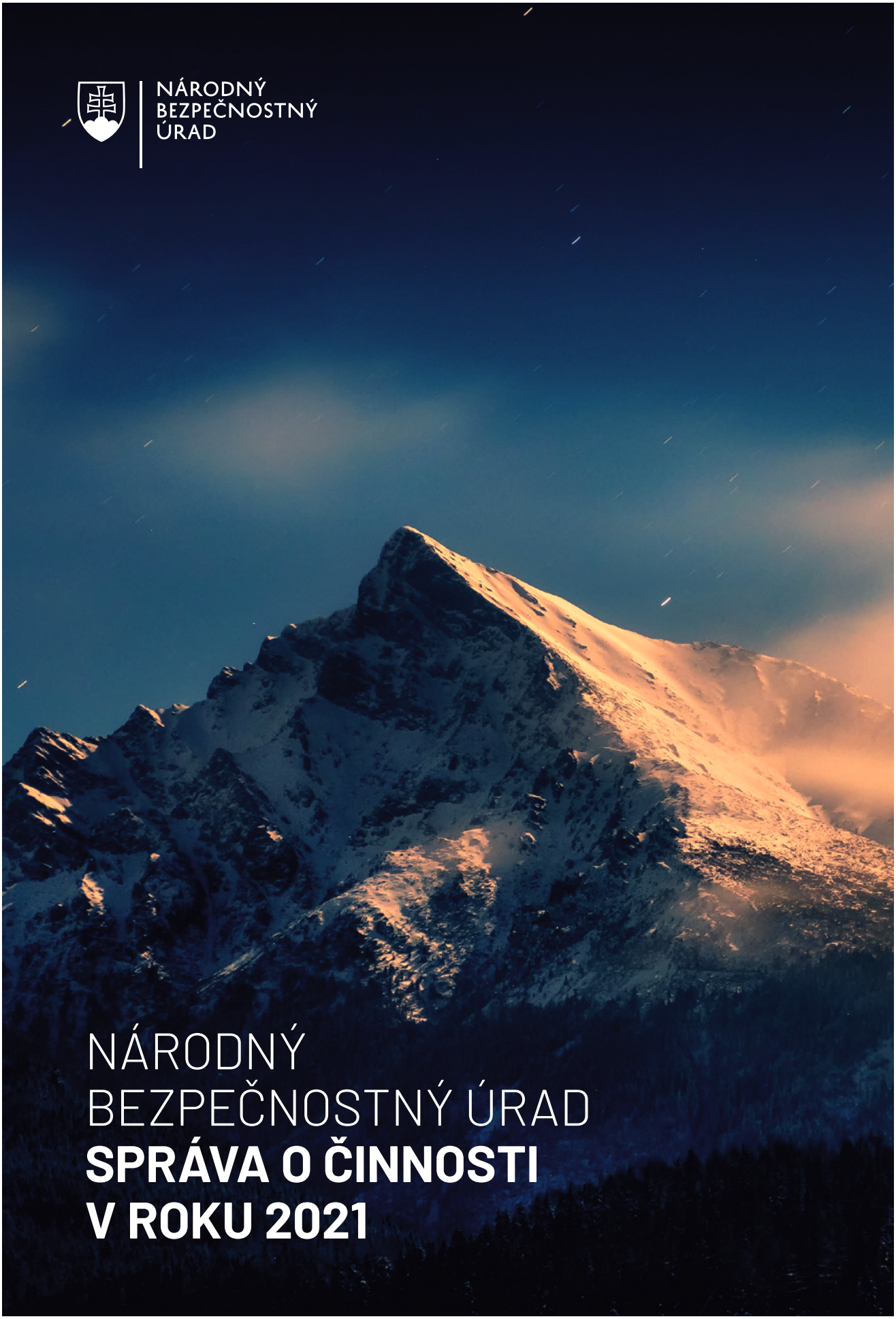

NÁRODNÝ
BEZPEČNOSTNÝ
ÚRAD
NÁRODNÝ
BEZPEČNOSTNÝ ÚRAD
SPRÁVA O ČINNOSTI
V ROKU 2021

OBSAH

1 IDENTIFIKÁCIA ORGANIZÁCIE 5

2 ĽUDSKÉ ZDROJE 11

3 LEGISLATÍVA 15

4 OCHRANA UTAJOVANÝCH SKUTOČNOSTÍ 19

5 ŠIFROVÁ OCHRANA INFORMÁCIÍ 27

6 DÔVERYHODNÉ SLUŽBY 29

7 KYBERNETICKÁ BEZPEČNOSŤ 33

8 MEDZINÁRODNÁ SPOLUPRÁCA 39

9 HOSPODÁRENIE 47

10 KONTROLA A AUDIT 51

11 ZÁVERY A PRIORITY NA ROK 2022 53

1. IDENTIFIKÁCIA ORGANIZÁCIE

IDENTIFIKÁCIA ORGANIZÁCIE

Národný bezpečnostný úrad zodpovedá za tvorbu a realizáciu štátnej politiky pre **oblasti ochrany utajovaných skutočností, šifrovej služby, dôveryhodných služieb a kybernetickej bezpečnosti.**

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

NBÚ 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.

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.

V oblasti šifrovej ochrany informácií vykonáva úrad certifikáciu jej prostriedkov, vydáva bezpečnostné štandardy a koordinuje výskum a vývoj prostriedkov šifrovej ochrany.

Plní úlohu gestora a národnej autority v medzinárodnej spolupráci a zabezpečuje funkciu Národnej distribučnej autority, ktorá je vstupným a kontaktným bodom Slovenskej republiky pri výmene a distribúcii šifrového materiálu a šifrovacích zariadení.

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 a takisto plní úlohu národnej jednotky CSIRT (jednotky pre riešenie kybernetických bezpečnostných incidentov).

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 postupuje úrad podľa zákona o kybernetickej bezpečnosti č. 69/2018 a podľa príslušných vyhlášok vydaných na vykonanie zákona.

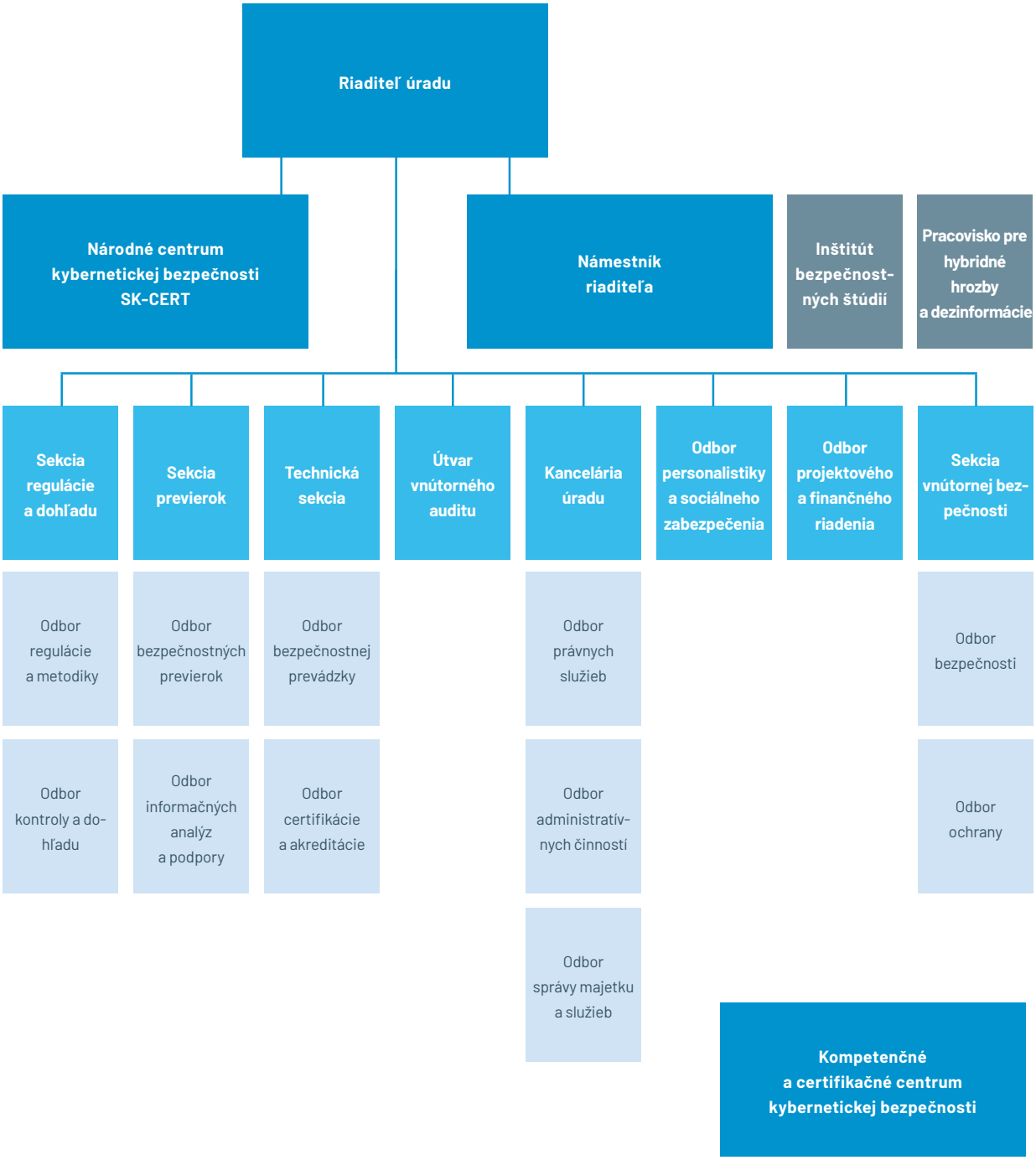
VEDENIE ÚRADU

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 certifikáty podnikateľa o priemyselnej bezpečnosti pre oboznamovanie sa s utajovanými skutočnosťami NATO a EÚ; vydáva certifikáty pre prístup k utajovaným skutočnostiam 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 styčného dôstojníka, vyslaného k zastupiteľskému úradu SR pri EÚ a k stálej delegácii NATO, plní úlohy pri rozvíjaní a budovaní medzinárodných vzťahov a spolupráce úradu v zahraničí. Styčný dôstojník zabezpečuje komunikáciu medzi úradom a zahraničnými partnermi, zastupuje záujmy Slovenskej republiky v oblastiach zverených do právomoci úradu v NATO, v európskych inštitúciách a agentúrach. Realizuje aj 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 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.

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: fyzickú a technickú ochranu objektov úradu, riaditeľa úradu a pracovníkov úradu. 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 audítora vykonáva vnútorný audit úradu a plní ďalšie úlohy podľa zákona o finančnej kontrole a audite.

2. ĽUDSKÉ ZDROJE

ĽUDSKÉ ZDROJE

2020

104 mužov

121 žien

202 príslušníkov
23 zamestnancov

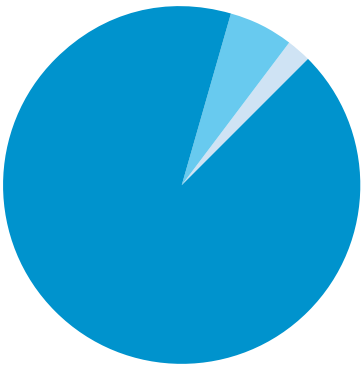
2021

102 mužov

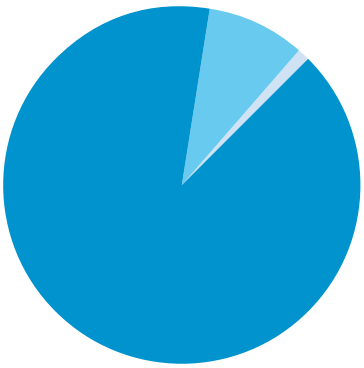
126 žien

207 príslušníkov
21 zamestnancov

Príslušníci v štátnej službe

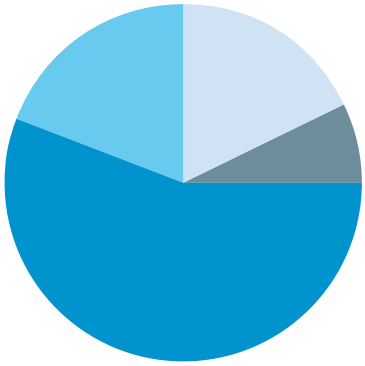


- **90 %** stála štátna služba
- **9 %** prípravná štátna služba
- **1 %** dočasná štátna služba



- **81 %** stála štátna služba
- **17 %** prípravná štátna služba
- **2 %** dočasná štátna služba

Vek

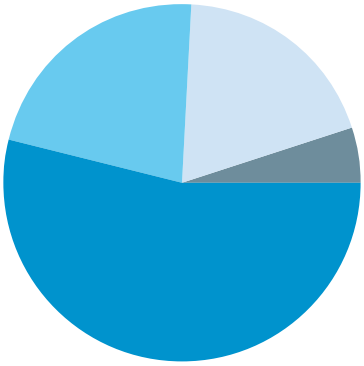


56 % 35 až 49 rokov

19 % 50 až 59 rokov

18 % mladší ako 34 rokov

7 % nad 60 rokov



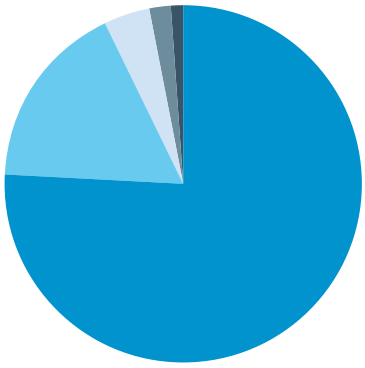
54 % 35 až 49 rokov

22 % 50 až 59 rokov

19 % mladší ako 34 rokov

5 % nad 60 rokov

Vzdelanie



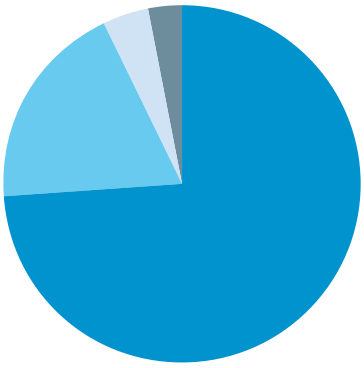
76 % vysokoškolské vzdelanie II. stupňa

17 % úplné stredné vzdelanie

4 % vysokoškolské vzdelanie III. stupňa

2 % vysokoškolské vzdelanie I. stupňa

1 % základné vzdelanie



74 % vysokoškolské vzdelanie II. stupňa

19 % úplné stredné vzdelanie

4 % vysokoškolské vzdelanie III. stupňa

3 % vysokoškolské vzdelanie I. stupňa

0 % základné vzdelanie

PREHLBOVANIE KVALIFIKÁCIE a ZVYŠOVANIE ZRUČNOSTÍ

Úrad príslušníkom a zamestnancom umožňuje udržiavať ich odbornú pripravenosť, nadobúdať nové zručnosti a prehlbovať kvalifikáciu na odborných kurzoch, seminároch a školeniach doma i v zahraničí. v prípade potreby zabezpečuje aj zvyšovanie ich kvalifikácie na vysokých školách.

Pre novoprijatých príslušníkov každoročne realizuje v spolupráci s Akadémiou Policajného zboru v Bratislave špecializované policajné vzdelávanie, ktoré je podmienkou pre zaradenie novoprijatých príslušníkov do stálej štátnej služby.

Príslušníci aj zamestnanci štandardne absolvovali vstupné a pravidelné školenia bezpečnosti a ochrany zdravia pri práci a takisto ochrany pred požiarmi.

Limitované bolo udržiavanie a zvyšovanie fyzickej kondície z dôvodu pandemických opatrení.

Príslušníci najmä sekcie vnútornej bezpečnosti pravidelne absolvujú cvičné streľby, taktické cvičenia aj simulované bezpečnostné scenáre vo viacerých objektoch ministerstva vnútra a ministerstva obrany.

BOJ PROTI KORUPCII

Národný bezpečnostný úrad nedostal v roku 2021 žiadne oznámenie o protispoločenskej činnosti vo vzťahu ku svojim príslušníkom.

4. LEGISLATÍVA

LEGISLATÍVA

Sekcia regulácie a dohľadu pracovala minulý rok na viacerých väčších legislatívnych zmenách. Výsledky niektorých legislatívnych procesov budú premietnuté do praxe v roku 2022. Kontinuálne však útvar pripravoval viaceré novely zákonov:

> príprava novely zákona č. 215/2004 o ochrane utajovaných skutočností

V roku 2021 pokračovali práce na novele zákona č. 215/2004. v auguste 2021 bola zverejnená na portáli SLOV-LEX predbežná informácia k novele zákona. Cieľom novely zákona je modernizovať systém ochrany utajovaných skutočností, postupy a procesy prispôsobiť v najvyššej možnej miere predpisom EÚ a NATO, zvýšiť kvalitu a efektivitu realizácie bezpečnostných previerok odstránením zákonných prekážok pri poskytovaní informácií potrebných pri výkone bezpečnostných previerok.

Návrhom sa prehodnotia pojmy spôsobom, aby nenavádzali na rozdielny výklad. Novela tohto zákona bude predložená do medzirezortného pripomienkového konania v roku 2022.

> začiatkom roka nadobudol účinnosť zákon č. 423/2020 Pozmenil a doplnil zákona o ochrane utajovaných skutočností. Rozšíril okruh oprávnených osôb s osobitným postavením podľa tohto zákona o člena súdnej rady.

Navrhovaná právna úprava súvisí s novými kompetenciami súdnej rady v oblasti dohľadu nad spĺňaním predpokladov sudcovskej spôsobilosti podľa zákona č. 185/2002 o Súdnej rade Slovenskej republiky. Okruh subjektov považovaných na účely zákona o ochrane utajovaných skutočností za ústredné orgány štátnej správy sa rozšíril aj o Kanceláriu Najvyššieho správneho súdu Slovenskej republiky.

> vyvrcholil legislatívny proces novely zákona č. 69/2018 o kybernetickej bezpečnosti. Národná rada Slovenskej republiky schválila novelu zákona v júni 2021. v Zbierke zákonov je novela zverejnená pod č. 287/2021 Z. z. Účinnosť nadobudla 1. augusta 2021 a jej cieľom je posilnenie legislatívnej úpravy v oblasti kybernetickej bezpečnosti, právomocí príslušných vnútroštátnych orgánov a zabezpečuje vyššiu mieru súladu s právom EÚ.

V novele zákona sa precizujú a dopĺňajú niektoré definície, upravuje sa procesný postup pri certifikácii kybernetickej bezpečnosti, ktorá vyplýva z nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti).

Novelou zákona sa posilnili kompetencie úradu v oblasti kybernetickej bezpečnosti.

Národné centrum kybernetickej bezpečnosti SK-CERT plní úlohy národnej jednotky CSIRT a súčasne je ústrednými orgánmi štátnej správy – v prípade, že nedisponujú vlastnou jednotkou CSIRT, využívaná na zabezpečenie plnenia úloh súvisiacich s kybernetickou bezpečnosťou.

Novelou zákona sa upustilo od povinnosti zriadiť a prevádzkovať vlastnú akreditovanú jednotku CSIRT, pričom ostáva aj naďalej možnosť daná na výber zriadiť si vlastnú jednotku CSIRT, v prípade, ak ústredný orgán takúto potrebu vyhodnotí pozitívne.

Novela zákona zaviedla všeobecnú povinnosť pre orgány verejnej moci, prevádzkovateľov základných služieb a príslušné právnická osoby poskytnúť úradu súčinnosť v rámci kybernetickej bezpečnosti, najmä teda, ak pôjde o také informácie, ktoré si úrad nevie zabezpečiť vlastnými prostriedkami, avšak vyžiadanie takýchto

informácií musí byť riadne odôvodnené.

Novela priniesla aj rozšírenie oblastí, pre ktoré sa bezpečnostné opatrenia v rámci kybernetickej bezpečnosti prijímajú a realizujú, vyjasnila sa úloha manažéra kybernetickej bezpečnosti a predefinovali sa ustanovenia týkajúce sa auditu kybernetickej bezpečnosti spôsobom aby vyhovovali podmienkam aplikačnej praxe a boli zrozumiteľnejšie. Súčasne sa zaviedla povinnosť automatizovaného zasielania systémových informácií zo sietí a informačných systémov pre prevádzkovateľov základných služieb. Ide o zasielanie takých údajov, ktoré sú potrebné pri riešení kybernetického bezpečnostného incidentu.

Doplnené a spresnené boli ustanovenia týkajúce sa obmedzení používania konkrétneho produktu, procesu, služby alebo tretej strany, povinností prevádzkovateľov základných služieb a sankčného mechanizmu nastaveného zákonom (priestupky a správne delikty).

Novela zároveň zaviedla možnosť zjednodušeného spôsobu overenia miery implementácie požiadaviek zákona a plnenia povinností zo strany prevádzkovateľov základných prostredníctvom tzv. samohodnotenia, ktoré plne nahrádza potrebu auditu kybernetickej bezpečnosti pre identifikovanú I. a II. kategóriu informačných systémov.

Začiatkom roka 2021 schválila vláda uznesením č. 5/2021 Národnú stratégiu kybernetickej bezpečnosti na roky 2021 až 2025. Úradu vyplynula úloha z uznesenia vlády č. 498/2020 aj zo zákona o kybernetickej bezpečnosti.

Stratégia je určená pre všetky subjekty, ktoré sa podieľajú na budovaní systému kybernetickej bezpečnosti. Určuje strategické ciele a má ambíciu moderným spôsobom reagovať na aktuálne a potenciálne bezpečnostné hrozby. Ponúka ucelený koncept riadenia informačnej a kybernetickej bezpečnosti.

Ide o východiskový strategický dokument, ktorý určuje prístup Slovenska k zvyšovaniu úrovne kybernetickej bezpečnosti. Jej víziou je posilňovanie, resp. vytvorenie otvoreného, slobodného a zároveň bezpečného kybernetického priestoru pre všetkých.

V roku 2021 pokračovala príprava realizácie stratégie, ktorá má stanoviť konkrétne časové, vecné, ale aj finančné kritéria rozvoja kybernetickej bezpečnosti na Slovensku. v druhej polovici roku 2021 schválila vláda SR uznesením č. 416/2021 Akčný plán realizácie stratégie kybernetickej bezpečnosti na roky 2021 až 2025, ktorý obsahuje konkrétne úlohy pre jednotlivé ústredné orgány štátnej správy v medziach ich kompetencií a prípadné vplyvy, ktoré nová alebo upravená legislatíva prinesie.

Aktívne sme participovali na príprave návrhu novej Bezpečnostnej stratégie Slovenskej republiky a Obrannej stratégie Slovenskej republiky najmä v častiach o činnostiach a operáciách v kybernetickom priestore.

Po zverejnení návrhu revízie nariadenia eIDAS počas roku 2021, sa aktívne zúčastňuje na procese príprav revízie nariadenia eIDAS, ktoré by malo nadobudnúť účinnosť koncom roku 2022, navrhuje postupy ktoré sa stanú súčasťou implementačných aktov, najmä príprav peňaženky digitálnej identity v expertných skupinách Európskej komisie.

INTERNÉ PREDPISY

Kancelária úradu vydala 15 nariadení riaditeľa úradu, 43 rozkazov riaditeľa úradu a dva štatúty.

Nariadenia a štatúty majú zefektívniť vnútorné procesy a implementovať všeobecne záväzné právne predpisy, napr. nové nariadenie o vybavovaní oznámení o protispoločenskej činnosti, o opatreniach v oblasti prevencie korupcie, o finančnom riadení a finančnej kontrole, o rezortnej koordinačnej skupine, o terminologickej skupine, úprava organizačného poriadku alebo úprava činnosti rozkladovej komisie a poradnej komisie.

Nové štatúty majú útvary vnútorného auditu a pracovisko pre hybridné hrozby a dezinformácie.

Rozkazy riaditeľa úradu slúžili na určenie nositeľov konkrétnych úloh – napr. pri zriaďovaní projektových tímov, menovaní členov do rôznych komisií alebo inventarizácii majetku.

SPRÁVNE a PRIESTUPKOVÉ KONANIE

Úrad ako správny orgán **prijal 10 podnetov** na neoprávnenú manipuláciu s utajovanými skutočnosťami a v **8 podnetoch**, v ktorých preveroval porušenie zákona o ochrane utajovaných skutočností, uložil pokuty za spáchanie priestupku na úseku ochrany utajovaných skutočností v súhrnnej sume 500 eur a za spáchanie správneho deliktu na úseku ochrany utajovaných skutočností v súhrnnej sume 4 200 eur.

NBÚ prijal aj jedno podanie na úseku leteckého snímkovania. Vec odložil záznamom, lebo nebol spáchaný priestupok podľa zákona o ochrane utajovaných skutočností.

4. OCHRANA UTAJOVANÝCH SKUTOČNOSTÍ

OCHRANA UTAJOVANÝCH SKUTOČNOSTÍ

Národný bezpečnostný úrad aj v roku 2021 aplikoval všetky dostupné opatrenia, aby pretrvávajúca pandémia neovplyvnila systém zabezpečenia ochrany utajovaných skutočností.

PERSONÁLNA BEZPEČNOSŤ

Bezpečnostné previerky fyzických osôb sú jednou z hlavných a kľúčových činností NBÚ.

Sekcia previerok minulý rok vydala **6057 osvedčení na oboznamovanie sa s utajovanými skutočnosťami stupňov Dôverné, Tajné a Prísne tajné**; z toho 3630 pre príslušníkov a zamestnancov ministerstva obrany.

	2020	2021
Dôverné	**1924**	**1947**
pre MO SR	377	318
Tajné	**2409**	**3662**
pre MO SR	1915	3034
Prísne tajné	**279**	**448**
pre MO SR	133	278
SPOLU	**4612**	**6057**

V roku 2021 **vydal úrad 98 rozhodnutí** a fyzické osoby podali **18 odvolaní proti rozhodnutiu** úradu. v jednom prípade NBÚ rozhodol v autoremedúre.

Výbor Národnej rady Slovenskej republiky na preskúmavanie rozhodnutí Národného bezpečnostného úradu rozhodoval o 15 odvolaniach.

V trinástich prípadoch ich zamietol, dve rozhodnutia úradu zrušil. k 31.12.2021 bolo 5 odvolaní v odvolacom procese.

Navrhované osoby podali proti rozhodnutiu dve žaloby na Najvyšší súd SR.

	2020	2021
Rozhodnutia úradu	**42**	**98**
Odvolania	**12**	**18**
Odvolania – autoremedúra	1	1
Odvolania zamietnuté výborom	8	13
Rozhodnutia zrušené výborom	1	2
Podané žaloby na najvyššom súde	1	2

Vo vzťahu k utajovaným skutočnostiam postupovaným NATO a EÚ vydal úrad navrhovaným osobám **7713 certifikátov**, z toho **3827 certifikátov NATO** a **3886 certifikátov EÚ**.

Z celkového počtu certifikátov NATO úrad vydal **7 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.

NBÚ vydal **94 potvrdení o priemyselnej bezpečnosti**, z toho **2 potvrdenia stupňa utajenia Vyhradené, 78 potvrdení stupňa utajenia Dôverné, 11 potvrdení stupňa utajenia Tajné** a **3 potvrdenia stupňa utajenia Prísne tajné.**

Stupeň utajenia	2020	2021
Vyhradené	5	2
Dôverné	66	78
Tajné	17	11
Prísne tajné	2	3
Spolu	**90**	**94**

Úrad vydal 20 **rozhodnutí,** odvolanie proti nim podali deviati podnikatelia.

V troch prípadoch rozhodol úrad v autoremedúre a v jednom prípade podnikateľ zmeškal lehotu na odvolanie. Výbor rozhodol o piatich odvolaniach. Výbor päť odvolaní zamietol a nezrušil žiadne rozhodnutie úradu. Ku koncu roka nebolo žiadne odvolanie v odvolacom procese.

Na najvyššom súde bola podaná 1 žaloba.

	2020	2021
Rozhodnutia úradu	**17**	**20**
Odvolania	**4**	**9**
Odvolania – autoremedúra	1	3
Odvolania zamietnuté výborom	3	5
Rozhodnutia zrušené výborom	0	0
Podané žaloby na najvyššom súde	1	1

Vo vzťahu k utajovaným skutočnostiam NATO a EÚ vydal úrad podnikateľom **7 certifikátov NATO** a **7 certifikátov EÚ**, ktoré oprávňujú podnikateľov oboznamovať sa v utajovanými skutočnosťami NATO, resp. EÚ.

Úrad má uzatvorených **16 zmlúv** o prístupe podnikateľa k utajovaným skutočnostiam, v roku 2021 úrad **uzatvoril 1 zmluvu**.

ADMINISTRATÍVNA BEZPEČNOSŤ

V roku 2021 úrad **prijal a odoslal 1735 utajovaných registratúrnych záznamov.**

Vyhláškou Národného bezpečnostného úradu č. 48/2019, ktorou sa ustanovujú podrobnosti o administratívnej bezpečnosti utajovaných skutočností, sa zjednotil proces evidovania so systémom evidencie registratúrnych záznamov utajovaných skutočností s registratúrnymi záznamami ešte v roku 2020.

V roku 2021 bol na evidenciu utajovaných a neutajovaných registratúrnych záznamov plne využívaný elektronický informačný systém pre správu registratúry.

(poznámka: údaje o výmene utajovaných skutočnostiach v internom prostredí – interná komunikácia medzi útvarmi v celkových počtoch nie je uvedená)

Stupeň utajenia	2020	2021
Vyhradené	3561	826
Dôverné	807	898
Tajné	13	11
Prísne tajné	0	0
Spolu	**4381**	**1735**

4. OCHRANA UTAJOVANÝCH SKUTOČNOSTÍ

FYZICKÁ BEZPEČNOSŤ a OBJEKTOVÁ BEZPEČNOSŤ

Úrad v roku 2021 posudzoval opatrenia fyzickej bezpečnosti a objektovej bezpečnosti na ochranu utajovaných skutočností, a to v rámci realizovaných bezpečnostných previerok podnikateľov. Vykonaných bolo **40 posúdení** (v roku 2020 posudzoval úrad v 32 prípadoch).

Vydali sme 40 certifikátov mechanických zábranných a technických zabezpečovacích prostriedkov.

Stupeň utajenia	Vyhradené	Dôverné	Tajné	Prísne tajné	Spolu
MZP	0	7	4	2	**13**
TZP	**0**	**10**	**10**	7	**27**
Spolu	**0**	**17**	**14**	**9**	**40**

BEZPEČNOSŤ TECHNICKÝCH PROSTRIEDKOV

Za rok 2021 úrad vydal 45 certifikátov technických prostriedkov a 8 dodatkov k už vydaným certifikátom technických prostriedkov.

Stupeň utajenia	Vyhradené	Dôverné	Tajné	Prísne tajné	Spolu
TP	12	24	9	0	**45**

AKREDITÁCIA KOMUNIKAČNÝCH A INFORMAČNÝCH SYSTÉMOV

NBÚ vykonal 2 akreditácie komunikačných a informačných systémov NATO v súlade s Bezpečnostnou politikou NATO C-(2002)49-REV1 a 2 akreditácie komunikačných a informačných systémov EÚ v súlade s Rozhodnutím rady (2013/488/EÚ).

Koncom roka sme certifikovali a schválili do prevádzky BKIS-V (Bezpečný komunikačno-informačný systém pre stupeň utajenia Vyhradené.

Jeho súčasťou je **Automatizovaný systém na správu registratúry (FABASOFT),** určený na prácu s utajovanými skutočnosťami stupňa utajenia Vyhradené.

OCHRANA PRED NEŽIADUCIM ELEKTROMAGNETICKÝM VYŽAROVANÍM

Úrad vykonával zónové merania chránených priestorov (mobilnou meracou aparatúrou) a merania technických prostriedkov a prostriedkov šifrovej ochrany informácií v špecializovanom TEMPEST laboratóriu na zabezpečenie ochrany utajovaných skutočností pred únikom cez nežiaduce elektromagnetické vyžarovanie.

Na základe doručených žiadostí príslušníci úradu vykonali **678 meraní zariadení** (technických prostriedkov a prostriedkov šifrovej ochrany informácií) a **69 zónových meraní priestorov,** na základe ktorých bolo kategorizovaných 183 komponentov zariadení technických prostriedkov a 96 miestností.

Príslušníci vykonali aj technické bezpečnostné prehliadky priestorov – **32 prehliadok miestností a 35 motorových vozidiel.**

BUDOVANIE BEZPEČNOSTNÉHO POVEDOMIA

Úrad vykonáva skúšky bezpečnostného zamestnanca a preškolenia osôb v rôznych oblastiach bezpečnosti. v minulosti boli zabezpečované prezenčnou formu v sídle úradu. Nielen globálna pandémia urýchlila presun týchto aktivít do virtuálneho priestoru.

Príslušníci úradu vykonávajú skúšanie žiadateľov formou on-line testu v prostredí samostatnej webovej aplikácie. Komunikácia počas skúšky prebieha vo virtuálnej video-konferenčnej miestnosti.

V minulom roku pozval úrad na skúšku 556 uchádzačov, úspešne ju vykonalo 417 z nich (85 uchádzačov bolo neúspešných, zvyšok sa na skúške nezúčastnil).

Príslušníci pozvali na preškolenie 851 uchádzačov, úspešne ju absolvovalo 783 ľudí.

V roku 2021 bolo vydaných aj 8 nových potvrdení o absolvovaní skúšky (tzv. „duplikáty“) na žiadosť držiteľov potvrdenia.

5. ŠIFROVÁ OCHRANA INFORMÁCIÍ

ŠIFROVÁ OCHRANA INFORMÁCIÍ

ŠIFROVÁ OCHRANA INFORMÁCIÍ

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

Úrad v roku 2021 zabezpečoval správu systémov a prostriedkov ŠOI prevádzkovaných na úrade a v orgánoch štátnej správy. Priebežne zabezpečoval operatívne požiadavky rezortov a poskytoval im súvisiacu podporu, najmä výrobu a distribúciu národného šifrového materiálu a poradenstvo pre údržbu používaných systémov a prostriedkov.

Pokračovali sme v priebežnej distribúcii technických prostriedkov použiteľných na bezpečnú výmenu informácií medzi vládnymi inštitúciami v režime stupňa utajenia Vyhradené, Dôverné a Tajné. Pri zabezpečení vládneho spojenia boli tieto technické prostriedky dodané registrom vládnych inštitúcií.

Počas pandemickej situácie zabezpečoval úrad prostredníctvom utajovaného vládneho spojenia videokonferencie a prenos informácií pre najvyšších vládnych činiteľov na zabezpečenie plynulého chodu vlády Slovenskej republiky.

V roku 2021 pokračovala všetka komunikácia medzi jednotlivými rezortnými šifrovými orgánmi a ústredným šifrovým orgánom elektronicky. Predmetom komunikácie 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.

Vzhľadom na situáciu sa nemohli konať ani záväzne plánovať hromadné stretnutia rezortných šifrových orgánov.

ŠIFROVÉ A TECHNICKÉ PROSTRIEDKY

Za rok 2021 úrad vydal **7 certifikátov prostriedkov šifrovej ochrany informácií a 1 dodatok k už vydanému certifikátu.**

Stupeň utajenia	Vyhradené	Dôverné	Tajné	Prísne tajné	Spolu
TP	3	0	4	0	**7**

6. DÔVERYHODNÉ SLUŽBY

DÔVERYHODNÉ SLUŽBY

Európska komisia vlani zverejnila návrh nariadenia Európskeho parlamentu a Rady, ktorým sa mení a dopĺňa nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu (nariadenie eIDAS).

Pred zverejnením návrhu jeho revízie, organizovala EK bilaterálne stretnutia s členskými krajinami, kde úrad zastupoval Slovenskú republiku. Prednesené návrhy príslušníkmi úradu prispeli k spresneniu návrhu revízie nariadenia eIDAS.

Komisia od zverejnenia návrhu organizuje pravidelné stretnutia na úrovni expertnej skupiny, ktorú zastrešuje úrad v oblasti prípravy technických postupov a legislatívne stretnutia prebiehajúce v réžii aktuálnych predsedníckych krajín, pričom v roku 2021 prebehlo len prvé čítanie návrhu revízie nariadenia eIDAS.

V súlade s nariadením eIDAS, zákonom o dôveryhodných službách a schémou dohľadu vykonáva úrad dohľad nad kvalifikovanými poskytovateľmi dôveryhodných služieb. Nad nekvalifikovanými poskytovateľmi dôveryhodných služieb sa vykonáva ex post dohľad, a to iba v prípade, ak úrad získa informácie nasvedčujúce tomu, že poskytujú služby, ktoré nespĺňajú požiadavky stanovené nariadením.

Úrad na úrovni expertnej skupiny pripravuje podklady a aktívne sa zúčastňuje na prácach, ktoré zadefinujú postupy aj podľa článku 45d – 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 cez určených sprostredkovateľov uznaných na vnútroštátnej úrovni v súlade s vnútroštátnym právom alebo právom Únie a v prípadoch, keď sa tieto atribúty opierajú o autentické zdroje vo verejnom sektore.

CERTIFIKÁCIA

V roku 2021 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 zverejňuje na svojom webovom sídle dôveryhodný zoznam obsahujúci informácie o poskytovateľoch kvalifikovaných dôveryhodných služieb, ktorí sú pod dohľadom Slovenskej republiky a informácie o poskytovaných kvalifikovaných dôveryhodných službách.

Dôveryhodný zoznam má konštitutívny charakter pre validáciu kvalifikovaných podpisov, pečatí, časových pečiatok a stavu kvalifikovaných služieb, čím úrad vedie nevyhnutnú dôveryhodnú infraštruktúru pre zabezpečenie funkčnosti národných a EÚ systémov.

V priebehu roka 2021 úrad **publikoval dôveryhodné zoznamy č. 72 až 84.**

ZOZNAM OPRÁVNENÍ

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

V roku 2021 bolo na základe žiadostí štátnych orgánov a orgánov územnej samosprávy do zoznamu zapísaných 10 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 troch kvalifikovaných poskytovateľov o zámere poskytovať kvalifikovanú dôveryhodnú službu. Poskytovatelia mali povinnosť predložiť oznámenia so záverečnou správou o posúdení zhody.

Úrad posúdil a vyhovel trom žiadostiam kvalifikovaných poskytovateľov dôveryhodných služieb, ktorým bolo celkovo udelených **štrnásť kvalifikovaných štatútov** na kvalifikovanú dôveryhodnú službu.

Kvalifikovaní poskytovatelia dôveryhodných služieb predložili orgánu dohľadu päť správ 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.

TVORBA MEDZINÁRODNÝCH NORIEM

Pri tvorbe medzinárodných technických noriem použiteľných pre implementáciu nariadenia eIDAS bol príslušník úradu projektovým vedúcim pre ISO 14533-1 v rámci ISO TC 154. Práce na revízii ISO 14533-1 budú pokračovať aj v roku 2022.

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.

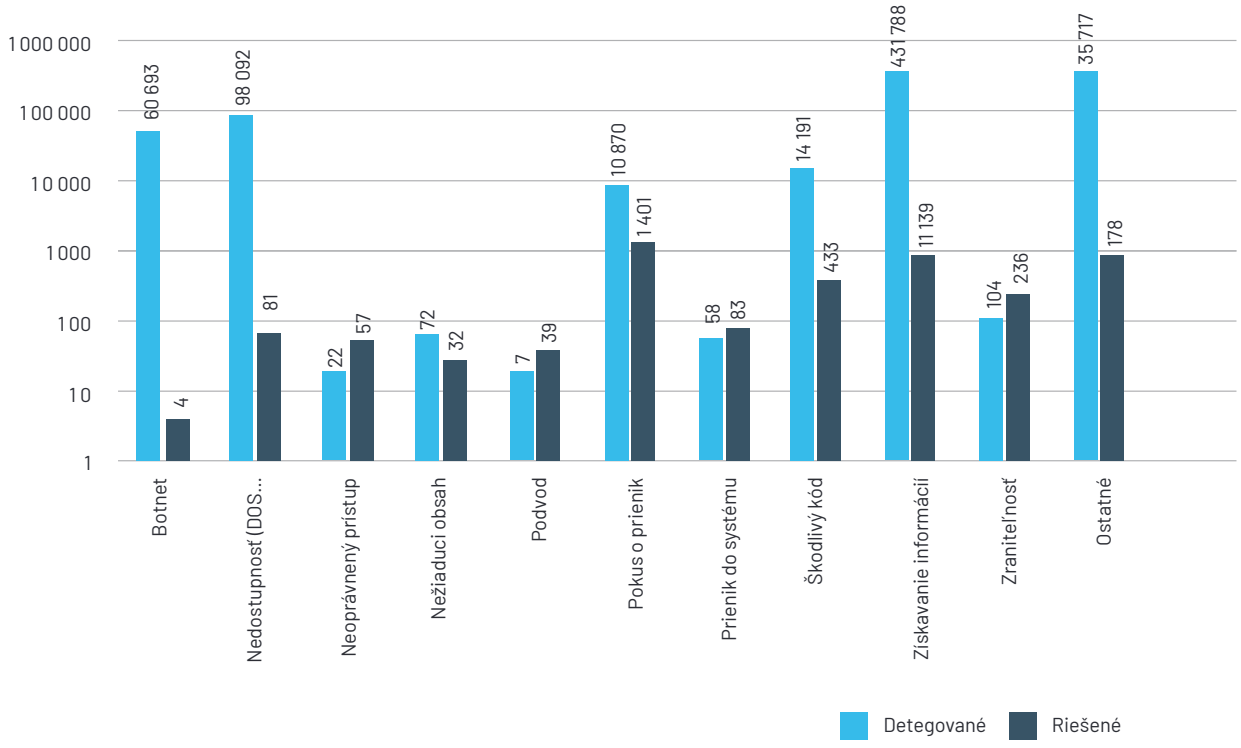
7. KYBERNETICKÁ BEZPEČNOSŤ

KYBERNETICKÁ BEZPEČNOSŤ

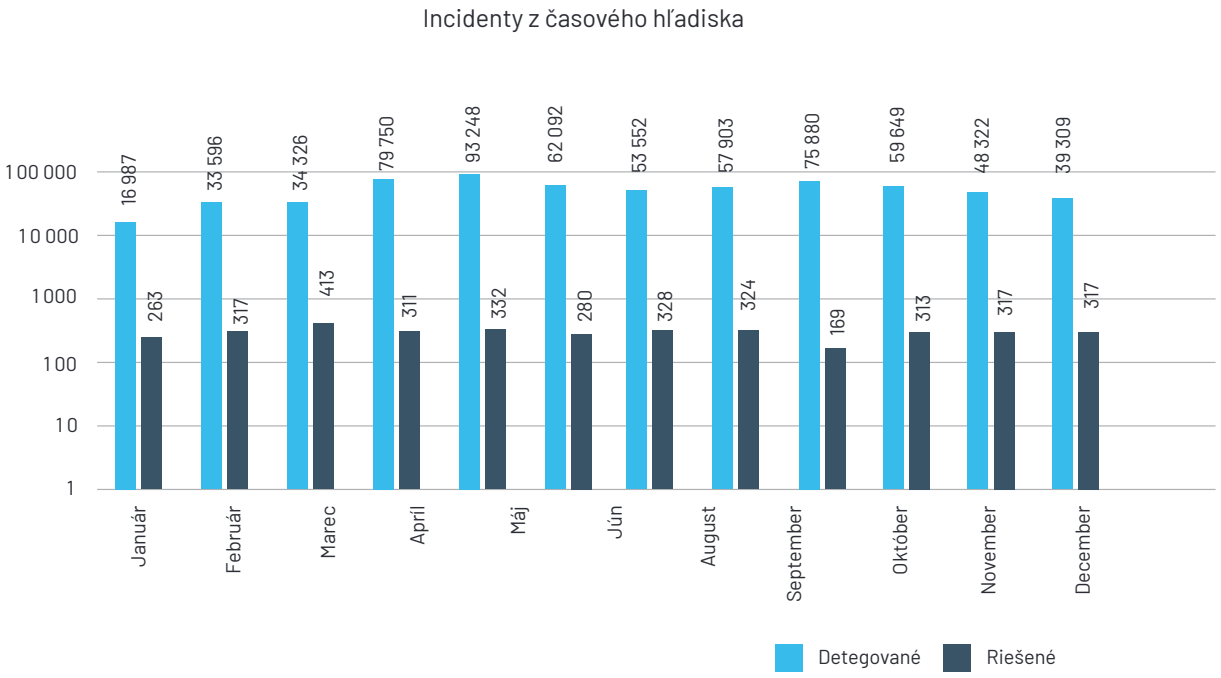
Národné centrum kybernetickej bezpečnosti SK-CERT monitorovalo slovenský kybernetický priestor; agregovalo, analyzovalo a vyhodnocovalo kyberneticky relevantné informácie a prijímalo hlásenia o kybernetických bezpečnostných incidentoch.

Zistené dáta pochádzajú z vlastnej detekcie, povinných hlásení od prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb, dobrovoľných hlásení od firiem, súkromných osôb a ďalších partnerov. Tvoria pohľad na objem incidentov.

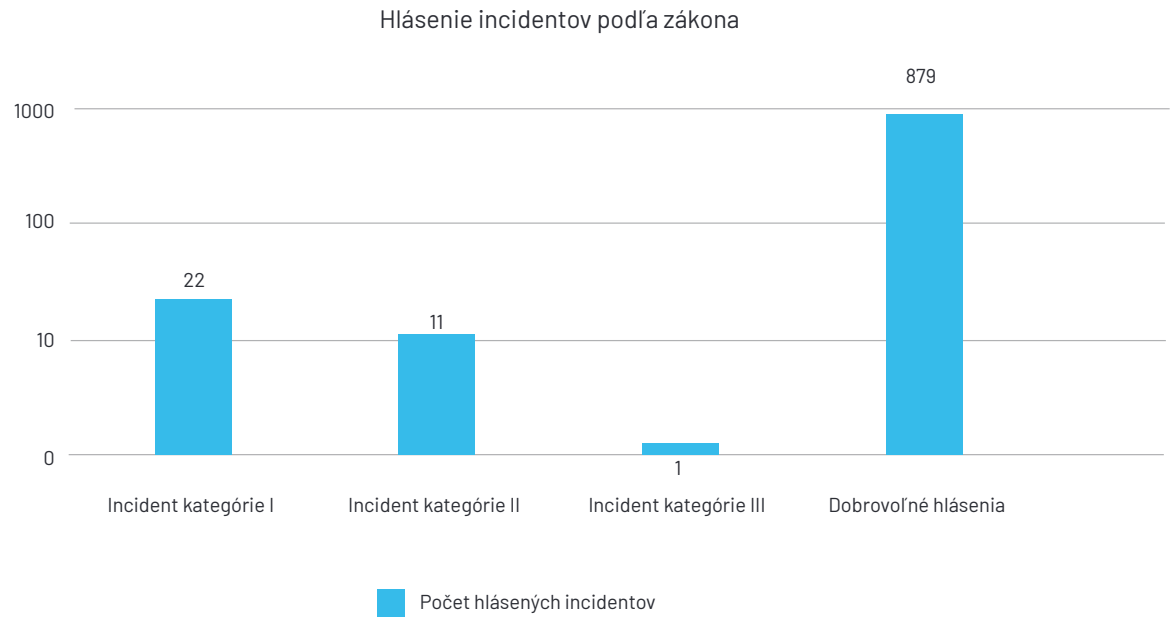
Počet detegovaných a riešených incidentov podľa typu – rok 2021



V kategórii Nežiaduci obsah sú odfiltrované potenciálne incidenty, resp. bezpečnostné udalosti, ktoré boli detegované na základe signatúr na bezpečnostných prvkoch a automaticky vyriešené. Zaevidovali sme celkovo 41 430 926 – najviac incidentov bolo detegovaných a hlásených v máji; najviac riešených v marci.



Zákonnou povinnosťou prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb je hlásenie každého závažného kybernetického bezpečnostného incidentu Národnému bezpečnostnému úradu. Zaznamenali sme nárast hlásených incidentov najmä v oblasti dobrovoľných hlásení, čo hodnotíme kladne.



Útočníci sa zameriavali na viacero typov aktivít – najmä na krádež osobných údajov a vydieranie. Motiváciou útočníkov bolo získať čo najviac informácií od obete, pričom hlavným účelom bolo ich následné speňaženie (monetizácia). v prípade vydierania sa zameriavali na priame získavanie financií – žiadali platbu, najčastejšie v kryptomene, za nezverejnenie toho, čo od obete získali pri útoku.

Najčastejšie boli na útoky využívané phishingové kampane, cez ktoré útočníci zbierali osobné a iné citlivé údaje, šírili ransomvér alebo iný škodlivý kód. Hlavným cieľom útočníkov bolo zneprístupniť alebo znefunkčniť systémy kritické pre poskytovanie služieb v rôznych sektoroch (napríklad priemysel, tepelná energetika, elektroenergetika a verejná správa) a žiadať výkupné za ich znovusprístupnenie, resp. rozšifrovanie zašifrovaných údajov, ale ako nový trend útočníci kradli údaje obetí pred zašifrovaním za účelom ďalšieho speňaženia.

Rok 2021 možno charakterizovať ako príznačný pre výskyt veľkých, závažných zraniteľností v bežne používaných produktoch a službách. Národné centrum kybernetickej bezpečnosti SK-CERT pozoruje kontinuálny nárast závažných zraniteľností, ktorý je spôsobený najmä tlakom na rýchly vývoj produktov a služieb, a teda nedostatočným dôrazom na bezpečnosť pri vývoji, zanedbaným testovaním výsledného produktu alebo služby pred uvedením na trh a následne aj zlom udržiavaní produktov a služieb výrobcami aj užívateľmi.

Výskyt zraniteľnosti neznamená nevyhnutne problém, ten nastáva až pri zneužití takejto zraniteľnosti. Takéto zneužívanie však rastie nielen celosvetovo, ale aj na Slovensku. Trendom roka 2021 bol nárast tzv. supply chain útokov, spočívajúcich v napadnutí dodávateľa, ktorý následne (nevedomky) slúži ako prostredník medzi útočníkom a obeťou.

Útočník môže využiť viacero možností, ako supply chain útok vykonať, napríklad implementáciou zraniteľnosti do produktu alebo služby dodávateľa, ktorý si obeť kúpi, resp. jeho používanie platí.

NBÚ vykonával tiež aktivity spojené s ochranou prevádzkovateľov základných služieb vrátane prvkov kritickej infraštruktúry. Medzi takéto aktivity patrili najmä koordinácia riešenia kybernetických bezpečnostných incidentov, konzultácie v oblasti kybernetickej bezpečnosti a vydávanie varovaní a odporúčaní na zraniteľnosti a hrozby.

Národné centrum kybernetickej bezpečnosti SK-CERT vydalo celkovo **53 súhrnných bezpečnostných bulletinov a 295 bezpečnostných varovaní na 711 konkrétnych zraniteľností v produktoch a službách.**

Vláda Slovenskej republiky schválila v januári **Národnú stratégiu kybernetickej bezpečnosti na roky 2021 až 2025.** Ide o východiskový strategický dokument v oblasti kybernetickej bezpečnosti, ktorý stanovuje smerovanie krajiny v tejto oblasti na ďalšie obdobie.

Stratégia určuje základné princípy systému riadenia kybernetickej bezpečnosti. Rešpektuje pritom základné práva a slobody v kybernetickom priestore, zákonnosť a mechanizmy bezpečnostného systému, komplexnosť prístupu k problematike kybernetickej bezpečnosti, ale aj riadenie národnej kybernetickej bezpečnosti cez riadenie rizík.

Stratégia identifikovala najzávažnejšie hrozby, ktoré sú spôsobilé narušiť systém riadenia kybernetickej bezpečnosti na národnej úrovni, ohroziť fungovanie štátu a jeho občanov.

V stratégii je definovaných 7 strategických cieľov (prioritných oblastí):

- dôveryhodný štát pripravený na hrozby
- efektívne odhaľovanie a objasňovanie počítačovej kriminality
- odolný súkromný sektor
- kybernetická bezpečnosť ako základná súčasť verejnej správy
- silné partnerstvá
- vzdelaní odborníci a verejnosť
- výskum a vývoj v oblasti kybernetickej bezpečnosti

Definuje aj hlavných zahraničnopolitických partnerov, spôsob implementácie stratégie a spôsob jej financovania.

V júli prijala vláda plán, ako bude stratégiu aplikovať v praxi – **Akčný plán realizácie Národnej stratégie kybernetickej bezpečnosti na roky 2021 až 2025.**

Akčný plán **obsahuje 155 úloh**, rozdelených podľa prioritných oblastí. Celkovo je do akčného plánu zainteresovaných 20 subjektov, ktoré sú zodpovedné za jednotlivé úlohy.

Národný bezpečnostný úrad zriadil stály monitorovací výbor, ktorý bude monitorovať a vyhodnocovať implementáciu a realizáciu úloh. Sú v ňom zastúpené všetky zainteresované subjekty. Monitorovací výbor sa prvý raz stretol v decembri 2021. Pravidelné stretnutia budú pokračovať až do roku 2025.

Príslušníci a zamestnanci Národného centra kybernetickej bezpečnosti SK-CERT sa aktívne podieľali na národných aj medzinárodných aktivitách a posilňovali postavenie SK-CERT aj Národného bezpečnostného úradu ako rešpektovaného a hodnotného člena bezpečnostnej komunity.

Počas roka sa zúčastňovali na konferenciách, workshopoch, pracovných skupinách a iných formátoch. Prezentovali stav kybernetickej bezpečnosti, prístupy k ochrane informačných aktív, legislatívne prostredie a iné súvisiace témy. v pracovných skupinách v Európskej komisii, NATO a OBSE presadzovali záujmy Slovenska v oblasti kybernetickej bezpečnosti a podieľali sa na tvorbe strategických a legislatívnych dokumentov.

Národné centrum kybernetickej bezpečnosti SK-CERT v roku 2021 sprístupnil nový vlastný nástroj na agregáciu a analýzu informácií z otvorených zdrojov – TaranisNG. Ide o tzv. open-source softvér, ktorý si môže stiahnuť a používať ktokoľvek úplne zadarmo.

Je určený najmä pre bezpečnostné tímy, bezpečnostných výskumníkov a analytikov, pričom má dnes viac ako 280 stiahnutí a používaný je v 4 štátoch EÚ a v jednom štáte mimo Únie. Spustili sme aj pilotnú prevádzku Jednotného informačného systému kybernetickej bezpečnosti.

NBÚ ako hlavný kontaktný bod na medzinárodnej úrovni spolupracoval so svojimi zahraničnými partnermi a partnerskými organizáciami, najmä prostredníctvom platformy NIS Cooperation Group, CSIRT Network, CyCLONe a organizácií Trusted Introducer a FIRST. Spolupráca spočívala v zdieľaní skúseností, výmene operatívnych informácií pri riešení kybernetických bezpečnostných incidentov a najlepšej praxe pri ochrane informačných aktív. Najdôležitejšími aktivitami bola výmena informácií a koordinácia pri závažných incidentoch s medzinárodným presahom. Zástupca úradu aktívne pôsobil v ENISA Management Board a ENISA Executive Board. NBÚ zastupuje Slovenskú republiku v oblasti kybernetickej bezpečnosti aj v OBSE.

Na národnej úrovni pokračovali procesy zdieľania a výmeny relevantných informácií, ale aj riešenia strategických a koncepčných otázok. Relevantné subjekty (NBÚ, SIS, VS, NASES, PZ, MIRRI) na pravidelnej báze komunikovali a zdieľali informácie pre zabezpečenie národného kybernetického priestoru a spolupodieľali sa na riešení operatívnych, ale aj strategických problémov.

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

V roku 2021 sme naďalej poskytovali metodickú pomoc, konzultácie a usmernenia pri implementácii zákonných požiadaviek, a to najmä prevádzkovateľom základných služieb a poskytovateľom digitálnych služieb, ako aj ústredným orgánom podľa zákona.

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 bezpeč-

nosti, 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 20000-1:2018, riadenia kontinuity činností podľa ISO 22301:2019 a riadenia kvality podľa ISO 9001:2015.

Pre všetky uvedené systémy manažérstva, ako aj pre posudzovanie odbornej spôsobilosti audítorov a manažérov kybernetickej bezpečnosti má KCCKB k dnešnému dňu udelené akreditačné rozhodnutia od Slovenskej národnej akreditačnej služby. Ako jediný orgán posudzovania zhody na Slovensku tak KCCKB 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 a to 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 k dnešnému dňu poodpísané memorandá o spoluopráci s absolútnou väčšinou relevantných vysokoškolských pracovísk, ktoré poskytujú študijné programy a odbory v oblasti ochrany informačných aktív – napríklad s Technickou univerzitou v Košiciach, Fakultou informatiky a informačných technológií Slovenskej technickej univerzity v Bratislave, s Fakultou bezpečnostného inžinierstva Žilinskej univerzity, s Univerzitou Pavla Jozefa Šafárika v Košiciach, s Fakultou managementu Univerzity Komenského v Bratislave a s Akadémiou policajného zboru.

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

8. MEDZINÁRODNÁ SPOLUPRÁCA

MEDZINÁRODNÁ SPOLUPRÁCA

EURÓPSKA ÚNIA

Smerovanie úradu v budovaní bezpečnostného prostredia korešponduje s princípmi prijatej Stratégie EÚ pre bezpečnostnú úniu na obdobie 2020 až 2025. Prioritami sú najmä zvyšovanie odolnosti kritickej infraštruktúry, kybernetickej bezpečnosti a v nastavení procesov na zaistenie bezpečnosti vo fyzickom aj digitálnom prostredí.

Pandémia mala značný vplyv na osobné pracovné stretnutia v jednotlivých pracovných platformách. Veľa rokovaní bolo opäť vo virtuálnom priestore. Úrad má expertné zastúpenie vo všetkých troch platformách orgánov a inštitúcií EÚ zaoberajúcich sa politikou bezpečnosti a ochrany utajovaných informácií EÚ (EUCI).

> V prostredí Rady EÚ sa úrad naďalej aktívne zúčastňoval na zasadnutiach Bezpečnostného výboru Rady EÚ (CSC) ako poradného orgánu Generálneho sekretariátu Rady EÚ pri príprave politík bezpečnosti a ochrany utajovaných skutočností EÚ.

Diskusie boli venované najmä revízii Bezpečnostných predpisov Rady na ochranu utajovaných skutočností EÚ (CSR). Úrad ďalej participoval aj v dvoch podvýboroch Rady (Výbor pre informačnú bezpečnosť a Výbor pre bezpečnostnú akreditáciu).

> V roku 2021 sme aktívne participovali na tvorbe nových pravidiel fyzickej a objektovej bezpečnosti. V uplynulom roku sa začali diskusie o zmenách pri výmene utajovaných skutočností EÚ s tretími krajinami a medzinárodnými organizáciami, ale aj o návrhu dohody medzi Európskym parlamentom, Radou EÚ a vysokým predstaviteľom EÚ pre zahraničné veci a bezpečnostnú politiku o prístupe EP k utajovaným skutočnostiam z oblasti spoločnej a zahraničnej bezpečnostnej politiky.

> Na pôde Európskej komisie bol úrad zastúpený v Skupine expertov Európskej komisie pre bezpečnostnú politiku (ComSEG), ktorá zodpovedá za prípravu a výkon bezpečnostných politík a pravidiel v jej podriadených inštitúciách. Úrad sa zapojil okrem Bezpečnostného výboru pre Vesmírne programy EÚ (EUSPA SPC-SC), pod ktorý spadajú programy ako Galileo, Copernicus a GOVSATCOM aj do Bezpečnostného akreditačného panela EUSPA.

> V Európskej službe pre vonkajšiu činnosť (EEAS) sa úrad zúčastňoval na zasadnutiach v Bezpečnostnom výbore EEAS (SC EEAS) pre prípravu politík a návrhov (bezpečnosti vo všeobecnosti) v oblasti ochrany EUCI v podmienkach EEAS a jej zahraničných delegáciách, ale aj na aktualizácii medzinárodných zmlúv v oblasti EUCI. Pandémia spôsobila, že fyzické zasadnutie výboru bolo až v novembri 2021.

> V celkovom pohľade reflektovala agenda ochrany EUCI v roku 2021 na pandemickú situáciu, čo vyústilo v Rade EÚ, EK a EEAS do otvorenia otázok technického riešenia pre bezpečnú hlasovú komunikáciu EUCI, či už počas zasadnutí Rady EÚ cez videokonferencie, pri výmene EUCI v Komisii a jej podriadených subjektoch, alebo v EEAS a jej zahraničných delegáciách.

> Európska komisia predstavila koncom roka 2020 legislatívny návrh Nariadenia o informačnej bezpečnosti v inštitúciách, orgánoch a agentúrach EÚ, ktoré by zjednotilo bezpečnostné pravidlá na ochranu EUCI. Členské štáty vyzývali úrady EÚ na tento krok niekoľko rokov. Pri schvaľovaní sú naši experti pripravení na odbornú diskusiu.

V oblasti kybernetickej bezpečnosti rezonovali viaceré témy. Úrad úspešne reprezentoval Slovensko v platformách Blue OLEx 2021 (tabletop cvičenie a strategická politická diskusia ku kybernetickej bezpečnosti) a CyCLONe (nástroj k implementácii „Blueprint" Európskej komisie pre rýchlu reakciu na núdzové situácie v prípade rozsiahleho cezhraničného kybernetického in-

cidentu alebo krízy) s cieľom budovať pevnejší vzťah v komunite kybernetickej bezpečnosti.

> Európske centrum odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti a sieť národných koordinačných centier bolo zriadené na obdobie od 28. júna 2021 do 31. decembra 2029 nadobudnutím účinnosti nariadenia práve o Európskom kompetenčnom centre.

Zástupcovia vlád členských štátov vybrali za sídlo inštitúcie Bukurešť. Členské štáty a EK vyvíjali úsilie o personálne a administratívne zabezpečenie Európskeho kompetenčného centra. V priebehu roka boli designovaní zástupcovia jednotlivých členských štátov a Komisie za riadnych členov správnej rady, kde má tak svoje zastúpenie aj úrad v podobe svojho nominanta a jeho alternáta.

Dohodu dosiahli aj vo viacročnom finančnom rámci na roky 2021 – 2027, najmä v programoch Horizon Europe a Digital Europe. Implementovať ich bude práve európske kompetenčné centrum.

Slovensko bude musieť určiť vnútroštátnu inštitúciu „národného koordinačného centra" a jeho zapojenie do siete národných koordinačných centier. Najväčšie predpoklady v tomto smere má Kompetenčné a certifikačné centrum kybernetickej bezpečnosti (KCCKB.

> V nelegislatívnej oblasti priniesol rok 2021 pokračujúcu úspešnú implementáciu opatrení 5G toolbox (súbor opatrení určených na riešenie rizík v oblasti kybernetickej bezpečnosti 5G sietí). Rada prijala závery, v ktorých vyzvala EÚ a členské štáty, aby ďalej rozvíjali rámec EÚ pre krízové riadenie kybernetickej bezpečnosti, a to aj preskúmaním potenciálu spoločnej kybernetickej jednotky. Rada vo svojich záveroch zdôrazňuje potrebu konsolidovať existujúce siete a zmapovať možné medzery a potreby v oblasti výmeny informácií medzi kybernetickými komunitami.

> V roku 2021 boli naďalej aplikované reštriktívne opatrenia v oblasti kybernetickej bezpečnosti. Tento rámec umožňuje EÚ ukladať cielené reštriktívne opatrenia voči osobám alebo subjektom zapojeným do kybernetických útokov, ktoré majú významný vplyv a predstavujú vonkajšiu hrozbu pre EÚ alebo jej členské štáty.

Rada EÚ schválila prvý sankčný zoznam a druhý sankčný zoznam proti kybernetickým útokom ohrozujúcim EÚ a jej členské štáty. Do zoznamov bolo zaradených osem fyzických osôb a štyri právnické osoby (subjekty), ktoré boli zodpovedné za kybernetické útoky alebo pokusy o kybernetické útoky (najmä pokus o kybernetický útok na OPCW, kybernetické útoky WannaCry a NotPetya; Operation Cloud Hopper a kybernetický útok so závažným vplyvom na nemecký spolkový snem

> Komisia a vysoký predstaviteľ Únie pre zahraničné veci a bezpečnostnú politiku predložili v decembri tzv. nový balík kybernetickej bezpečnosti. Tvoria ho najmä nová stratégia kybernetickej bezpečnosti EÚ – kľúčový prvok formovania digitálnej budúcnosti Európy, Plán obnovy pre Európu a Stratégie EÚ pre bezpečnostnú úniu.

Hlavným cieľom je posilniť kolektívnu odolnosť Európy proti kybernetickým hrozbám a zabezpečiť, aby mohli všetci občania a podniky plne využívať dôveryhodné a spoľahlivé služby a digitálne nástroje.

> EK predložila aj návrhy na riešenie kybernetickej aj fyzickej odolnosti kritických subjektov a sietí: smernicu o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (revidovaná smernica NIS 2) a novú smernicu o odolnosti kritických subjektov.

Nová legislatíva na úrovni EÚ sa týka širokej škály odvetví a je zameraná na riešenie súčasných a budúcich online a offline rizík; od kybernetických útokov po trestnú činnosť alebo prírodné katastrofy. Úrad vo všetkých pracovných platforiem presadzoval zachovanie právnej formy revidovanej smernice NIS 2 a úspešne naplnil tento cieľ.

> Národný bezpečnostný úrad aktívne pôsobil v Európskej organizácii pre kybernetickú bezpečnosť (ECSO). V organizačnej štruktúre je členom Výboru zástupcov národných verejných autorít (NAPAC) a pozorovateľom v predstavenstve.

Naši príslušníci pôsobiil v pracovných formátoch Komisie (Skupina pre spoluprácu – NIS a Pracovná skupina pre hodnotenie národných stratégii) a Rady EÚ HWPCI. Ich hlavnou úlohou je zabezpečovať a zintenzívňovať vzájomnú strategickú a analytickú spoluprácu a zdieľať informácie medzi orgánmi zodpovednými za kybernetickú bezpečnosť členských štátov a ich jednotkami.

Medzi kľúčové priority Skupiny pre spoluprácu 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 2021 k tejto úlohe pribudli aj ďalšie dôležité témy ako „Spoločná kybernetická jednotka", ENISA prezentovala 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 ransomvér).

Počas roka vznikla 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. Členstvo prináša radu výhod – najmä však zdieľanie expertízy, praxe a skúseností. NBÚ prejavil záujem o členstvo a neskôr ho aj získal.

NATO

Rokovania Bezpečnostného výboru NATO (SC) boli tiež poznamenané pandemickou situáciou. Po dlhom čase zasadol v októbri 2021 vo všetkých svojich formátoch – vo formáte bezpečnostných politík, bezpečnosti komunikačných a informačných systémov a na najvyššej úrovni – riaditeľov bezpečnostných úradov členských štátov.

> Rok 2021 bol z pohľadu ochrany utajovaných skutočností NATO v znamení pokračovania v rozsiahlej revízii bezpečnostných pravidiel NATO. Po revízii jej základného dokumentu Bezpečnosti v Organizácie Severoatlantickej zmluvy C-M(2002)49-REV1 a jeho príslušných smerníc, boli revidované aj podporné dokumenty o bezpečnostných opatreniach pre utajované zasadnutie NATO uskutočnené v zariadeniach nezriadených na tieto účely a o bezpečnostnom vzdelávaní a povedomí.

> Pod vedením Bezpečnostného úradu NATO (NOS) sa v roku 2021 vytvorila expertná skupina špecialistov z členských štátov na oblasť priemyselnej bezpečnosti a počas spomínaného zasadnutia predostreli NOS a delegátom svoje návrhy na zmenu Smernice o utajovaných projektoch a priemyselnej bezpečnosti.

> V roku 2021 takisto vznikla expertná skupina pre tvorbu základných prvkov novej oblasti ochrany utajovaných skutočností – bezpečnosť výstavby (construction security). Rokovanie bezpečnostné výboru na najvyššej úrovni prvý raz viedol nový riaditeľ NOS Paul Avallone, ktorý predstavil najväčšie priority NOS (doriešenie situácie v Afganistane – prenos utajovaných skutočností, posilnenie a budovanie kontrarozviednych programov, častejšie zasadnutia SC na najvyššej úrovni).

> NATO aj v roku 2021 čelilo viacerým kybernetickým hrozbám, čo viedlo k zmene niektorých politík kybernetickej obrany, rovnako ako aj k inštitucionálnym zmenám vnútri NATO. Výbor kybernetickej obrany (CDC) vypracoval program kybernetickej adaptácie NATO pre najbližšie roky. Taktiež spracoval novú spoločnú politiku kybernetickej obrany NATO.

Jej upravená verzia bola poskytnutá aj partnerom NATO, pretože jedným z hlavných poslaní komuniké generálneho tajomníka NATO z bruselského summitu bola spolupráca s partnermi pre lepšie zabezpečenie

odolnosti aliancie. Ostatné aktivity CDC boli v stupni utajenia NATO RESTRICTED a vyššie.

> Spoločné aliančné cvičenie NATO Abble Staff 2020 bolo pre pandémiu zrušené tesne pred jeho novembrovým začiatkom a uskutočnilo sa na prelome februára a marca 2021. Cvičenie NATO Abble Staff 2021 bolo v novembri 2021.

> Úrad pôsobí aj v nadnárodnej pracovnej skupine MISWG (Multinational Industrial Security Working Group) s cieľom adaptovať bezpečnostné postupy v neustále sa vyvíjajúcom bezpečnostnom prostredí a zohľadňovať meniace sa trendy v obrannom priemysle a v oblasti medzinárodnej priemyselnej bezpečnosti. Tvoria ju členské štáty NATO (okrem Islandu), ale aj viacero nečlenov (Rakúsko, Fínsko, Švédsko, Švajčiarsko, Izrael, Nový Zéland, Austrália a Severné Macedónsko).

Skupina vytvára spoločné opatrenia a postupy pri ochrane utajovaných skutočností týkajúcich sa medzinárodných obranných programov a záležitostí priemyselnej bezpečnosti v medzinárodnom kontexte. Plenárne zasadnutie skupiny je raz ročne v niektorom z členských štátov. Pre pandémiu bolo vlani iba online formou.

REGIONÁLNA SPOLUPRÁCA

Národný bezpečnostný úrad dlhodobo považuje regionálnu spoluprácu za dôležitú prioritu. V roku 2021 preto pokračoval v rozvoji osvedčených a fungujúcich vzťahov so strategickými partnermi z krajín Vyšehradskej štvorky a Rakúska.

Efekt spolupráce v stredoeurópskom regióne sa potvrdil najmä v neformálnej Stredoeurópskej platforme pre kybernetickú bezpečnosť CECSP (Central Europen Cyber Security Pla orm). Opäť sa v nej darilo nachádzať spoločné a zjednocujúce názory na aktuálne európske témy.

Spolupráca prebiehala ad hoc, virtuálne a cez elektronickú poštu. Platforme predsedalo vlani Poľsko a počas dvoch online stretnutí (máj a december 2021) sa zástupcovia jednotlivých štátov okrem nadväzovania spolupráce zamerali aj na výmenu skúsenosti v oblasti kybernetickej bezpečnosti v súvislosti s prebiehajúcou pandémiou ochorenia COVID-19.

BILATERÁLNE PARTNERSTVÁ

Úrad pokračoval v rozvíjaní bilaterálnej spolupráce so svojimi partnermi vo všetkých svojich oblastiach pôsobnosti – najmä pri výmene a ochrane utajovaných skutočností, uznávaní bezpečnostných previerok vydaných v zahraničí a podobne.

Úrad ako gestorský orgán oslovuje svojich partnerov v zahraničí a pripravuje návrhy textov dohôd, ktoré schvaľuje vláda Slovenskej republiky.

Príslušníci úradu rozvíjali bilaterálne vzťahy na dennej báze naprieč všetkými pracovnými platformami – či už pri kontakte počas zasadnutia pracovných skupín, alebo pri ad hoc plnení úloh práve na bilaterálnej úrovni.

V roku 2021 sa zintenzívnila spolupráca úradu so Spojenými štátmi americkými najmä pre nevyhnutnosť uzavretia novej bezpečnostnej zmluvy medzi vládami oboch krajín o vzájomnej ochrane utajovaných skutočností.

Aktuálne platná bezpečnostná dohoda je z roku 1995. Slovenský bezpečnostný systém odvtedy zaznamenal rozsiahle inštitucionálne aj legislatívne.

Americká strana v júli 2021 vykonala na Slovensku bezpečnostnú hodnotiacu návštevu, ktorá bola jednou z podmienok podpisu novej bezpečnostnej zmluvy. Fyzickej návšteve predchádzala virtuálna – počas niekoľkých dní bol americký partner informovaný o slovenskej legislatíve v oblasti ochrany utajovaných skutočností a jej implementovaní v podmienkach úradu, ministerstva obrany, ministerstva hospodárstva a ministerstva zahraničných vecí.

Niekoľkomesačné úsilie všetkých zainteresovaných strán aj priebeh návštevy boli americkou stranou vyhodnotené veľmi pozitívne. USA skonštatovali, že úroveň ochrany utajovaných skutočnosti v Slovenskej republike je na veľmi vysokej úrovni a podpisu predmetnej zmluvy v roku 2022 už preto nič nebráni.

V oblasti bilaterálnych medzinárodných zmlúv uzatvoril úrad zmluvy s Maltskou republikou a Spojenými arabskými emirátmi.

Nadchádzajúcou zmluvou, ktorá je v štádiu negociácií, je bilaterálna zmluva o ochrane a výmene utajovaných skutočností s Európskou vesmírnou agentúrou (ESA). Uzatvorenie zmluvy s ESA je jedným z prvotných krokov Slovenskej republiky, ktoré môžu v budúcnosti dopomôcť k získaniu plnohodnotného členstva v tejto organizácii

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.

Úrad jednotlivým registrom utajovaných skutočností, zriadenými orgánmi verejnej moci, naďalej poskytoval metodickú pomoc pri elektronickej evidencii utajovaných skutočností.

Pracovisko centrálneho registra spracovalo **3680 utajovaných skutočností NATO a 1525 utajovaných skutočností EÚ**. Úrad sprostredkoval aj **výmenu 103 utajovaných skutočností cudzej moci**.

Na úrade od roku 2010 pôsobí vytvorený register utajovaných skutočností NATO ATOMAL. V minulom roku v ňom neboli zaevidované žiadne ATOMAL utajované písomnosti.

Stupeň utajenia	2020	2021
NATO Restricted	1754	1739
EU Restricted	802	693
Cudzia moc Vyhradené	83	48
NATO Confidential	1089	732
EU Confidential	364	486
Cudzia moc Dôverné	66	49
NATO Secret	1379	1209
EU Secret	186	346
Cudzia moc Tajné	2	3
NATO Top Secret	0	0
EU Top Secret	1	0
Cudzia moc Prísne tajné	1	3
NATO spolu	**4222**	**3680**
EU spolu	**1353**	**1525**
Cudzia moc spolu	**152**	**103**

S účinnosťou zákona č. 364/2020, ktorým sa mení a dopĺňa zákon č. 395/2002 o archívoch a registratúrach zriadil NBÚ centrálne úložisko utajovaných skutočností pre dočasné uloženie utajovaných skutočností, ktoré majú trvalú dokumentárnu hodnotu.

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

9. HOSPODÁRENIE

HOSPODÁRENIE

Rozpis záväzných ukazovateľov rozpočtu kapitoly 41 – Národný bezpečnostný úrad na rok 2021: vplyv rozpočtových opatrení na výšku upraveného rozpočtu, skutočné čerpanie rozpočtových prostriedkov k 31. decembru 2021 a percentuálne vyhodnotenie plnenia k upravenému rozpočtu.

Ukazovatele	Schválený rozpočet	Upravený rozpočet	Skutočnosť k 31.12.2021	Plnenie k upr. rozpočtu
I. Príjmy kapitoly	22 000,00	22 000,00	20 772,66	94,42 %
A. Záväzný ukazovateľ	20 000,00	20 000,00	20 539,00	102,70 %
B. Prostriedky Európskej únie	0,00	0,00	0,00	-
II. Výdavky kapitoly celkom (A + B+ C)	**12 730 671,00**	**13 108 044,30**	**12 636 045,06**	**96,40 %**
A. Výdavky spolu bez prostriedkov podľa § 17 ods. 4 zákona č. 523/2004 Z. z. a prostriedkov Európskej únie	**12 728 671,00**	**12 913 980,29**	**12 443 755,71**	**96,36 %**
z toho:				
A.1. rozpočtové prostriedky kapitoly (kód zdroja 111 + 11H + 131)	12 728 671,00	12 835 372,23	12 365 836,77	96,34 %
z toho: kód zdroja 111	12 728 671,00	12 600 159,60	12 130 828,16	96,28 %
kód zdroja 131	0,00	235 212,63	235 008,61	99,91 %
A.2. prostriedky na spolufinancovanie	0,00	78 608,06	77 918,94	99,12 %
z toho: kód zdroja 1AC3	0,00	13 014,46	13 014,46	100,00 %
kód zdroja 3AA2	0,00	9 470,74	9 470,74	100,00 %
kód zdroja 3AA3	0,00	8 139,97	8 139,97	100,00 %
kód zdroja 3AC2	0,00	24 422,88	23 733,76	97,18 %
kód zdroja 3AC3	0,00	23 560,01	23 560,01	100,00 %
A.3. mzdy, platy, služ. príj. a ost. os. vyrovnania (610), (kód zdroja 111 + 11H) z toho: mzdy, platy, služ. príjmy a ost. os. vyrovnania aparátu ústred. orgánu (kód zdroja 111 + 11H)	6 492 661,00	6 603 791,77	6 311 203,29	95,57 %
	6 492 661,00	6 603 791,77	6 311 203,29	95,57 %
Počet zamestnancov rozpočtových organizácií podľa prílohy č. 1 k uzneseniu vlády SR č. 649/2020	238 osôb	250 osôb	215 osôb*	86,00 %
z toho: aparát ústredného orgánu				
- administratívne kapacity rozp. org. osobitne sledované, podľa prílohy č. 1 k UV SR č. 649/2020	238 osôb	250 osôb	215 osôb*	86,00 %
z toho: aparát ústredného orgánu	0 osôb	0 osôb	0 osôb	-
	0 osôb	0 osôb	0 osôb	-
A.4. kapitálové výdavky (700) (bez prostriedkov na spolufinancovanie)	0,00	253 970,23	253 766,21	99,92 %
z toho: kód zdroja 111	0,00	18 757,60	18 757,60	100,00 %
kód zdroja 131I	0,00	138 626,16	138 626,16	100,00 %
kód zdroja 131J	0,00	35 654,47	36 654,47	100,00 %
kód zdroja 131K	0,00	60 932,00	60 727,98	99,67 %
B. Prostriedky podľa § 17 ods. 4 zákona č. 523/2004 Z. z. (Podľa § 17 ods. 4 zákona č. 523/2004 Z. z. je rozpočtová organizácia oprávnená čerpať tento limit do výšky rozpočtovaných príjmov skutočne prijatých a je oprávnená prekročiť limit výdavkov z dôvodu dosiahnutia vyšších ako rozpočtovaných príjmov.)	**2 000,00**	**2 000,00**	**233,66**	**11,68 %**
C. Prostriedky Európskej únie	**0,00**	**192 064,01**	**192 055,69**	**100,00 %**
z toho: kód zdroja 1AC1	0,00	92 458,46	92 450,14	99,99 %
kód zdroja 3AA1	0,00	53 667,50	53 667,50	100,00 %
kód zdroja 3AC1	0,00	45 938,05	45 938,05	100,00 %
D. Výdavky štátneho rozpočtu na realizáciu programov vlády SR a časti prog. vlády SR	**12 730 671,00**	**13 108 044,30**	**12 636 045,06**	**96,40 %**
	12 487 317,00	12 894 305,30	12 440 148,88	96,48 %
0D9 Bezpečnosť informácií	243 354,00	213 739,00	195 896,18	91,65 %
0EK0U Informačné technológie financované zo štátneho rozpočtu – NBÚ				
E. Systemizácia policajtov v štátnej službe	**216 osôb**	**228 osôb**	**194 osôb***	**85,09 %**
	5 905 472,00	**6 013 703,77**	**5 808 977,06**	**96,60 %**

Záväzné ukazovatele rozpočtu úradu pre rok 2021 boli úradom dodržané. Pri hospodárení s finančnými prostriedkami úrad postupoval podľa zásad hospodárnosti, efektívnosti a účelnosti pri dodržiavaní legislatívnych predpisov.

ROZPOČET NA ROK 2022

Zákonom č. 534/2021 Z. z. o štátnom rozpočte na rok 2022 boli schválené záväzné ukazovatele štátneho rozpočtu jednotlivých kapitol na rok 2022. V nadväznosti na bod C.1. uznesenia vlády SR č. 577 zo dňa 14. októbra 2021 k návrhu rozpočtu verejnej správy na roky 2022 až 2024 a ustanovenie § 6 ods. 3 zákona č. 523/2004 Z. z. o rozpočtových pravidlách verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov boli úradu oznámené záväzné ukazovatele štátneho rozpočtu na rok 2022.

Výdavky úradu pre rok 2022 sú rozpočtované v programe 0D9 – Bezpečnosť informácií a medzirezortného podprogramu 0EK0U – Informačné technológie financované zo štátneho rozpočtu – NBÚ v celkovej sume 12 844 288,00 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 záväzkov voči EÚ a NATO.

10. KONTROLA A AUDIT

KONTROLA A AUDIT

NBÚ pokračoval v dohľadovej (kontrolnej) činnosti štátnych orgánov, podnikateľov a jednej medzinárodnej organizácie.

V oblasti ochrany utajovaných skutočností vykonal kontrolu 13 subjektov, v ktorých boli vykonané kontroly s rôznymi predmetmi kontroly v rôznych kombináciách - ochrana utajovaných skutočností (10-krát), šifrová ochrana informácií (1-krát) a kontrola splnenia opatrení (4-krát).

Štyri kontrolné aktivity boli zamerané na oblasť kybernetickej bezpečnosti a plnenia záväzkov vyplývajúcich z členstva v NATO, jedna na oblasť dôveryhodných služieb.

Deväť kontrol bolo v štátnych orgánoch, sedem v podnikateľských subjektoch a jedna v medzinárodnej organizácii.

Kontrolné skupiny sa zamerali najmä na komplexnosť prijatých ochranných opatrení a ich koordináciu naprieč jednotlivými oblasťami bezpečnosti.

Nedostatky boli zistené v **6 kontrolovaných subjektoch**. Spolu bolo zistených 46 kontrolných zistení:

- 10 v oblasti administratívnej bezpečnosti,
- 21 v oblasti fyzickej bezpečnosti a objektovej bezpečnosti,
- 2 v oblasti technických prostriedkov,
- 4 v oblasti personálnej bezpečnosti,
- 9 v oblasti kybernetickej bezpečnosti.

VNÚTORNÝ AUDIT

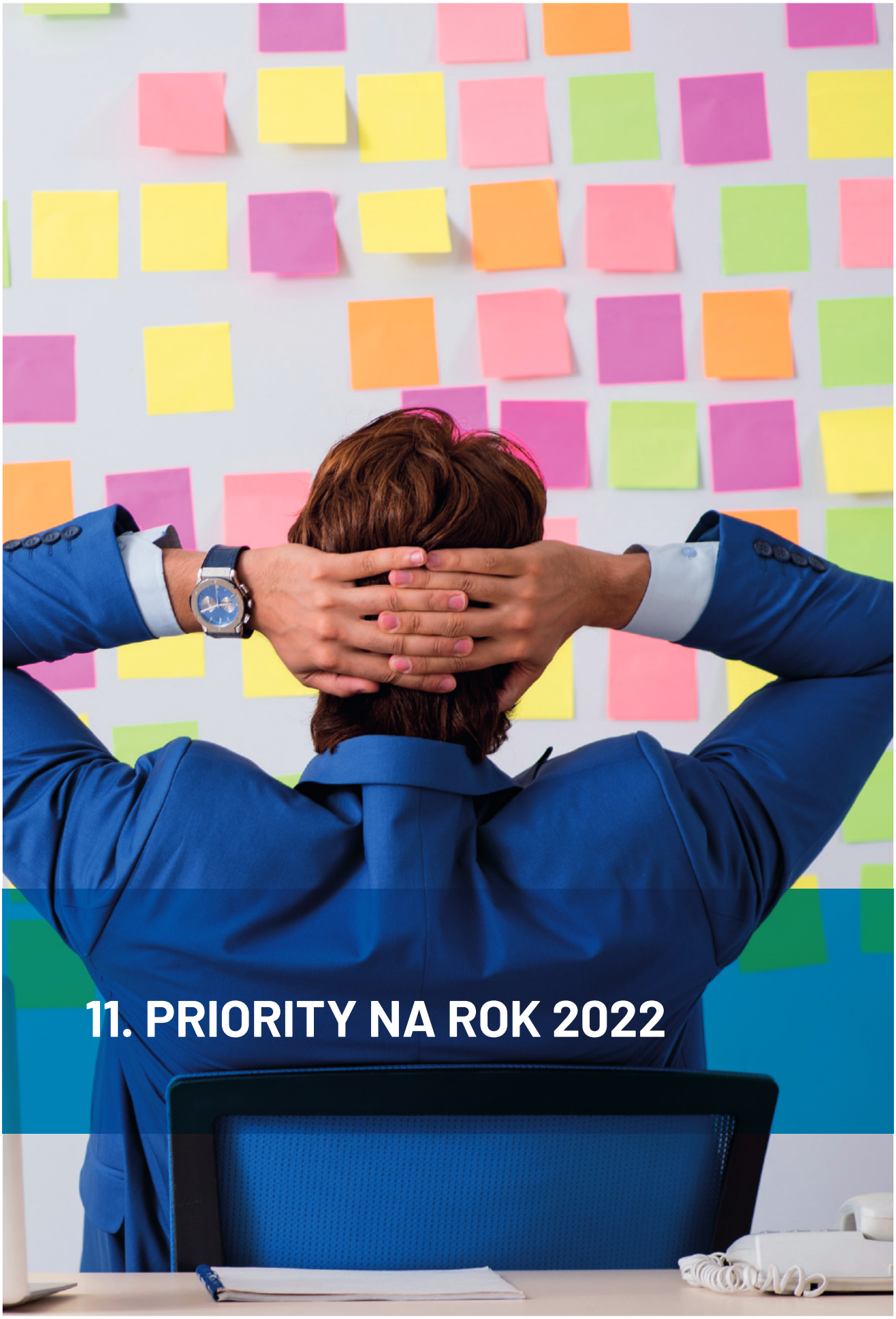
V roku 2021 boli útvarom vnútorného auditu vykonané **4 vnútorné audity,** z toho 3 plánované a 1 neplánovaný.

Boli zamerané na overenie a zhodnotenie vynakladania verejných prostriedkov na tuzemské služobné a pracovné cesty v rokoch 2019 a 2020, prevádzky služobných motorových vozidiel NBÚ so zameraním na oprávnenosť vyplácania príplatkov za vedenie služobných motorových vozidiel úradu v rokoch 2019 a 2020.

Venovali sa aj postupu NBÚ v zmysle zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov v znení neskorších predpisov v rokoch 2019 a 2020.

Neplánovaný vnútorný audit bol zameraný na overenie zákazky „Vybudovanie novej fyzickej a objektovej bezpečnosti NBÚ“ pred podpisom rámcovej zmluvy.

Vykonanými vnútornými auditmi **neboli v povinnej osobe zistené nedostatky**.



11. PRIORITY NA ROK 2022

PRIORITY NA ROK 2022

Medzi hlavné ciele na rok 2022 patrí ďalšia elektronizácia procesov a zvyšovanie pripravenosti Národného bezpečnostného úradu po všetkých stránkach.

Úrad bude pokračovať v implementácii projektu Elektronické služby spracovania bezpečnostných spisov, ktorý je určený najmä pre sekciu previerok. Kľúčové pracovisko úradu získa informačný systém v oblasti ochrany utajovaných skutočností, ktorý poslúži na vnútornú aj vonkajšiu komunikáciu s príslušnými subjektmi.

NBÚ bude pokračovať v snahe o ďalší rozvoj fyzickej a objektovej bezpečnosti svojho sídla.

Národný bezpečnostný úrad v súčasnosti prechádza rozsiahlou generačnou výmenou, a preto kladie dôraz na vylepšenie prijímacieho procesu a ďalšie vzdelávanie príslušníkov a zamestnancov v súlade s modernými trendmi.

Úrad dlhodobo pracuje aj na pripravovaných legislatívnych zmenách – na vyhláške k zákonu o kybernetickej bezpečnosti a krátkej novele zákona o ochrane utajovaných skutočností.

podatelna@nbu.gov.sk

+421 2 6869 1111

www.nbu.gov.sk