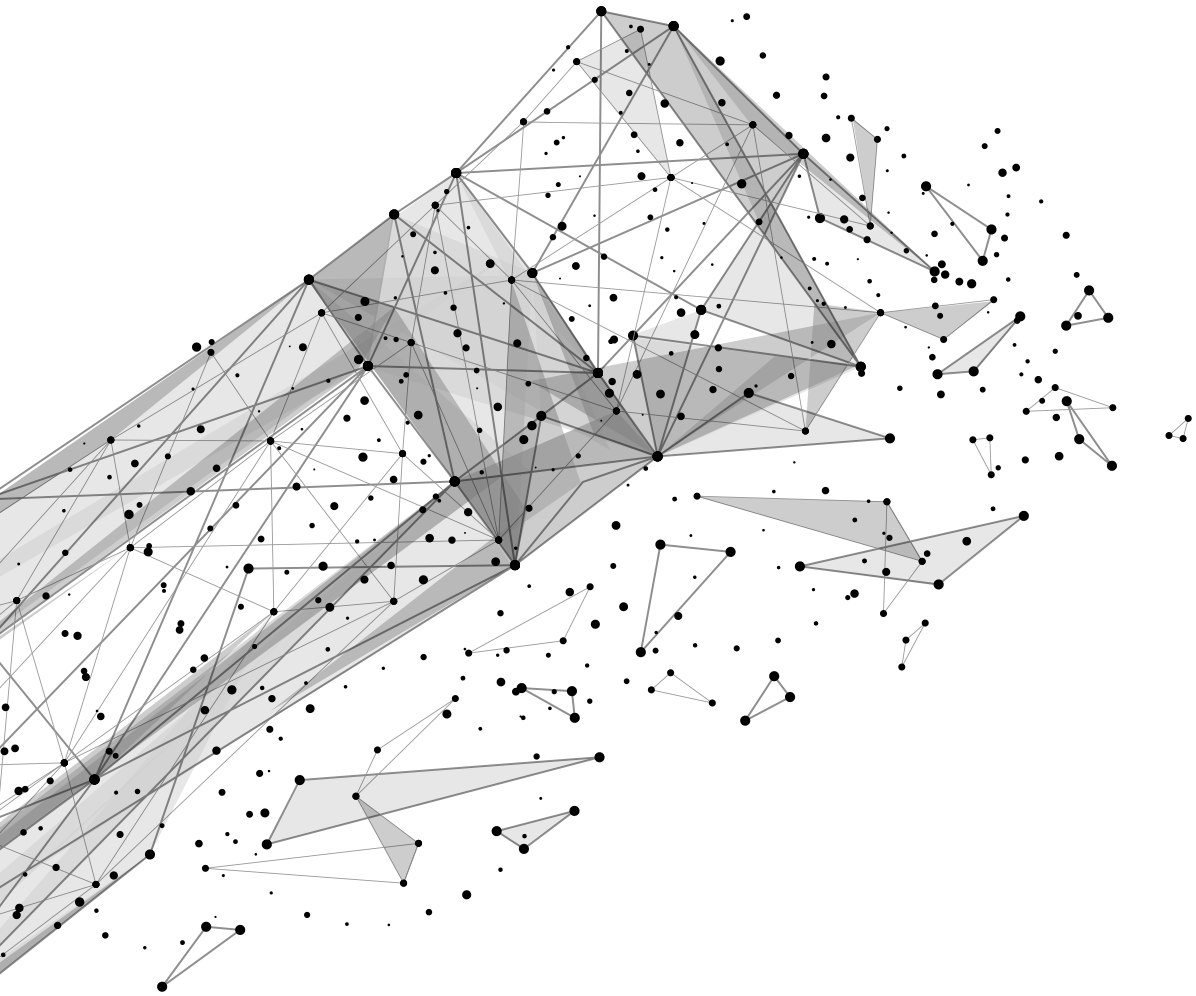
Úrad v roku 2022 na úseku vnútornej bezpečnosti získaval, sústreďoval, analyzoval a preveroval informácie o bezpečnostných rizikách týkajúcich sa pôsobnosti úradu, jeho príslušníkov a zamestnancov.

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 2022 nebola úradu doručená žiadna petícia.

PRIORITY
NA ROK 2023





Národný bezpečnostný úrad bude na úseku dôveryhodných služieb modernizovať vybrané prevádzkované komponenty dôveryhodnej infraštruktúry.

Na úseku šifrovej ochrany informácií bude pokračovať v budovaní zabezpečenej infraštruktúry v jednotlivých segmentoch.

Prioritou ďalej zostávajú vzdelávanie a výcvik špecialistov na odborných kurzoch, seminároch a školeniach doma i v zahraničí s cieľom nadobúdať nové zručnosti a prehlbovať ich kvalifikáciu.

Úrad bude kontinuálne rozvíjať spôsobilosti v oblasti certifikácie mechanických zabezpečovacích, technických zabezpečovacích a technických prostriedkoch, či prostriedkoch šifrovej ochrany.

K prioritám pre rok 2023 patrí aj realizácia projektov:
- projekt Elektronické služby spracovania bezpečnostných spisov Národného bezpečnostného úradu, ktorý je zameraný na vytvorenie informačných systémov pre elektronizáciu služieb NBÚ v oblasti ochrany utajovaných skutočností a interných procesov súvisiacich s bezpečnostnými previerkami fyzických osôb a podnikateľov,
- projekt vybudovanie novej fyzickej a objektovej bezpečnosti,
- projekt implementácie modelu CAF (Common Assessment Framework) zameraný na rozvoj systému manažérstva a získaného medzinárodného certifikátu kvality.