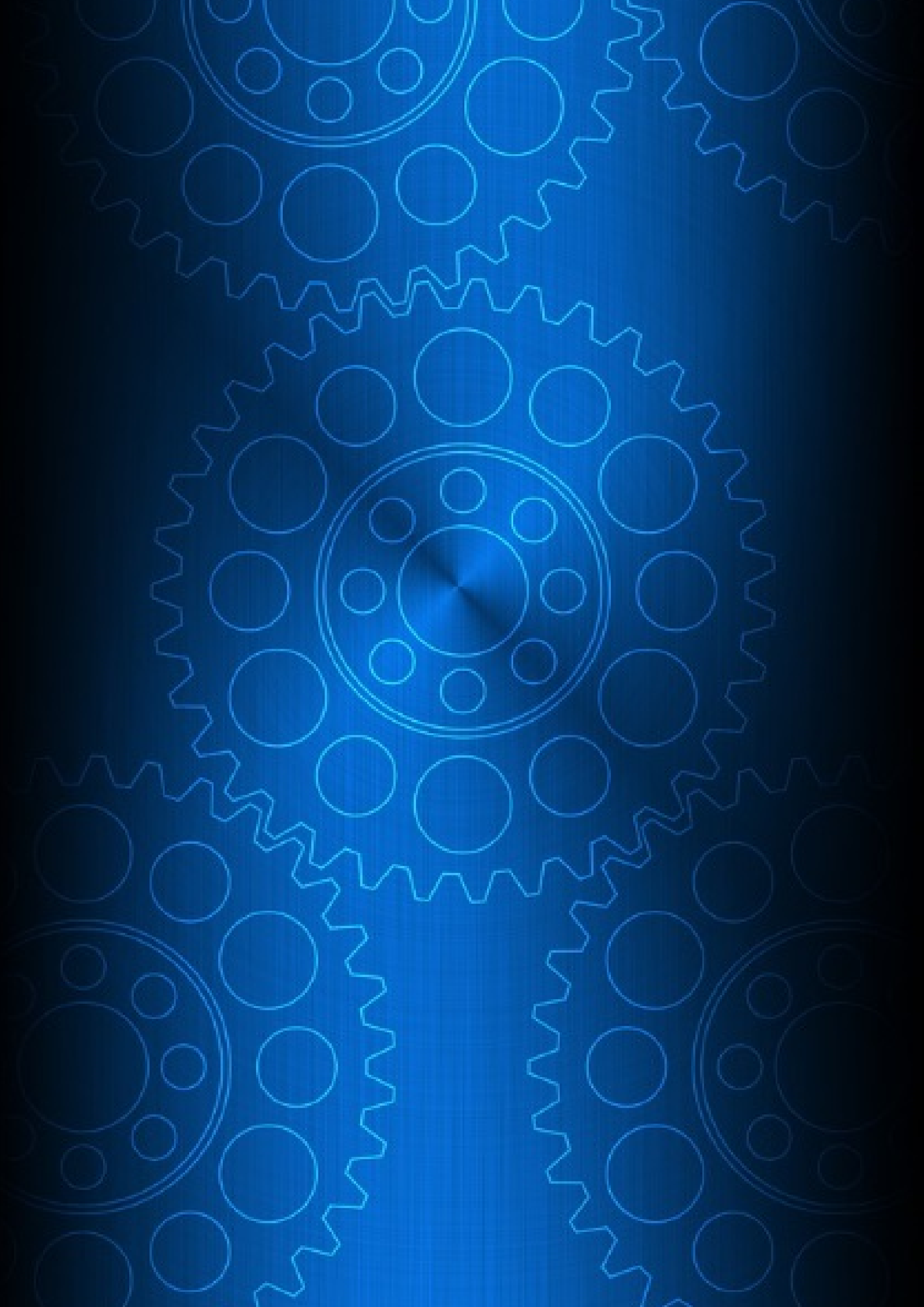
NÁRODNÝ
BEZPEČNOSTNÝ
ÚRAD

Správa o činnosti

2019



OBSAH

1. IDENTIFIKÁCIA ORGANIZÁCIE

NÁZOV	Národný bezpečnostný úrad
SÍDLO	Budatínska 30, 851 06 Bratislava
DRUH	ústredný orgán štátnej správy
ŠTATUTÁRNY ORGÁN	JUDr. Roman Konečný, riaditeľ
DÁTUM VZNIKU	1. novembra 2001
KONTAKT	+421 2 6869 1111, podatelna@nbu.gov.sk
WEBOVÉ SÍDLO	www.nbu.gov.sk

HLAVNÉ ČINNOSTI

Národný bezpečnostný úrad (ďalej len „úrad“) zodpovedá za tvorbu a realizáciu štátnej politiky pre **oblasť ochrany utajovaných skutočností, šifrovej služby, dôveryhodných služieb a kybernetickej bezpečnosti.** V každej oblasti vykonáva činnosti, ktoré napomáhajú pri plnení cieľov úradu.

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. Ďalej akredituje komunikačné a informačné systémy pre manipuláciu s utajovanými informáciami, 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 a 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 písomností a posudzovania podmienok na ochranu pred nežiaducim elektromagnetickým vyžarovaním. Vlastnou kontrolnou činnosťou úrad overuje podmienky zabezpečenia ochrany utajovaných skutočností v štátnych a samosprávnych orgánoch a u podnikateľov a vydáva metodické usmernenia k jednotlivým aspektom bezpečnosti utajovaných skutočností. Realizuje aktivity posilňujúce bezpečnostné povedomie a vykonáva skúšku bezpečnostného zamestnanca. Pri medzinárodnej výmene utajovaných skutočností plní úrad funkciu centrálneho registra utajovaných skutočností v Slovenskej republike a podieľa sa na ochrane zahraničných utajovaných skutočností.

V oblasti **šifrovej ochrany informácií** (ŠOI) vykonáva úrad certifikáciu prostriedkov ŠOI, vydáva bezpečnostné štandardy a koordinuje výskum a vývoj prostriedkov ŠOI. Plní úlohu garanta a národnej autority v rámci medzinárodnej spolupráce v oblasti ŠOI 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 v Slovenskej republike. Realizuje úlohy súvisiace s certifikáciou zariadení na vyhotovovanie kvalifikovaných elektronických podpisov a kvalifikovaných elektronických pečatí; vytvára, vedie a zverejňuje dôveryhodný zoznam a zoznam oprávnení na účel vydávania mandátnych certifikátov. Prevádzkuje Koreňovú certifikačnú autoritu Slovenskej republiky, ktorá vydáva kvalifikovaným poskytovateľom dôveryhodných služieb certifikáty verejných kľúčov. Do 31. júla 2019 úrad prevádzkoval aj Slovenskú národnú certifikačnú autoritu (SNCA), ktorá je kvalifikovaným poskytovateľom dôveryhodných služieb pre orgány verejnej moci a poskytuje kvalifikované dôveryhodné služby orgánom verejnej moci. Služby SNCA od 1. augusta 2019 zabezpečuje Národná agentúra pre sieťové a elektronické služby.

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, ktorými je Slovenská republika viazaná, 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 podľa **zákona o ochrane utajovaných skutočností** (zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, súvisiacich vykonávacích predpisov a platných štandardov. 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 o dôveryhodných službách** (zákon č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov). Pri plnení úloh v oblasti kybernetickej bezpečnosti postupuje úrad podľa **zákona o kybernetickej bezpečnosti** (zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov a podľa príslušných vyhlášok vydaných na vykonanie zákona).

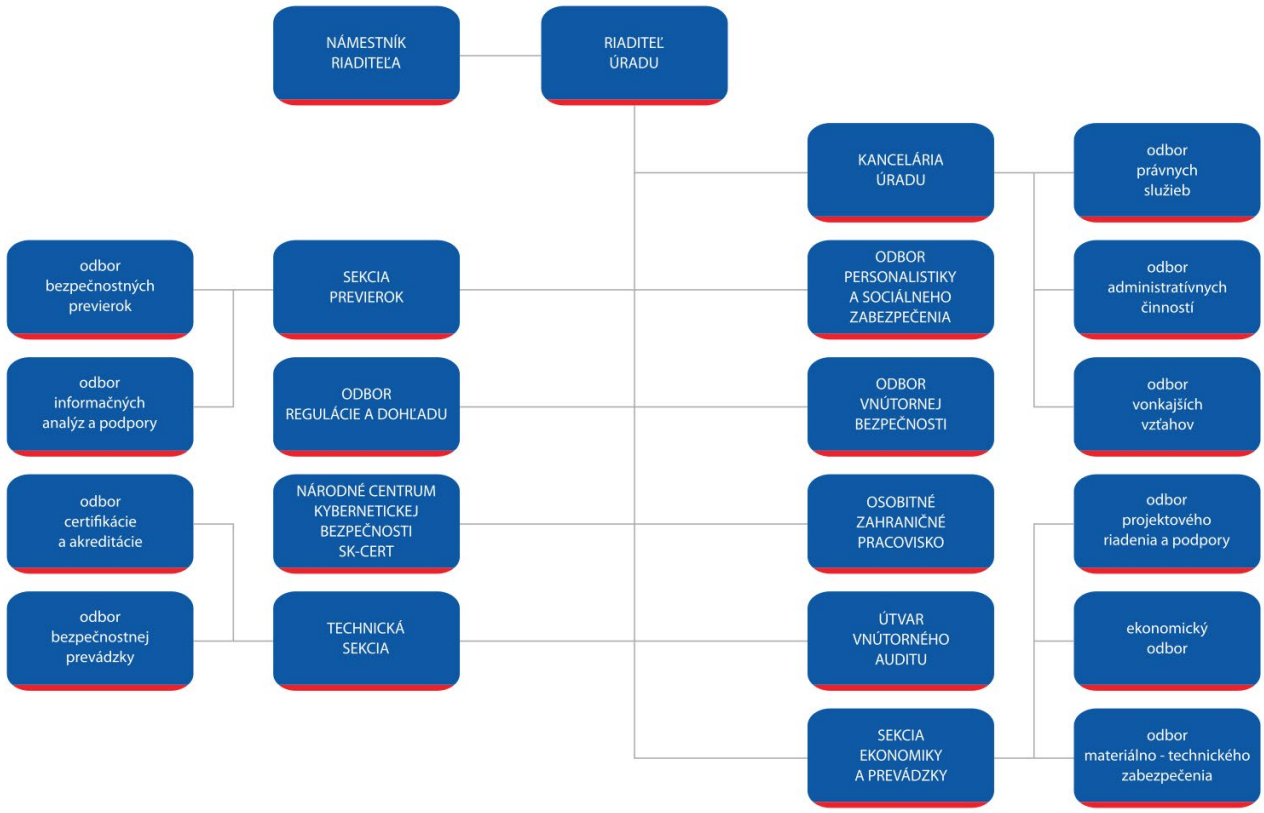
VEDENIE ÚRADU

Na čele úradu stojí **riaditeľ,** ktorý zodpovedá za činnosť úradu. Riadi a reprezentuje úrad navonok. Riaditeľ rozhoduje o spôsobe realizácie hlavných úloh úradu, schvaľuje interné právne predpisy, rozhoduje o vnútornom organizačnom usporiadaní úradu a o personálnych otázkach jeho príslušníkov a zamestnancov. Zastrešuje medzirezortnú spoluprácu úradu 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.

Vnútorné členenie úradu **k 31. decembru 2019:**



ÚTVARY ÚRADU

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; vykonáva bezpečnostné previerky fyzických osôb a podnikateľov, vydáva certifikáty pre prístup k utajovaným skutočnostiam NATO a EÚ a vyjadruje sa o navrhovaných osobách podľa medzinárodných zmlúv, ktorými je Slovenská republika viazaná.

Odbor 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 rámci programu 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 štandardy a znalostné štandardy, certifikačné politiky a podpisové politiky, politiku správania sa v kybernetickom priestore, zásady predchádzania kybernetickým bezpečnostným incidentom a zásady ich riešenia. 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.

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.

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 a zabezpečuje komunikáciu smerom k verejnosti.

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

Odbor vnútornej bezpečnosti zaisťuje vnútornú bezpečnosť úradu a zabezpečuje fyzickú a technickú ochranu objektov úradu. Vykonáva vnútornú kontrolu a finančnú kontrolu, vybavuje sťažnosti a petície. Plní úlohy zodpovednej osoby pri vybavovaní oznámení o protispoločenskej činnosti a na úseku ochrany osobných údajov; vypracúva zmluvy o prístupe podnikateľa k utajovaným skutočnostiam a plní aj úlohy na úseku BOZP a ochrany pred požiarmi.

Osobitné zahraničné pracovisko plní úlohy pri rozvíjaní a budovaní medzinárodných vzťahov a spolupráce úradu v zahraničí. Pracovisko zabezpečuje komunikáciu medzi úradom a zahraničnými partnermi, zastupuje záujmy Slovenskej republiky v oblastiach zverených do právomoci úradu v NATO, v európskych inštitúciách a agentúrach a realizuje bilaterálnu a multilaterálnu spoluprácu v rámci zastúpenia úradu v zahraničí.

Útvar vnútorného audítora vykonáva vnútorný audit úradu a plní ďalšie úlohy podľa zákona o finančnej kontrole a audite.

Sekcia ekonomiky a prevádzky zabezpečuje finančné riadenie úradu, koordináciu v procese hospodárenia s finančnými prostriedkami, vrátane účtovníctva a výkazníctva, správu a údržbu majetku úradu a realizuje verejné obstarávanie pre potreby úradu a participuje na koordinácii v rámci projektového a riadenia programov a projektov financovaných zo zdrojov EÚ.

2. ĽUDSKÉ ZDROJE

Na úrade pracujú príslušníci v služobnom pomere podľa zákona č. 73/1998 Z. z. o štátnej službe príslušníkov Policajného zboru, Slovenskej informačnej služby, Zboru väzenskej a justičnej stráže Slovenskej republiky a Železničnej polície a zamestnanci v pracovnom pomere podľa zákona č. 552/2003 Z. z. o výkone prác vo verejnom záujme.

PROTIKORUPČNÝ PROGRAM

Úrad v roku 2019 vypracoval vlastný **Protikorupčný program,** ktorý vychádza z Protikorupčnej politiky Slovenskej republiky na roky 2019 – 2023 z decembra 2018. Podrobnejšie a adresnejšie premieta vládnu protikorupčnú politiku do podmienok úradu. Úradný protikorupčný program je nástrojom na **posilňovanie a presadzovanie protikorupčnej kultúry,** či zdokonalenie riadenia a rozpoznávania korupčných rizík. Úrad v ňom posudzuje a vyhodnocuje existujúce korupčné riziká a zavádza konkrétne systémové opatrenia zamerané na prevenciu korupcie a podporu protikorupčného správania pracovníkov úradu.

ETICKÝ KÓDEX

Na jeseň 2019 sformuloval Etický kódex, ktorý stanovuje **pravidlá pre dodržiavanie čestných, korektných, spoločensky zodpovedných, profesionálnych a morálnych zásad** správania pracovníkov úradu. Nielen pri vzájomnej komunikácii, ale aj pri vzťahoch vo vonkajšom prostredí. Etický kódex objasňuje politiku úradu v citlivých otázkach a vyjadruje snahu úradu pracovať a riadiť sa najvyššími princípmi spoločenskej etiky.

Spoločne s Protikorupčným programom predstavuje etický kódex nástroj pozitívnej motivácie pracovníkov úradu posilnením ich vedomia, že pracujú v etickom prostredí s jasnými pravidlami platnými pre každého. Kódex sa vzťahuje na všetkých pracovníkov úradu, bez rozdielu v ich pracovnom zaradení alebo postavení v hierarchii riadenia. Sankcie za porušenie stanovených etických princípov ukladá Etická komisia úradu. V roku 2019 neboli komisii predložené žiadne podnety voči porušeniu zásad etického kódexu pracovníkmi.

ŠTATISTICKÉ UKAZOVATELE

Celkový počet pracovníkov úradu bol za uplynulé tri roky relatívne stabilný. Zásadne sa nezmenil ani pomer medzi počtom príslušníkov a zamestnancov (približne 90:10), zachovaná ostala aj mierna prevaha počtu žien nad počtom mužov. Údaje k 31. decembru príslušného kalendárneho roka sú podrobne rozpísané v tabuľke č. 1.

Tabuľka č. 1: Počet príslušníkov a zamestnancov v rokoch 2017 – 2019

	k 31.12.2017	k 31.12. 2018	k 31.12. 2019
Príslušníci	**197 (90,78%)**	**200 (89,69%)**	**195 (89,45%)**
v prípravnej štátnej službe	19 (9,64%)	18 (9,00%)	12 (6,15%)
v stálej štátnej službe	177 (89,85%)	179 (89,50%)	180 (92,31%)
v dočasnej štátnej službe	1 (0,51%)	3 (1,50%)	3 (1,54%)
Zamestnanci	**20 (9,22%)**	**23 (10,31%)**	**23 (10,55%)**
Spolu	**217** (115 žien a 102 mužov)	**223** (119 žien a 104 mužov)	**218** (118 žien a 100 mužov)

V roku 2019 sa udržal trend posilňovania najpočetnejšie zastúpenej vekovej skupiny 35 až 49 rokov. V roku 2019 členovia tejto skupiny tvorili medzi príslušníkmi až 62,05% (26,09% medzi zamestnancami). Skupinu pritom tvoria najmä skúsení odborníci s niekoľkoročnou praxou v najproduktívnejšom veku. Všetky údaje o vekovej štruktúre úradu sú uvedené v tabuľke č. 2.

Tabuľka č. 2: Vek príslušníkov a zamestnancov úradu v rokoch 2017 – 2019

	k 31.12.2017		k 31.12.2018		k 31.12.2019	
	príslušníci **197** (100%)	zamestnanci **20** (100%)	príslušníci **200** (100%)	zamestnanci **23** (100%)	príslušníci **195** (100%)	zamestnanci **23** (100%)
Mladší ako 34 rokov	**39** (19,80%)	**1** (5,00%)	**38** (19,00%)	**6** (26,09%)	**35** (17,95%)	**6** (26,09%)
35 až 49 rokov	**117** (59,39%)	**2** (10,00%)	**121** (60,50%)	**3** (13,04%)	**121** (62,05%)	**6** (26,09%)
50 až 59 rokov	**32** (16,24%)	**10** (50,00%)	**35** (17,50%)	**7** (30,43%)	**32** (16,41%)	**6** (26,09%)
Starší ako 60 rokov	**9** (4,57%)	**7** (35,00%)	**6** (3,00%)	**7** (30,43%)	**7** (3,59%)	**5** (21,74%)

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. Údaje o vzdelanostnej štruktúre príslušníkov a zamestnancov úradu sú uvedené v tabuľke č. 3.

Tabuľka č. 3: Vzdelanie príslušníkov a zamestnancov úradu v rokoch 2017 – 2019

	k 31.12.2017		k 31.12.2018		k 31.12.2019	
	príslušníci **197** (100%)	zamestnanci **20** (100%)	príslušníci **200** (100%)	zamestnanci **23** (100%)	príslušníci **195** (100%)	zamestnanci **23** (100%)
Základné	**0** (0,00%)	**2** (10,00%)	**0** (0,00%)	**2** (8,70%)	**0** (0,00%)	**2** (8,70%)
Úplné stredné	**30** (15,23%)	**12** (60,00%)	**32** (16,00%)	**12** (52,17%)	**29** (14,87%)	**12** (52,17%)
Vysokoškolské - I. stupeň	**4** (2,03%)	**0** (0,00%)	**5** (2,50%)	**1** (4,35%)	**6** (3,08%)	**0** (0,00%)
Vysokoškolské - II. stupeň	**154** (78,17%)	**6** (30,00%)	**152** (76,00%)	**7** (30,43%)	**150** (76,92%)	**8** (34,78%)
Vysokoškolské - III. stupeň	**9** (4,57%)	**0** (0,00%)	**11** (5,50%)	**1** (4,35%)	**10** (5,13%)	**1** (4,35%)

Okrem periodických školení BOZP a ochrany pred požiarmi boli v roku 2019 realizované aj ďalšie interné vzdelávacie podujatia. Zameriavali sa na praktickú aplikáciu interných právnych predpisov, uplatňovanie personálnej a disciplinárnej právomoci nadriadených a dodržiavanie režimových opatrení objektu úradu. Úrad zabezpečil aj účasť vybraných príslušníkov úradu, určených na plnenie úloh v oblasti ochrany objektu a osobnej ochrany, na špeciálnej príprave v Centre výcviku Ministerstva obrany Slovenskej republiky na Lešti. S cieľom dosiahnuť požadovanú úroveň telesnej zdatnosti pracovníkov úradu bolo v roku 2019 rozšírené materiálne vybavenie telocvične, ktorá je prístupná pre všetkých pracovníkov úradu. Podporuje udržiavanie a zvyšovanie ich fyzickej kondície a vitality.

3. OBLASTI PÔSOBENIA

Úrad pri plnení úloh zohľadňuje právny rámec, ktorý vymedzuje jeho pôsobnosť. S plnením určených úloh súvisí množstvo výkonných, no aj legislatívnych, administratívnych a ďalších podporných činností.

3.1 LEGISLATÍVA

Úrad v roku 2019 reagoval na vývoj v bezpečnostnom prostredí, predovšetkým na prudkú informatizáciu spoločnosti a rastúcu dynamiku bezpečnostných hrozieb **prípravou legislatívnych návrhov** a zavádzaním vhodných legislatívnych podmienok, ktorými bolo potrebné reagovať na vývojové trendy a na problémy z aplikačnej praxe.

VŠEOBECNE ZÁVÄZNÉ PRÁVNE PREDPISY

Počas roka 2019 pokračovali práce na príprave **novej legislatívy v oblasti ochrany utajovaných skutočností**, ktorých účelom bolo stanoviť optimálne zásady a minimálne štandardy na vytvorenie bezpečného prostredia pre utajované skutočnosti. V roku 2019 plynula legisvakančná lehota predchádzajúca nadobudnutiu účinnosti **vyhlášky o administratívnej bezpečnosti** (vyhláška NBÚ č. 48/2019, ktorou sa ustanovujú podrobnosti o administratívnej bezpečnosti utajovaných skutočností). Účelom stanovenia takmer ročnej lehoty medzi nadobudnutím platnosti a účinnosti predmetnej vyhlášky, ktorá zásadným spôsobom mení doterajšiu filozofiu v tejto oblasti, bolo poskytnúť fyzickým a právnickým osobám dostatočný časový rámec na to, aby sa so zmenami v tejto striktne regulovanej oblasti stihli pred 1. januárom 2020 oboznámiť. Úrad lehotu využil aj na zorganizovanie série prezentácií, metodických dní a dvojstranných expertných stretnutí so zástupcami najexponovanejších orgánov verejnej moci i podnikateľov.

1. septembra 2019 nadobudla účinnosť **novela zákona proti byrokracii** (č. 221/2019 Z. z.), podľa ktorej sa zmenil a doplnil aj zákon o ochrane utajovaných skutočností: konkrétne vydaním nového bezpečnostného dotazníka podnikateľa. V súlade s filozofiou antibyrokratického zákona boli podnikatelia oslobodení od povinnosti predkladať úradu so žiadosťou o vykonanie previerky priemyselnej bezpečnosti údaje, ktoré úrad dokáže získať na základe prístupu do viacerých existujúcich štátnych registrov, resp. v spolupráci s orgánmi verejnej moci.

19. júna 2019 bol v Zbierke zákonov Slovenskej republiky vyhlásený **zákon č. 211/2019 Z. z.,** ktorým sa mení a dopĺňa zákon č. 305/2013 Z. z. **o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci** a o zmene a doplnení niektorých zákonov (zákon o e-Governmente) v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony, o. i. aj zákon o dôveryhodných službách.

1. januára 2019 nadobudla účinnosť **vyhláška č. 362/2018, ktorou sa ustanovuje obsah bezpečnostných opatrení,** obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení. V auguste 2019 úrad predložil do medzirezortného pripomienkového konania iniciatívny **návrh vyhlášky o audite kybernetickej bezpečnosti a znalostnom štandarde audítora.** Keď prešla vnútroštátnym legislatívnym procesom, bola 11. decembra 2019 vydaná v Zbierke zákonov pod č. 436/2019 Z. z. (s účinnosťou od 1. januára 2020). Ide o v poradí piaty vykonávací predpis k zákonu o kybernetickej bezpečnosti.

INTERNÉ PREDPISY

V roku 2019 vydal úrad **12 nariadení** riaditeľa úradu, **32 rozkazov** riaditeľa úradu a **tri štatúty.** Nariadenia a štatúty boli vydávané s cieľom **zefektívniť vnútorné procesy** a **implementovať všeobecne záväzné právne predpisy** (napr. nové nariadenie **o verejnom obstarávaní, o rozkladovej komisii,** nový **registratúrny poriadok, Etický kódex,** úprava **organizačného poriadku,** úprava **personálnej evidencie** a úloh útvarov úradu súvisiacich so služobným pomerom príslušníkov, nový **štatút o vnútornom audite** a nový **štatút Národného centra kybernetickej bezpečnosti SK-CERT**). Rozkazy riaditeľa úradu slúžili na určenie nositeľov konkrétnych úloh – napr. pri výcviku, inventarizácii majetku, delimitácii majetku a pri zriaďovaní projektových tímov.

SPRÁVNE A PRIESTUPKOVÉ KONANIE

V roku 2019 úrad prijal **osem podnetov na prešetrenie neoprávnenej manipulácie** s utajovanými skutočnosťami. Ako správny orgán pre túto oblasť uložil pokuty v súhrnnej sume 300 eur. Úrad sa zaoberal aj **piatimi podnetmi** na začatie správneho konania vo veci **porušenia zákona o dôveryhodných službách.** Vo všetkých prípadoch konanie zastavil.

Úrad prijal aj **päť podaní na úseku leteckého snímkovania.** Vo všetkých prípadoch úrad vec odložil záznamom, pretože nedošlo k spáchaniu priestupku podľa zákona o ochrane utajovaných skutočností.

ZNALECKÁ ČINNOSŤ

Úrad je **znalecká organizácia** zapísaná v zozname Ministerstva spravodlivosti Slovenskej republiky v odbore 50 00 00 – ochrana utajovaných skutočností. V roku 2019 príslušné orgány nepožiadali úrad o znalecké skúmanie.

3.2 MEDZINÁRODNÉ VZŤAHY

V roku **2019 úrad spolupracoval s bezpečnostnými orgánmi EÚ a NATO** a s ďalšími medzinárodnými organizáciami vo všetkých oblastiach svojej pôsobnosti. Úrad vyvíjal aktívne kroky smerujúce k **podpore regionálnej spolupráce a rozvoju bilaterálnych partnerstiev** umožňujúcich výmenu skúseností, formuláciu jednotných stanovísk a koordináciu postupov pri presadzovaní spoločných záujmov. Prostredníctvom pracoviska Centrálneho registra úrad zabezpečoval **medzinárodnú výmenu utajovaných skutočností** a podieľal sa na ich ochrane.

PÔSOBENIE V ORGÁNOCH EURÓPSKEJ ÚNIE

Úrad má expertné zastúpenie vo všetkých troch platformách orgánov a inštitúcií EÚ zaoberajúcich sa politikou **bezpečnosti a ochrany utajovaných informácií EÚ** (EUCI). Ťažiskom agendy súvisiacej s ochranou EUCI v roku 2019 boli otázky tvorby bezpečnostných politík zameraných na priemyselnú bezpečnosť, bezpečnostné predpisy **Rady a EEAS,** návrh bezpečnostných pravidiel **Súdneho dvora a Všeobecného súdu,** ako aj **spolupráca medzi inštitúciami, agentúrami, úradmi a orgánmi EÚ** pri ochrane EUCI.

Na pôde **Európskej Komisie** bola v roku 2019 venovaná veľká miera pozornosti bezpečnostnému rámcu **Programu rozvoja európskeho obranného priemyslu.** Príslušníci úradu sa zúčastňovali aj na zasadnutiach **Skupiny expertov pre bezpečnostnú politiku (ComSEG),** ktorá zodpovedá za prípravu a výkon bezpečnostných politík a pravidiel v spektre inštitúcií EÚ. Ďalšími formátmi EK, do ktorých boli zapojení zástupcovia úradu, sú **Expertný bezpečnostný výbor pre globálny navigačný satelitný systém (GNSS SB)** a **Bezpečnostný akreditačný panel** Európskej GNSS agentúry (GSA) v rámci budovania satelitného systému Galileo (SAB).

V **Európskej službe pre vonkajšiu činnosť (EEAS)** pôsobí Bezpečnostný výbor EEAS pre prípravu politík a návrhov (bezpečnosti vo všeobecnosti), ochrany utajovaných informácií v podmienkach EEAS a jej zahraničných delegáciách, ako aj aktualizácii medzinárodných zmlúv v oblasti EUCI, v ktorom pôsobili aj delegovaní zástupcovia úradu. Experti úradu sa zúčastňovali aj na zasadnutiach podvýboru EEAS (SAB) – Podvýbor pre bezpečnostnú akreditáciu EEAS EU OPS WAN.

Rada EÚ venovala pozornosť používaniu prostriedkov **šifrovej ochrany informácií** na ochranu EUCI v podmienkach členských štátov, najmä v spojitosti s misiami a operáciami pod vedením EÚ. Príslušníci úradu sa pravidelne zúčastňovali na **Bezpečnostnom výbore Rady EÚ (CSC),** kde sa v **Implementačnej pracovnej skupine pre TEMPEST (ITTF),** venovali otázkam súvisiacim s ochranou pred nežiaducim elektromagnetickým vyžarovaním.

V roku 2019 bolo prijatých viacero dôležitých právnych aktov EÚ na **posilnenie boja proti kybernetickým hrozbám,** z ktorých najdôležitejším je **nariadenie o agentúre ENISA** (Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881 o Agentúre Európskej únie pre kybernetickú bezpečnosť ENISA) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti)), ktoré nadobudlo účinnosť 7. mája 2019. V nadväznosti na účinnosť uvedenej legislatívy bola zriadená **Európska skupina pre certifikáciu kybernetickej bezpečnosti ECCG**, v ktorej Slovenskú republiku reprezentuje úrad. ECCG je založené na princípoch a postupoch celosvetovo uznávaného certifikačného rámca CCRA (Common Criteria Recognition Arrangement). Súčasne so zapojením do zoskupenia sa úrad za Slovenskú republiku pripojil aj do rámca CCRA.

Slovenská republika prostredníctvom úradu v roku 2019 upevnila a prehĺbila spoluprácu s **agentúrou ENISA,** ktorá zo svojej pozície centra pre kybernetickú bezpečnosť v EÚ pomáha členským štátom, aby boli lepšie vybavené a pripravené na predchádzanie, odhaľovanie a riešenie problémov kybernetickej bezpečnosti. Spolupráca zahŕňala koordináciu reakcií na globálne kybernetické incidenty a týkala sa aj podielu na výkone činností agentúry ENISA, pripomienkovaním rozhodnutí a zastúpenia riaditeľa Národného centra pre kybernetickú bezpečnosť SK-CERT v **Management Board agentúry ENISA.** V roku 2019 bola za alternáta za SR menovaná vedúca Osobitného zahraničného pracoviska.

Vzhľadom na povinnosť členských štátov transponovať smernicu NIS do národných legislatív bolo potrebné aj v roku 2019 viesť neustály dialóg. Dôraz bol kladený najmä na riešenie otázok spojených s identifikáciu prevádzkovateľov základných služieb. Aktívnu pozíciu v tomto procese zastávala **Skupina pre spoluprácu (NIS Cooperation Group)** a **Sieť jednotiek pre riešenie počítačových bezpečnostných incidentov (CSIRT's Network).** Hlavnou úlohou týchto pracovných platforiem bolo zabezpečovať a zintenzívňovať vzájomnú strategickú a operačnú spoluprácu, zdieľať informácie medzi orgánmi kybernetickej bezpečnosti členských štátov a medzi ich jednotkami CSIRT. Platformy pracovali na periodickej báze a prijímali potrebné pravidlá a procesné postupy. Boli zadefinované kľúčové priority práce skupiny a úlohy siete CSIRT pre zabezpečenie operačných spôsobilostí EÚ, ako aj spoločná koordinovaná reakcia EÚ na kybernetické bezpečnostné incidenty a krízy veľkého rozsahu.

EK v druhej polovici roka 2018 navrhla právne nástroje na vykonávanie iniciatívy na posilnenie postavenia EÚ, ktoré by jej umožnilo stať sa globálnym lídrom v oblasti kybernetickej bezpečnosti s cieľom zabezpečiť dôveru, spoľahlivosť a ochranu občanov, spotrebiteľov a podnikov online a umožniť bezplatný a zákonný internet. Do legislatívneho procesu predložený návrh európskeho nariadenia na zriadenie **Európskeho centra odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti a siete národných koordinačných centier.** O jeho znení sa počas celého roka 2019 viedla diskusia na pôde pracovného formátu Rady EÚ a diskusia v legislatívnom procese.

Pracovný formát **Horizontálna pracovná skupina pre kybernetické záležitosti (HWP)** sa venoval prierezovým kybernetickým otázkam, zasahujúcim do oblasti hodnotenia kybernetických hrozieb, kybernetickej kriminality, kybernetickej diplomacie a certifikácie. V sledovanom období dominovali témy reformy databázy doménových mien WHOIS, implementácie rámca pre spoločnú diplomatickú reakciu EÚ voči škodlivým kybernetickým aktivitám, atribúcie (prisudzovania) škodlivých kybernetických aktivít a možnosti zavedenia rámca reštriktívnych opatrení s cieľom reagovať na kybernetické hrozby, alebo tieto hrozby odrádzať. Na pracovnej rovine HWP bolo v roku 2019 pripravené (a na ministerskej úrovni schválené) **Nariadenie a Rozhodnutie Rady o reštriktívnych opatreniach proti kybernetickým útokom ohrozujúcim Úniu alebo jej členské štáty.**

Nosnou nelegislatívnou témou v EÚ v roka 2019 bola téma kybernetickej bezpečnosti **sietí piatej generácie (5G).** Úrad v spolupráci s orgánmi verejnej moci, telekomunikačným regulátorom a telekomunikačnými operátormi, v kontexte Odporúčania EK o kybernetickej bezpečnosti 5G sietí z marca 2019, vypracoval národné posúdenie rizík implementácie 5G technológií, ktoré boli podkladom pre **Spoločné európske posúdenie rizík súvisiacich s 5G sieťami** vydané v októbri 2019. Začiatkom roka 2020 členské štáty EÚ, s podporou EK a agentúry ENISA, zverejnili **Súbor opatrení určených na riešenie rizík v oblasti kybernetickej bezpečnosti 5G sietí, tzv. 5G Toolbox.** Členské štáty by mali v ďalšom slede jednotlivé opatrenia implementovať a do 1. októbra 2020 by mali v spolupráci s EK posúdiť dopady a určiť, či bude potrebné vykonať ďalšie kroky.

Úrad počas celého roka 2019 aktívne pôsobil aj v **Európskej organizácii pre kybernetickú bezpečnosť (ECSO).** V organizačnej štruktúre ECSO je úrad členom Výboru zástupcov národných verejných autorít (NAPAC) a pozorovateľom v predstavenstve. Zástupcovia úradu sa zúčastňovali na práci troch zo šiestich pracovných skupín WG1: certifikácia, štandardizácia, WG5: vzdelávanie, budovanie bezpečnostného povedomia a tréningy v oblasti kybernetickej bezpečnosti, WG6: agenda strategického výskumu a inovácií.

PÔSOBENIE V ORGÁNOCH ORGANIZÁCIE SEVEROATLANTICKEJ ZMLUVY

Úrad sa aktívne zúčastňoval na pravidelných jarných a jesenných zasadnutiach **Bezpečnostného výboru NATO (SC)** na úrovni riaditeľov bezpečnostných autorít členských krajín a na úrovni tvorby bezpečnostných politík. Výbor rieši všetky otázky súvisiace s bezpečnostnou politikou aliancie a je poradným orgánom Severoatlantickej rady (NAC).

V Bezpečnostnom výbore pre tvorbu bezpečnostných politík zástupcovia úradu participovali na rozsiahlej revízii normy C-M(2002)49 (bezpečnostná politika NATO) a jej doplnkových direktív pre všetky oblasti bezpečnosti. Novinkou bolo predstavenie **dvoch nových direktív,** do ktorých sa obsahovo sústredili **všetky aspekty ochrany utajovaných skutočností** NATO vo vzťahu k nečlenským entitám ako požiadavka, ktorá vyplynula z aplikačnej praxe v podmienkach vojenských a civilných zložiek NATO. V máji 2019 sa vo Varšave uskutočnilo jedno z najväčších zasadnutí SC venované aspektom spolupráce s nečlenskými krajinami.

V kontexte vývoja v bezpečnostnom prostredí a po uznaní kybernetického priestoru ako operačnej domény NATO (Varšavský samit 2016) sa problematika kybernetickej bezpečnosti čoraz významnejšie dostáva do popredia záujmu orgánov NATO. Závery Londýnskeho samitu 2019 potvrdili, že kybernetické hrozby voči NATO sa stávajú častejšími, komplexnejšími a ničivejšími. Vo februári 2019 členské krajiny schválili príručku NATO, ktorá definuje **nástroje posilňujúce spôsobilosť aliancie reagovať na závažné kybernetické incidenty.** Pokračovali práce na vytvorení **Centra pre kybernetické operácie,** ktorá sa má stať súčasťou posilnenej veliteľskej štruktúry NATO. Úrad prostredníctvom svojho zástupcu pôsobil vo **Výbore pre kybernetickú obranu (CDC),** ktorý je zastrešujúcim politickým orgánom pre oblasť kybernetickej obrany aliancie a participoval na príprave strategických dokumentov NATO v oblasti kybernetickej bezpečnosti.

Úrad na národnej úrovni zastrešil 12. ročník cvičenia **Cyber Coalition 2019**, ktoré sa tradične konalo v Estónsku. Cvičenie bolo zamerané na preverenie národných spôsobilostí a postupov podľa platných legislatívnych pravidiel a postupov NATO, ako aj na podporu lepšej koordinácie a spolupráce medzi jednotlivými rezortmi. Úrad pôsobil aj v platforme **MN MISP** (Multinational Malware Information Sharing Platform), ktorá umožňuje neformálnu výmenu informácií o kybernetických hrozbách medzi 27 členskými krajinami NATO a šiestimi partnerskými krajinami NATO.

Príslušníci úradu v roku 2019 pôsobili v **Bezpečnostnom výbore NATO** vo formáte pre bezpečnosť komunikačných a informačných systémov SC (CISS) a v **Podvýbore NATO pre informačnú bezpečnosť a kybernetickú ochranu (CaP4).** V štruktúrach **systému BICES** (Battlefield Information Collection and Exploitation System) sa príslušníci úradu zúčastňovali na **Bezpečnostnej pracovnej skupine BSWG** (BICES Working Group) a **Bezpečnostnom akreditačnom paneli BSAB** (BICES Accreditation Board). Zúčastňovali sa aj na práci **Bezpečnostného výboru NATO pre informačnú bezpečnosť** SC (Information Assurance (CISS)), **Bezpečnostného akreditačného panelu systémov NATO** (NATO Security Accreditation Board) a **Špecifikácie interoperability pre správu kľúčov** (NATO-KM- ISPEC).

V roku 2019 sa úrad spolupodieľal na vyplnení dotazníka NATO o **spôsobilostiach obranného plánovania.** Slovenskej republike vyplýva raz za dva roky povinnosť vyplniť dotazník a odmerať tým pokrok v jednotlivých oblastiach. Úrad participoval v oblastiach kybernetickej obrany a civilného plánovania. Príslušníci úradu sa v októbri 2019 zúčastnili na rokovaniach s NATO o zodpovedaní doplňujúcich otázok. Vyhodnotenie bude známe na jar 2020.

Príslušníci úradu sa v roku 2019 pri plnení opatrení **Národného systému reakcie na krízové situácie** zúčastnili na **cvičení krízového riadenia NATO CMX** (cvičenie na najvyššej strategickej úrovni zamerané na precvičenie a skvalitnenie politických konzultácií a prijímania rozhodnutí). 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 2019,** ktoré malo preveriť komunikačné procedúry súvisiace s jadrovým plánovaním, precvičiť použiteľné opatrenia systému krízovej odozvy aliancie, priniesť zdokonalenie v konzultačnej oblasti, realizovať praktický výcvik personálu v centrále NATO, v Hlavnom veliteľstve spojeneckých síl v Európe (SHAPE) a v národných ústrediach. Úrad sa na cvičení zúčastňoval na distribučnej úrovni, prostredníctvom pracoviska centrálneho registra zabezpečil prijímanie a postupovanie utajovaných skutočností. Komunikácia počas cvičenia prebiehala prostredníctvom informačného systému NNCCRS (NATO Nuclear Command Control Response System), ktorým prúdil tok informácií medzi zainteresovanými rezortmi, úradom a centrálou NATO.

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. V septembri 2019 bolo pod záštitou chorvátskeho predsedníctva v Splite 34. plenárne zasadnutie MISWG, ktoré poskytlo platformu na výmenu a zdieľanie skúseností zástupcov partnerských bezpečnostných úradov s vykonávaním bezpečnostných previerok podnikateľov, vyhodnocovaním bezpečnostných rizík a ich elimináciou. Účastníci splitského zasadnutia MISWG rozhodli o prijatí Čiernej Hory za riadneho člena organizácie.

PÔSOBENIE V ORGANIZÁCII PRE BEZPEČNOSŤ A SPOLUPRÁCU V EURÓPE

Úrad je jediným oficiálnym kontaktným technickým bodom Slovenskej republiky v **Organizácii pre bezpečnosť a spoluprácu v Európe (OBSE)** pre oblasť kybernetickej bezpečnosti. Pôsobí v neformálnej pracovnej skupine pre kybernetické otázky a aktívne sa podieľa na plnení stanovených spoločných cieľov. V roku 2019 Slovenská republika predsedala OBSE. Predsedníctvo v marci zorganizovalo každoročné podujatie **Vienna Cyber Security Week** v spolupráci s nadáciou EnergyPact Foundation**.** V júni 2019 slovenské predsedníctvo OBSE zorganizovalo v Bratislave dvojdňovú medzinárodnú konferenciu **Bezpečnejšia kybernetická/IKT budúcnosť: Úloha OBSE pri podpore regionálnej kybernetickej bezpečnosti,** ktorá bola venovaná témam súvisiacim s bezpečnosťou informačno-komunikačných technológií a bezpečnosťou kybernetického priestoru.

REGIONÁLNA SPOLUPRÁCA

K dôležitým prioritám úradu v roku 2019 patrilo upevňovanie regionálnej spolupráce, ako súčasti širšie definovaného záujmu úradu na budovaní kvalitných medzinárodných vzťahov. Tento druh spolupráce slúži na výmenu skúseností a názorov združených krajín, no najmä na hľadanie spoločného konsenzu a podpory pri tvorbe európskej legislatívy. V roku 2019 preto úrad 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 rámci neformálnej **Stredoeurópskej platformy pre kybernetickú bezpečnosť, CECSP** (Central Europen Cyber Security Platform). Opäť sa v nej darilo nachádzať spoločné a zjednocujúce názory na aktuálne európske témy. Každoročné zasadnutie platformy bolo pod taktovkou rakúskeho predsedníctva v októbri 2019 vo Viedni. Hlavnými témami zasadnutia boli implementácia smernice NIS, bezpečnosť 5G sietí, certifikácia kybernetickej bezpečnosti a návrh na zriadenie Európskeho centra odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti a siete národných koordinačných centier. Na stretnutí bola osobitne zvýraznená dôležitosť formátu a aktuálnosť témy kybernetickej bezpečnosti v stredoeurópskom priestore. V roku 2020 platforme predsedá Maďarsko.

BILATERÁLNE PARTNERSTVÁ

Úrad v roku 2019 aktívne pôsobil v procese **realizovania bilaterálnych dohôd o výmene a ochrane utajovaných skutočností,** bez ktorých by nemohlo dochádzať k medzinárodnej výmene utajovaných skutočností, k uznávaniu bezpečnostných previerok vydaných v zahraničí a súkromný sektor by sa nemohol zúčastňovať na realizácii zákaziek, pri ktorých dochádza k postupovaniu zahraničných utajovaných skutočností. Úrad ako gestorský orgán oslovuje svojich partnerov v zahraničí a pripravuje návrhy textov dohôd, ktoré schvaľuje vláda Slovenskej republiky.

V roku 2019 sa zintenzívnili bilaterálne vzťahy úradu s českými partnermi z **Národného úradu pre kybernetickú a informačnú bezpečnosť (NÚKIB)** a **Národným bezpečnostným úradom (NBÚ).** Okrem pravidelných dvojstranných stretnutí riaditeľa úradu s českými partnermi bolo v Prahe, Brne a v Bratislave zorganizovaných viacero pracovných rokovaní k otázkam tvorby metodiky a práva v oblasti kybernetickej bezpečnosti, praktických skúseností z implementácie smernice NIS do národných legislatív. Zamerali sa aj na výmenu najnovších poznatkov o aplikačných postupoch v oblasti ochrany pred nežiaducim elektromagnetickým vyžarovaním a informácií o prístupoch uplatňovaných v oblasti šifrovej ochrany informácií.

V roku 2019 úrad pokračoval v ďalšom rozvoji dvojstranných strategických partnerstiev, a to najmä v oblasti kybernetickej bezpečnosti. Pokračoval vo vzájomnom dialógu so zástupcami francúzskej **Národnej agentúry pre kybernetickú bezpečnosť (ANSSI).** Dialóg bol podporený bilaterálnymi pracovnými stretnutiami v Paríži, Lille, v Haagu a v Bruseli. Jeho výsledkom bola konzultácia stanovísk, výmena skúseností a pohľadov, ktoré v prípade nájdenia zhody viedli k vzájomnej podpore pri tvorbe európskej politiky (legislatívny proces, 5G, atribučný proces a podobne).

Pokračovala aj spolupráca úradu s nemeckým **Federálnym úradom pre informačnú bezpečnosť (BSI),** ktorý je zároveň federálnou autoritou pre kybernetickú bezpečnosť. Okrem výmeny skúseností na bilaterálnych pracovných stretnutiach stáli úrad a BSI pri zrode novovznikajúceho formátu pravidelných stretnutí riaditeľov národných kybernetických autorít, ktorého cieľom je vytvoriť priestor pre výmenu strategických informácií na najvyššom stupni riadenia.

V roku 2019 úrad pokračoval aj v spolupráci s **americkým partnerom.** Boli obnovené rozhovory o novej bilaterálnej zmluve o vzájomnej výmene a ochrane utajovaných informácií medzi SR a USA. Prehĺbila sa ďalšia spolupráca v oblasti kybernetickej bezpečnosti. V súvislosti s brexitom sa začal dialóg s **britským partnerom** v oblasti kybernetickej bezpečnosti na ministerstve zahraničných vecí v Londýne. Prebehli prvé pracovné workshopy na aktuálne európske témy s cieľom nájsť efektívny spôsob ďalšej komunikácie po odchode Veľkej Británie z EÚ.

Medzinárodné posilnenie postavenia úradu, ktoré súvisí aj s prevádzkovaním Osobitného zahraničného pracoviska úradu v Bruseli umožnilo promptne zareagovať aj na požiadavku EÚ poskytnúť asistenciu partnerským krajinám v oblasti kybernetickej bezpečnosti. Takýmto príkladom je **aktívna spolupráca v užších formátoch,** napríklad vo formáte V4, ako aj v bilaterálnej spolupráci s jednotlivými krajinami (Fínsko a Rumunsko) na úrovni EÚ v Bruseli. Prostredníctvom osobitného pracoviska sa úrad aktívne zapájal aj do európskych dialógov na najvyššej úrovni EÚ – Čína, EÚ – Japonsko, EÚ – Ukrajina. Krajiny na nich prezentovali svoje systémy kybernetickej bezpečnosti a ochotu rozvíjať spoluprácu s EÚ a jej členskými štátmi.

V roku 2019 úrad participoval na odborných formátoch zameraných na kybernetickú bezpečnosť bankového sektora, kde sa na pozvanie holandskej národnej banky Dutch National Bank zúčastnil na pracovnom rokovaní k implementácii smernice NIS. Na základe pozvania holandského partnera z Národného centra pre kybernetickú bezpečnosť úrad participoval na jednej z najvýznamnejších medzinárodných konferencií ONE Conference 2019 v Haagu, ktorej cieľom bolo predstaviť najnovšie trendy a vývoj v oblasti kybernetickej bezpečnosti. V júni 2019 sa úrad svojou účasťou podieľal na workshope organizovanom európskou agentúrou ENISA v poľskej Varšave. Hlavnou témou bola tvorba národných stratégií kybernetickej bezpečnosti a výmena skúseností z jej implementácie. Ďalšou z významných aktivít bola medzinárodne uznávaná konferencia, ktorá sa konala v poľských Katowiciach a stretli sa na nej odborníci a spíkri z celého sveta, aby mohli diskutovať a prinášať nové pohľady na aktuálne témy kybernetickej bezpečnosti, akými sú bezpečnosť 5G sietí, umelá inteligencia, ochrana údajov v kybernetickom priestore, smart cities a podobne.

VÝMENA ZAHRANIČNÝCH INFORMÁCIÍ

Elektronizácia registrov zahraničných utajovaných skutočností z roku 2018 a ich online prepojenie s registrami orgánov verejnej moci umožňovala **bezpečnú a zároveň rýchlejšiu a flexibilnejšiu evidenciu a elektronickú distribúciu utajovaných skutočností.** V roku 2019 úrad pomáhal jednotlivým registrom utajovaných skutočností, zriadenými orgánmi verejnej moci, pri zavádzaní elektronickej evidencie utajovaných skutočností.

Prostredníctvom pracoviska centrálneho registra bolo v roku 2019 spracovaných **9 208 utajovaných skutočností NATO a 3 935 utajovaných skutočností EÚ.** Úrad sprostredkoval aj výmenu 145 utajovaných skutočností cudzej moci. Prehľad činnosti centrálneho registra v roku 2019 a porovnanie údajov s rokmi 2017 a 2018 je uvedený v tabuľke č. 4. Úrad prevádzkoval aj **register utajovaných skutočností NATO Atomal.** V roku 2019 v ňom neboli zaevidované žiadne utajované písomnosti označené stupňom utajenia NATO Secret Atomal.

Tabuľka č. 4: Výmena utajovaných písomností v rokoch 2017 – 2019

Stupeň utajenia	2017	2018	2019
NATO Restricted	2778	2371	4870
EU Restricted	4453	3773	2374
Cudzia moc Vyhradené	84	60	53
NATO Confidential	1576	1 851	1 847
EU Confidential	334	588	1131
Cudzia moc Dôverné	13	85	62
NATO Secret	2367	1837	2491
EU Secret	79	208	430
Cudzia moc Tajné	5	24	14
NATO Top Secret	0	0	0
EU Top Secret	0	0	0
Cudzia moc Prísne tajné	6	16	16
NATO spolu	**6721**	**6 059**	**9 208**
EU spolu	**4866**	**4 569**	**3 935**
Cudzia moc spolu	**108**	**185**	**145**

3.3 OCHRANA UTAJOVANÝCH SKUTOČNOSTÍ

V roku 2019 **nevznikli žiadne mimoriadne udalosti a okolnosti,** ktoré by narúšali systém zabezpečenia ochrany utajovaných skutočností v Slovenskej republike. Rada Európskej únie vykonala v septembri 2019 v SR inšpekciu ochrany utajovaných skutočností. Jej oficiálne výsledky neboli zatiaľ spracované. Európski inšpektori vo svojich predbežných záveroch pozitívne hodnotili nastavenie systému a pôsobenie jeho jednotlivých prvkov. Celkovo konštatovali vysokú úroveň zabezpečenia ochrany utajovaných skutočností v SR. Organizácia Severoatlantickej zmluvy avizovala vykonanie podobnej inšpekcie v roku 2020.

PERSONÁLNA BEZPEČNOSŤ

Vykonávanie bezpečnostných previerok fyzických osôb patrí ku kľúčovým činnostiam úradu. Úrad v roku 2019 vydal **4 268 osvedčení na oboznamovanie sa s utajovanými skutočnosťami,** z toho 2 248 pre rezort obrany. Prehľad počtu vydaných osvedčení v rokoch 2017 až 2019 je uvedený v tabuľke č. 5.

Tabuľka č. 5: Prehľad osvedčení vydaných v rokoch 2017 – 2019

Stupeň utajenia	2017	2018	2019
Dôverné	**3 060**	**2 728**	**2 166**
z toho Dôverné pre MO SR	1 308	780	730
Tajné	**1 590**	**1 700**	**1 807**
z toho Tajné pre MO SR	1 029	1 308	1 351
Prísne Tajné	**377**	**297**	**295**
z toho Prísne Tajné pre MO SR	212	154	167
Spolu	**5 027**	**4 725**	**4 268**

V roku 2019 úrad vydal **28 rozhodnutí** a fyzické osoby podali **14 odvolaní** proti rozhodnutiu úradu. Ani v jednom prípade úrad nerozhodol v autoremedúre. Výbor Národnej rady Slovenskej republiky na preskúmavanie rozhodnutí Národného bezpečnostného úradu (ďalej len „výbor“) rozhodoval o 13 odvolaniach, pričom vo všetkých prípadoch odvolanie zamietol. K 31. decembru 2019 sa jedno odvolanie nachádzalo v štádiu odvolacieho procesu.

Proti rozhodnutiu výboru bola na Najvyšší súd Slovenskej republiky (ďalej len „najvyšší súd“) podaná jedna žaloba, ktorá je v procese rozhodovania. Okrem uvedeného najvyšší súd v roku 2019 rozhodoval v piatich konaniach, v ktorých boli žaloby podané v predchádzajúcom období. V štyroch prípadoch najvyšší súd žalobu zamietol. V jednom prípade najvyšší súd konanie zastavil z dôvodu späťvzatia žaloby. Prehľad informácií o rozhodnutiach úradu, odvolaniach a žalobách podaných na najvyšší súd sa nachádza v tabuľke č. 6.

Tabuľka č. 6: Rozhodnutia úradu, odvolania fyzických osôb proti rozhodnutiam úradu a žaloby v rokoch 2017 – 2019

	2017	2018	2019
Rozhodnutia úradu	**28**	**20**	**28**
Odvolania	**12**	**10**	**14**
Odvolania – autoremedúra	0	1	0
Odvolania zamietnuté výborom	14	9	13
Rozhodnutia zrušené výborom	1	1	0
Podané žaloby na najvyššom súde	4	1	1

Vo vzťahu k **utajovaným skutočnostiam postupovaným NATO a EÚ** bolo navrhovaným osobám v roku 2019 vydaných **4 104 certifikátov**, z toho bolo vydaných 2 067 certifikátov NATO a 2 037 certifikátov EÚ. Z celkového počtu certifikátov NATO úrad vydal 22 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 2019 úrad vydal **109 potvrdení o priemyselnej bezpečnosti,** z toho 10 potvrdení stupňa utajenia Vyhradené, 76 potvrdení stupňa utajenia Dôverné, 22 potvrdení stupňa utajenia Tajné a jedno potvrdenie stupňa utajenia Prísne tajné. Prehľad uvádzaných údajov sa nachádza v tabuľke č. 7.

Tabuľka č. 7: Prehľad potvrdení o priemyselnej bezpečnosti vydaných v rokoch 2017 – 2019

Stupeň utajenia	2017	2018	2019
Vyhradené	3	4	10
Dôverné	60	50	76
Tajné	14	16	22
Prísne tajné	0	3	1
Spolu	**77**	**73**	**109**

Úrad v roku 2019 vydal **23 rozhodnutí.** Odvolanie proti rozhodnutiu úradu podalo päť podnikateľov. V dvoch prípadoch rozhodol úrad v autoremedúre a o dvoch odvolaniach rozhodoval výbor, ktorý odvolania podnikateľov zamietol. K 31. decembru 2019 sa jedno odvolanie nachádzalo v štádiu odvolacieho procesu. Ani v jednom prípade nebola podaná žaloba na najvyšší súd. Prehľad uvádzaných údajov sa nachádza v tabuľke č. 8.

Tabuľka č. 8: Rozhodnutia úradu, odvolania podnikateľov proti rozhodnutiam úradu a žaloby v rokoch 2017 – 2019

	2017	2018	2019
Rozhodnutia úradu	**13**	**24**	**23**
Odvolania	**2**	**6**	**5**
Odvolania - autoremedúra	1	3	2
Odvolania zamietnuté výborom	1	3	2
Rozhodnutia zrušené výborom	0	0	0
Podané žaloby na najvyššom súde	0	1	0

Vo vzťahu k utajovaným skutočnostiam NATO a EÚ bolo v roku 2019 podnikateľom vydaných **12 certifikátov NATO a 12 certifikátov EÚ**, ktoré oprávňujú podnikateľov oboznamovať sa s utajovanými skutočnosťami NATO, resp. EÚ.

Úrad má uzatvorených **13 zmlúv o prístupe podnikateľa** k utajovaným skutočnostiam, v roku 2019 úrad uzatvoril deväť zmlúv a päť dodatkov k uzatvoreným zmluvám.

ADMINISTRATÍVNA BEZPEČNOSŤ

V súlade so zákonom o ochrane utajovaných skutočností úrad zabezpečil v roku 2019 prevzatie utajovaných skutočností od jedného subjektu bez právneho nástupcu, odňatie utajovaných skutočností nepovolanej osobe a vykonal úkony potrebné na zabezpečenie ich ochrany.

V roku 2019 úrad prijal a odoslal 3 909 utajovaných písomností. Porovnanie počtu písomností zaevidovaných v protokole utajovaných písomností sa nachádza v tabuľke č. 10.

Tabuľka č. 10: Počet utajovaných písomností spracovaných na úrade v rokoch 2017 – 2019

Stupeň utajenia	2017	2018	2019
Vyhradené	3 439	3 201	3 655
Dôverné	290	216	247
Tajné	4	4	7
Prísne tajné	0	0	0
Spolu	**3 733**	**3 421**	**3 909**

FYZICKÁ BEZPEČNOSŤ A OBJEKTOVÁ BEZPEČNOSŤ

Úrad v roku 2019 posudzoval opatrenia fyzickej bezpečnosti a objektovej bezpečnosti na ochranu utajovaných skutočností podnikateľov, ktorí prechádzali bezpečnostnou previerkou. Vykonaných bolo 49 posúdení a vydané tri súhlasy so zriadením registra utajovaných skutočností.

V roku 2019 úrad vydal 86 certifikátov mechanických zábranných prostriedkov a technických zabezpečovacích prostriedkov.

OCHRANA PRED NEŽIADUCIM ELEKTROMAGNETICKÝM VYŽAROVANÍM

Pri opatreniach na zabezpečenie ochrany utajovaných skutočností pred únikom prostredníctvom nežiaduceho elektromagnetického vyžarovania úrad v roku 2019 vykonával zónové merania priestorov a merania technických prostriedkov a prostriedkov šifrovej ochrany informácií v špecializovanom TEMPEST laboratóriu. Na základe doručených žiadostí bolo vykonaných 876 meraní zariadení technických prostriedkov a prostriedkov ŠOI a 47 zónových meraní priestorov, na základe ktorých bolo kategorizovaných 241 zariadení TP a 31 priestorov. V roku 2019 bola prijatá jedna žiadosť o vykonanie meraní tienených komôr, na základe ktorej bolo vykonaných šesť meraní útlmu tienenej komory.

BEZPEČNOSŤ TECHNICKÝCH PROSTRIEDKOV

V roku 2019 úrad vydal 67 certifikátov technických prostriedkov a 25 dodatkov.

Tabuľka č. 9: Počet vydaných certifikátov v rokoch 2017 – 2019

Stupeň utajenia	2017	2018	2019
Vyhradené	5	7	24
Dôverné	28	22	37
Tajné	7	12	6
Prísne tajné	0	1	0
Spolu	**40**	**42**	**67**
Dodatky	16	19	25

AKREDITÁCIA KOMUNIKAČNÝCH A INFORMAČNÝCH SYSTÉMOV

V roku 2019 úrad vykonal dve aktualizácie akreditácie komunikačného a informačného systému BICES pre dočasné nasadenie technických prostriedkov pre manipuláciu utajovaných informácií NATO v súlade s Bezpečnostnou politikou NATO C-M(2002)49. Ďalej boli akreditované tri systémy pre EÚ v súlade s Rozhodnutím rady (2013/488/EÚ) a jeden systém v súlade s Bezpečnostnou politikou NATO C-M(2002)49.

ELEKTRONIZÁCIA SLUŽIEB ÚRADU

V roku 2019 úrad implementoval národný projekt Vybudovania **informačného systému pre elektronizáciu služieb úradu** v oblastiach ochrany utajovaných skutočností a interných procesov úradu. Projekt priniesol lepšie a bezpečnejšie prostredie pre prácu s utajovanými skutočnosťami a zároveň zredukoval existujúce obmedzenia pri práci s utajovanými skutočnosťami. Bola dosiahnutá modernizácia hardvérovej infraštruktúry, pomocou ktorej sa podarilo zabezpečiť vyššiu mieru bezpečnosti informačného systému, zlepšiť východiská pre sledovanie prevádzkových ukazovateľov prostredí, zvýšiť kvalitu dostupnosti a spoľahlivosti jednotlivých prostredí, vytvoriť lepšie pracovné prostredie s kratšími časovými odozvami a zvýšiť efektivitu práce, zvýšiť kvalitu jednotlivých prostredí z hľadiska dostupnosti a spoľahlivosti. Vybudovaná architektúra v budúcnosti umožní ďalší rozvoj systému. V roku 2020 bude vybudovaný systém certifikovaný podľa vyhlášky č. 339/2004 Z. z. o bezpečnosti technických prostriedkov.

ŠKOLIACA A OVEROVACIA ČINNOSŤ

V realizácii **Koncepcie budovania bezpečnostného povedomia** v oblasti ochrany utajovaných skutočností úrad v roku 2019 pokračoval v sérii **prednášok a školení zameraných na jednotlivé bezpečnostné oblasti.** Úrad vykonával aj skúšky **bezpečnostného zamestnanca** a v roku 2019 úspešným absolventom vydal **276 potvrdení** o vykonaní skúšky.

3.4 ŠIFROVÁ OCHRANA INFORMÁCIÍ

Systém šifrovej ochrany je v Slovenskej republike založený na overenej štruktúre rezortných šifrových orgánov a ich úzkej spolupráci s úradom, ktorý plní rolu ústredného šifrového orgánu. Úrad v roku 2019 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.

ŠIFROVÉ A TECHNICKÉ PROSTRIEDKY

Úrad v roku 2019 vydal **11 certifikátov prostriedkov ŠOI** a jeden dodatok k certifikátu prostriedku ŠOI.

V roku 2019 bol aktualizovaný technický prostriedok na bezpečnú komunikáciu pracovných staníc a mobilných zariadení v stupni utajenia Vyhradené. V systéme bolo zriadených 32 nových užívateľských účtov. Úrad pokračoval v priebežnej distribúcii **technických prostriedkov** použiteľných na bezpečnú výmenu informácií medzi vládnymi inštitúciami v režime stupňa utajenia Dôverné a Tajné. V rámci zabezpečenia vládneho spojenia boli tieto technické prostriedky dodané 33 registrom vládnych inštitúcií. Dodané technické prostriedky nahradili staršie prostriedky ŠOI, ktorým sa skončila platnosť certifikátov.

ELEKTRONICKÝ PROTOKOL

V roku 2019 bol v plnej prevádzke **elektronický protokol** utajovaných skutočností. Systém upravený internými zdrojmi prináša rýchlejšiu a flexibilnejšiu evidenciu utajovaných skutočností. Pred samotným spustením prebehli školenia pracovníkov registrov jednotlivých orgánov verejnej moci a počas troch mesiacov bola v prevádzke aj testovacia verzia produktu. Počas roka 2019 bol postavený segment „D“, „T“ a „TN“. Tieto segmenty zastrešujú online komunikáciu v danom stupni utajenia (DÔVERNÉ, TAJNÉ a TAJNÉ - NATO). Tieto segmenty boli certifikované a segment „D“ bol spustený do prevádzky.

3.5 KYBERNETICKÁ BEZPEČNOSŤ

Na rastúcu dynamiku kybernetických hrozieb, sofistikovanosť a flexibilitu útočníkov v roku 2019 bolo potrebné reagovať zavádzaním vhodných **legislatívnych podmienok,** budovaním **inštitucionálneho rámca,** posilňovaním **personálnych kapacít,** implementáciou najnovších **technologických riešení** a **intenzívnou spoluprácou** na vnútroštátnej i medzinárodnej úrovni.

NÁRODNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI SK-CERT

V súlade s Akčným plánom realizácie Koncepcie kybernetickej bezpečnosti SR 2015 – 2020 zriadil úrad 1. septembra 2019 **Národné centrum kybernetickej bezpečnosti SK-CERT (NCKB).** Centrum vzniklo transformáciou národnej jednotky na riešenie kybernetických bezpečnostných incidentov (CSIRT), ktorú úrad prevádzkuje v súlade so zákonom o kybernetickej bezpečnosti od roku 2018. NCKB 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.

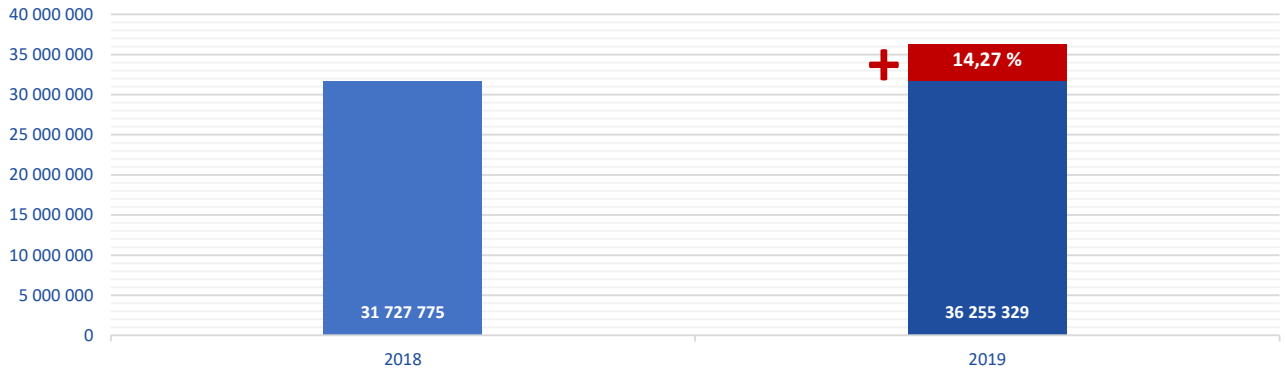
REGISTRE PREVÁDZKOVATEĽOV A POSKYTOVATEĽOV SLUŽIEB

V roku 2019 bolo do **registra prevádzkovateľov základných služieb** zaradených 142 prevádzkovateľov základných služieb, z toho 37 prevádzkovateľov základnej služby ako informačného systému verejnej správy. Počet **poskytovateľov digitálnej služby** sa v roku 2019 zvýšil o dvoch. V roku 2018 bolo do registra prevádzkovateľov základných služieb zaradených 100 prevádzkovateľov základných služieb, z toho 43 prevádzkovateľov základnej služby ako informačného systému verejnej správy.

BEZPEČNOSTNÉ INCIDENTY

Úrad prostredníctvom SK-CERT v rámci preventívnych aktivít pokračoval v distribúcii **bezpečnostných varovaní** a týždenných bezpečnostných bulletinov, ktoré obsahovali adresné upozornenia na aktuálne bezpečnostné incidenty, hrozby, zraniteľnosti a ďalšie relevantné informácie. V roku 2019 bolo zaevidovaných **36 255 329 kybernetických bezpečnostných incidentov,** teda v priemere viac ako tri milióny incidentov mesačne. V porovnaní s rokom 2018 došlo k nárastu evidovaných incidentov o 14,27 %. **Riešených bolo 8 815** incidentov, teda o 60,2 % viac ako v roku 2018. Údaje sú vizuálne znázornené v grafoch č. 1 a 2.

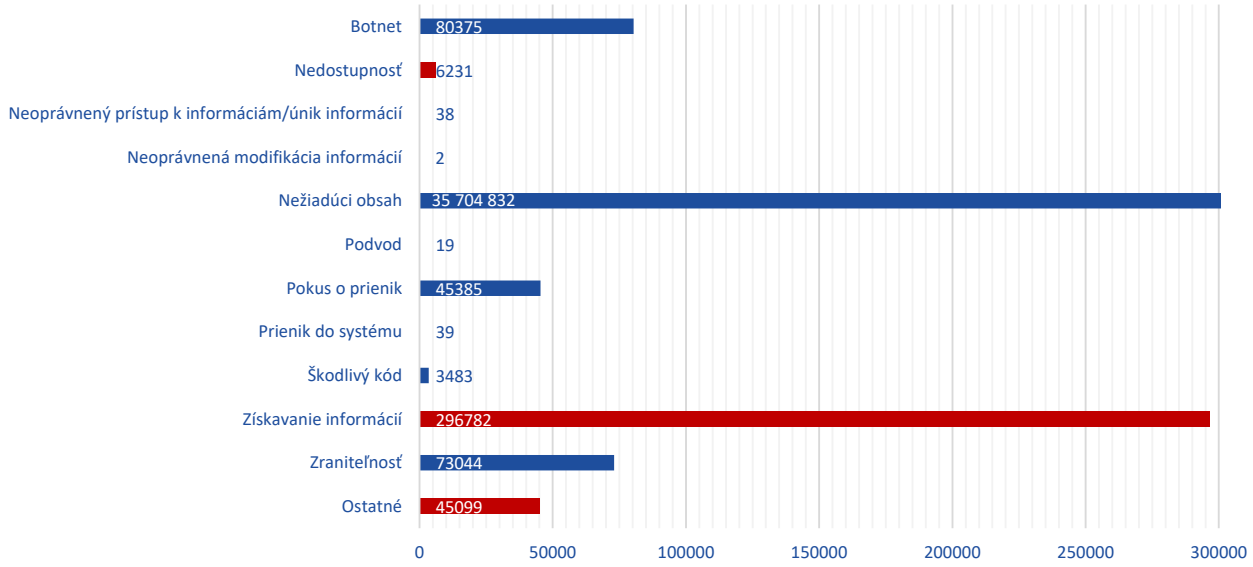
Graf č. 1: Nárast počtu evidovaných incidentov v roku 2019



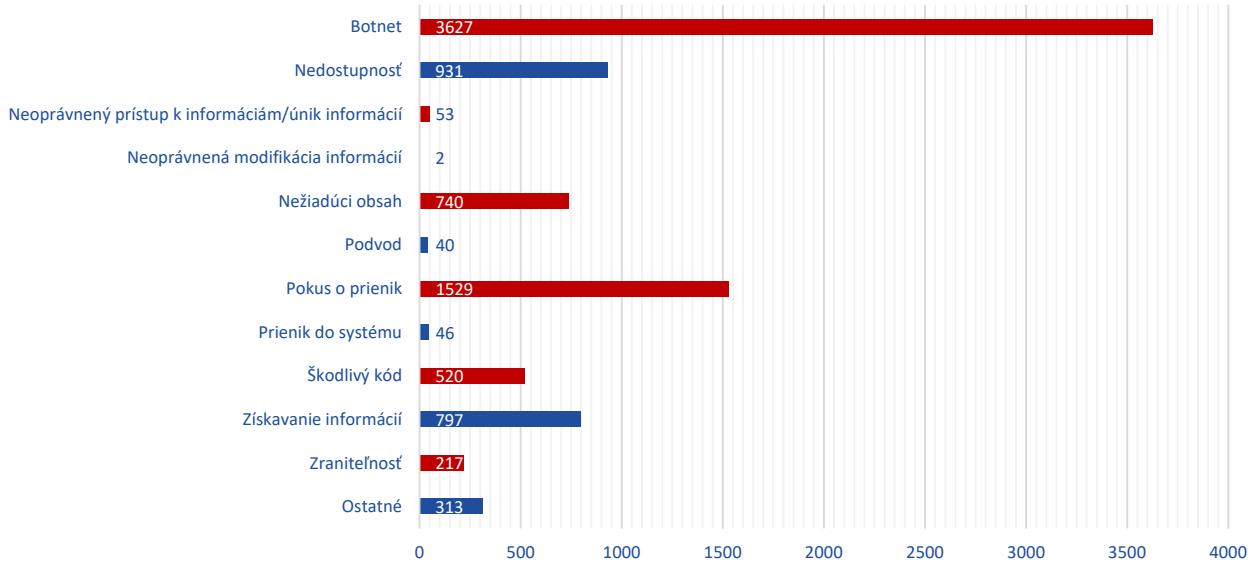
Graf č. 2: Nárast počtu riešených incidentov v roku 2019

Najpočetnejšiu skupinu incidentov predstavovali útoky využívajúce **nástroje sociálneho inžinierstva,** najmä phishingový obsah. Druhú najväčšiu skupinu incidentov reprezentovali útoky, pri ktorých boli zneužívané zastarané, neaktualizované, nesprávne nainštalované, či všeobecne **zle zabezpečené systémy.** Zvyšovanie počtu kybernetických bezpečnostných incidentov kopíruje celosvetový trend, týka sa všetkých sektorov, ale aj bežných ľudí.

Graf č. 3: Prehľad evidovaných incidentov podľa typu útoku



Graf č. 4: Prehľad riešených incidentov podľa typu útoku



V októbri 2019 vydal SK-CERT **Návod na oznamovanie zraniteľností,** ktorý slúži ako pomôcka pre bezpečnostných výskumníkov, vývojárov softvéru, výrobcov hardvéru a zariadení, ale aj pre verejnosť. V návode sa uvádza podrobný postup a odporúčané kroky pri oznamovaní novoobjavených zraniteľností, ako aj postup pri oznamovaní už existujúcich zraniteľností nájdených v prevádzkovaných systémoch a službách.

BUDOVANIE TECHNICKÝCH SPÔSOBILOSTÍ

V roku 2019 úrad pokračoval s budovaním **softvérového a hardvérového** vybavenia SK-CERT umožňujúceho zabezpečiť efektívny výkon bezpečnostného a prevádzkového monitoringu, sledovania, detekcie a vyhodnocovania kybernetických incidentov a hrozieb na národnej úrovni. Vybudovanie **modernej infraštruktúry** je dôležitým aspektom pre vytvorenie optimálnych podmienok vysokej úrovne kybernetickej bezpečnosti nielen na pracovisku SK-CERT, ale implementáciou najnovších technologických trendov v **národnom kybernetickom priestore.**

Úrad v roku 2019 začal realizovať **projekt budovania Národného systému riadenia incidentov** kybernetickej bezpečnosti vo verejnej správe, ktorý je spolufinancovaný z Európskeho fondu regionálneho rozvoja. Hlavným cieľom projektu je dobudovanie a zvýšenie kapacít infraštruktúr jednotky SK-CERT, ako aj dobudovanie špecializovaných

pracovísk pre komplexné riešenie riadenia incidentov v zmysle legislatívne vymedzených kompetencií a zákonných povinností jednotiek CSIRT. Projektové aktivity sú v súčasnosti v štádiu implementácie s predpokladaným ukončením projektu do konca roka 2020.

Do štádia prípravy sa v roku 2019 dostal **projekt na vybudovanie Centra simulácie, výskumu a výuky** kybernetických hrozieb a kybernetickej bezpečnosti. Úrad pristúpil k uzavretiu zmluvy o partnerstve, v zmysle ktorej bude v rámci projektu, s podporou európskych zdrojov, realizovať oprávnené aktivity s predpokladaným ukončením v júli 2021.

CERTIFIKÁCIA KYBERNETICKEJ BEZPEČNOSTI

V súlade so zámerom úradu naďalej rozširovať svoje kapacity boli v roku 2019 vykonané počiatočné kroky v oblasti certifikácie kybernetickej bezpečnosti. V programe EÚ CEF Telecom 2019 úrad na jeseň 2019 vypracoval **projekt Cybersecurity Certification Slovakia,** ktorý by mal úradu pomôcť s realizáciou zámeru vykonávať v Slovenskej republike akreditáciu certifikačných laboratórií kybernetickej bezpečnosti podľa legislatívy EÚ a podľa princípov a postupov celosvetovo uznávaného certifikačného rámca CCRA. Projekt zahŕňa technické oblasti certifikácie, akreditácie a auditu a počíta aj so vzájomnou podporou a výmenou najlepších postupov a ďalších relevantných informácií so zahraničnými partnerskými organizáciami. Oznámenie EK o schválení/neschválení financovania projektu sa očakáva v júni 2020.

POSILŇOVANIE PERSONÁLNYCH KAPACÍT

Snaha o vytváranie optimálnych technických podmienok je úzko spätá aj s personálnym zabezpečením SK-CERT. Personálny stav jednotky smeruje k ustáleniu jednotlivých rolí pracovníkov, aj keď je veľkou výzvou priamo obsadiť pozície **kvalifikovanými odborníkmi** či absolventmi škôl. V kybernetickej oblasti slovenské školy a akademická oblasť nepripravujú študentov na magisterskej či doktorandskej úrovni. SK-CERT využíva dostupné kapacitné modely tak, aby bolo možné pokryť všetky služby, ktoré musí jednotka poskytovať a zároveň akceptovateľne rozvíjať spôsobilosti úradu v tejto oblasti.

Dôležitou súčasťou neustáleho vylepšovania spôsobilostí úradu v oblasti riešenia kybernetických bezpečnostných incidentov je aj pravidelný praktický tréning v podobe účasti na **kybernetických cvičeniach** ako sú **LockedShield**, **SecOps Europe, Cyber Europe, Cyber Coalition** alebo **CyberEx**. Pri cvičeniach SK-CERT úzko spolupracoval s Ozbrojenými silami Slovenskej republiky, Policajným zborom Slovenskej republiky, Národnou agentúrou pre sieťové a elektronické služby, organizáciou CSIRT.sk a s inými štátnymi orgánmi či inštitúciami.

ROZŠIROVANIE SPOLUPRÁCE

Kybernetická bezpečnosť je najmä o dobre fungujúcej spolupráci medzi partnermi a subjektmi, ktoré zabezpečujú čiastkové úlohy v tejto oblasti. V roku 2019 došlo k **zintenzívneniu spolupráce na úrovni rezortov,** konkrétne medzi úradom, Úradom podpredsedu vlády Slovenskej republiky pre investície a informatizáciu, Národnou agentúrou pre sieťové a elektronické služby Slovenskou informačnou službou, Vojenským spravodajstvom Ministerstva obrany Slovenskej republiky a Ministerstvom zahraničných vecí a európskych záležitostí Slovenskej republiky. Intenzívna komunikácia a spolupráca prebiehala **s prevádzkovateľmi základných služieb, poskytovateľmi digitálnych služieb a súkromnými jednotkami CSIRT.** Úrad jednotlivým subjektom poskytoval metodickú pomoc pri uplatňovaní zásad zákona o kybernetickej bezpečnosti a konzultácie o praktických problémoch pri implementácii zákonných požiadaviek. Takýmto spôsobom bola získavaná aj spätná väzba, na základe ktorej môže úrad v budúcnosti poskytovať kvalitnejšie služby. Uzatvorené memorandá o spolupráci medzi úradom a **profesijnými združeniami,** najmä Asociáciou kybernetickej bezpečnosti, ISACA Slovensko, Združením bezpečnostného a obranného priemyslu a občianskym združením AFCEA Slovakia, otvárajú priestor na realizáciu zámeru úradu prepájať odborníkov z verejnej aj súkromnej sféry a odštartovať efektívnu a otvorenú diskusiu k spoločným prienikom v oblasti kybernetickej bezpečnosti.

Úrad v roku 2019 intenzívne rozvíjal aj medzinárodnú spoluprácu v oblasti kybernetickej bezpečnosti. Podrobné informácie sú uvedené v kapitole 3.2 Medzinárodná spolupráca**.**

BUDOVANIE BEZPEČNOSTNÉHO POVEDOMIA

Boli realizované aj aktivity v oblasti šírenia bezpečnostného povedomia. Úrad opakovane odporúčal dodržiavať **minimálne štandardy kybernetickej hygieny,** zverejňoval univerzálne platné rady a návody na to, **ako sa správať bezpečne na internete** a ako chrániť osobné a citlivé údaje používateľov. V roku 2019 zorganizoval aj sériu národných table-top cvičení pre prevádzkovateľov základných služieb a vybrané organizácie verejnej správy. Boli orientované na **tréning manažérskeho rozhodovania** organizácií pri kybernetických incidentoch a ich účastníci boli zapojení do riešenia fiktívnych kybernetických incidentov s hypotetickými udalosťami, na ktoré museli reagovať tak, ako by sa naozaj stali. Mali možnosť otestovať účinnosť vlastných postupov a procesov, absolvovať trénovanie úloh a zodpovedností jednotlivých rolí a manažérskeho rozhodovania.

KOMPETENČNÉ A CERTIFIKAČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI

V decembri 2019 úrad získal súhlas Ministerstva financií Slovenskej republiky na zriadenie príspevkovej organizácie, **Kompetenčného a certifikačného centra kybernetickej bezpečnosti** centra, ktoré zahájilo činnosť 1. januára 2020. Vznik kompetenčného centra vychádza z návrhu európskeho nariadenia na zriadenie Európskeho centra odvetvových,

technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti a vytvorenie siete národných koordinačných centier. Tematicky vychádza aj z návrhu nariadenia o zriadení programu Digitálna Európa a zo Stratégie digitálnej transformácie schválenej vládou SR v roku 2019.

Pôsobnosť kompetenčného centra (od 1. januára 2020) pokryje plnenie úloh národného odvetvového, technologického a výskumného centra v oblasti kybernetickej bezpečnosti, konkrétne na plnenie úloh certifikačného orgánu podľa zákona o kybernetickej bezpečnosti, činnosti autorizovanej osoby podľa zákona o ochrane utajovaných skutočností, zabezpečenie služieb súvisiacich s organizáciou a technickým zabezpečením vzdelávacích aktivít pre zriaďovateľa, zónové merania a merania nežiaduceho elektromagnetického vyžarovania, vykonávanie znaleckej a expertíznej činnosti, vykonávanie vedeckej, výskumnej činnosti a vývoja v oblasti kybernetickej bezpečnosti a informačno-komunikačných technológií a konzultačnú činnosť v oblasti ochrany utajovaných skutočností, kybernetickej bezpečnosti a dôveryhodných služieb, organizovanie vzdelávacích podujatí, kurzov, školení a seminárov.

3.6 DÔVERYHODNÉ SLUŽBY

V súlade s nariadením eIDAS, zákonom o dôveryhodných službách a schémou dohľadu úrad vykonáva **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 v nariadení eIDAS.

V roku 2019 úrad vydal **jeden certifikát zariadenia na vyhotovenie kvalifikovaných elektronických podpisov a pečatí.** Úradu bola doručená jedna **žiadosť o certifikáciu bezpečného produktu pre kvalifikovaný elektronický podpis,** konanie však bolo zastavené z dôvodu certifikácie uvedeného zariadenia v inej krajine Európskej únie a jeho zverejnením v zozname certifikovaných kvalifikovaných zariadení na vyhotovenie elektronických podpisov Európskej komisie.

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 2019 úrad publikoval 12 verzií dôveryhodného zoznamu.

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 2019 bolo na základe žiadostí štátnych orgánov a orgánov územnej samosprávy do zoznamu zapísaných 17 nových oprávnení. V priebehu roka úrad publikoval osem verzií zoznamu oprávnení. Jeho aktuálna verzia bola vždy doplnená archívom predchádzajúcich verzií.

NOVÉ DÔVERYHODNÉ SLUŽBY

Úrad prijal oznámenie od **troch kvalifikovaných poskytovateľov o zámere poskytovať kvalifikovanú dôveryhodnú službu** vydávania kvalifikovaných elektronických časových pečiatok. Oznámenie boli poskytovatelia povinní predložiť so záverečnou správou o posúdení zhody. Celkovo bolo udelených **30 kvalifikovaných štatútov** na kvalifikovanú dôveryhodnú službu. Úrad v roku 2019 posúdil a vyhovel žiadostiam troch kvalifikovaných poskytovateľov dôveryhodných služieb o rozšírenie existujúcich kvalifikovaných služieb o službu OCSP (Online Certificate Status Protocol). Zároveň boli v roku 2019 kvalifikovanými poskytovateľmi dôveryhodných služieb predložené orgánu dohľadu štyri správy o posúdení zhody vykonané orgánom posudzovania zhody do 24 mesiacov od vykonania posledného auditu, ktoré potvrdzujú, že kvalifikovaní poskytovatelia dôveryhodných služieb a kvalifikované dôveryhodné služby, ktoré poskytujú spĺňajú požiadavky stanovené v nariadení eIDAS.

TVORBA MEDZINÁRODNÝCH NORIEM

Pri tvorbe medzinárodných technických noriem použiteľných pre implementáciu nariadenia eIDAS bol príslušník úradu projektovým vedúcim pre ISO 14533-4 v rámci ISO TC 154. Vďaka jeho aktívnej účasti na plnení povinností vyplývajúcich z tejto funkcie bol 27. augusta 2019 vydaný štandard ISO/DIS 14533-4, do ktorého boli zahrnuté aj požiadavky zo schémy dohľadu, ktorú úrad vydal ako zoznam odporúčaných technických postupov implementácie legislatívnych požiadaviek definovaných v nariadení eIDAS pre kvalifikované dôveryhodné služieb, pre ktoré komisia nevydala voliteľné implementačné akty.

DÔVERYHODNÁ INFRAŠTRUKTÚRA

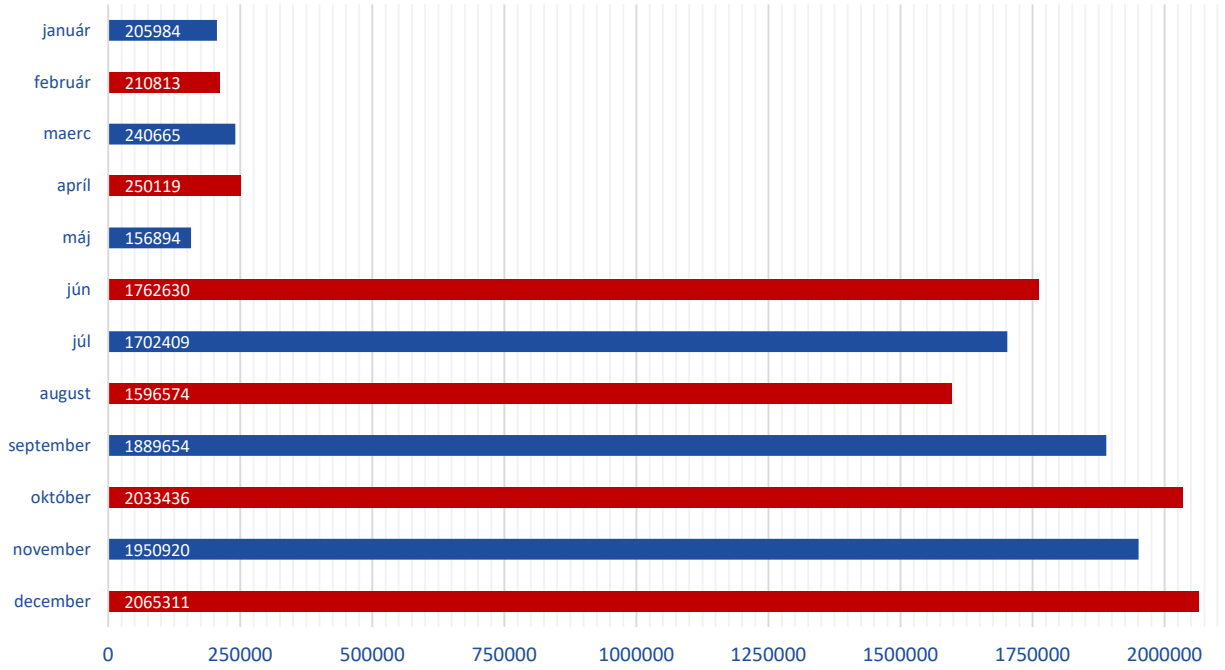
Úrad prevádzkuje v rámci dôveryhodnej infraštruktúry **koreňovú certifikačnú autoritu Slovenskej republiky,** ktorá vydáva certifikáty verejných kľúčov a vedie dlhodobú databázu vydaných kvalifikovaných certifikátov s ich stavom platnosti, vydaných poskytovateľmi, ktorým úrad udelil kvalifikovaný štatút.

SLOVENSKÁ NÁRODNÁ CERTIFIKAČNÁ AUTORITA

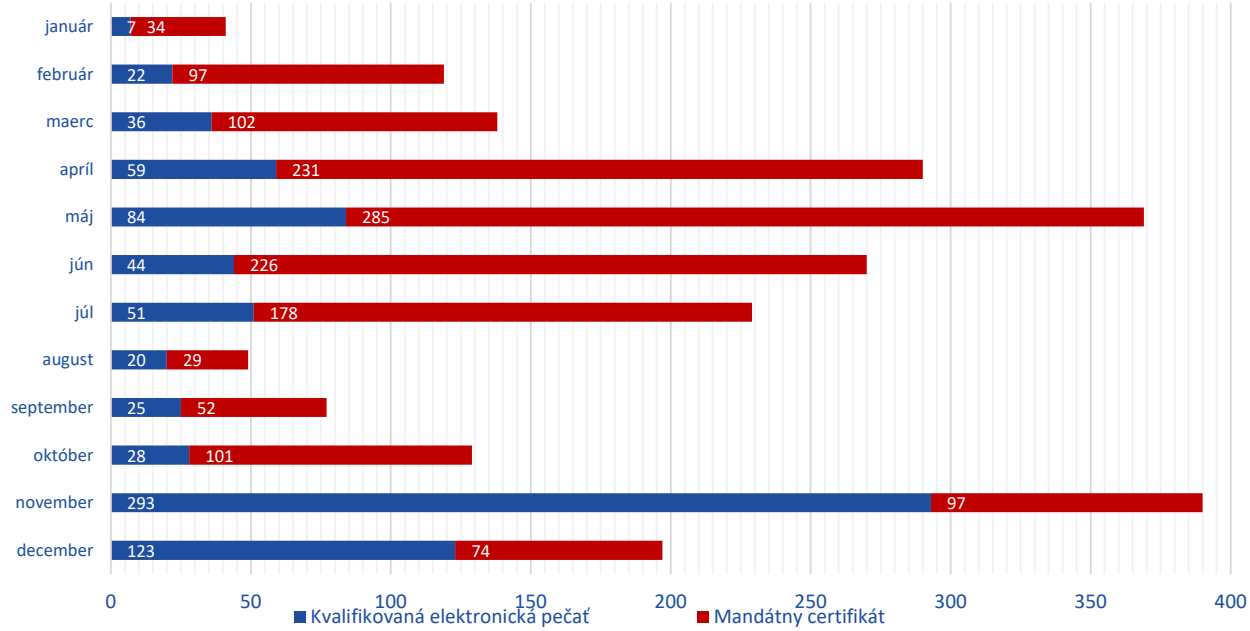
V roku 2019 úrad prostredníctvom Slovenskej národnej certifikačnej autority (SNCA) bezodplatne poskytoval **kvalifikované dôveryhodné služby orgánom verejnej moci.** SNCA zabezpečovala kvalifikovanú dôveryhodnú službu vyhotovovania a overovania kvalifikovaných certifikátov pre elektronickú pečať, kvalifikovanú dôveryhodnú službu vyhotovovania kvalifikovaných elektronických časových pečiatok a kvalifikovanú dôveryhodnú službu vyhotovovania a overovania kvalifikovaných certifikátov pre elektronický podpis, vrátane vydávania mandátnych certifikátov.

Počet vyhotovených kvalifikovaných elektronických časových pečiatok a vydaných kvalifikovaných certifikátov pre orgány verejnej moci mal počas roku 2019 rastúcu tendenciu. Trend je znázornený v grafoch č. 5 a 6.

Graf č. 5: Počet časových pečiatok vydaných v roku 2019



Graf č. 6: Počet kvalifikovaných certifikátov vydaných v roku 2019



Poskytovanie služieb SNCA bolo v súlade s novelou zákona o dôveryhodných službách 1. augusta 2019 prevedené na Národnú agentúru pre sieťové a elektronické služby (NASES). Úrad v ďalšom období poskytoval agentúre plnú súčinnosť a podporu prevádzky prevzatých služieb SNCA.

4. HOSPODÁRENIE

V súlade so zákonom č. 370/2018 Z. z. o štátnom rozpočte na rok 2019 z 5. decembra 2010 boli schválené záväzné ukazovatele štátneho rozpočtu jednotlivých kapitol na rok 2019 vrátane NBÚ.

ROZPIS ZÁVÄZNÝCH UKAZOVATEĽOV ROZPOČTU

Rozpis záväzných ukazovateľov rozpočtu kapitoly 41 – Národný bezpečnostný úrad, vplyv rozpočtových opatrení na výšku rozpočtu k 31. decembru 2019 a porovnanie čerpania finančných prostriedkov k upravenému rozpočtu k 31. decembru 2019 je uvedený v tabuľke č. 11.

Tabuľka č. 11: Rozpočet úradu v roku 2019

	Schválený rozpis	Upravený rozpočet	Skutočnosť	Plnenie k upravenému rozpočtu
I. Príjmy kapitoly	**22 000,00 €**	**13 955,72 €**	**18 801,17 €**	**134,72%**
A. Záväzný ukazovateľ (zdroj 111)	20 000,00 €	11 955,72 €	12 300,72 €	102,89%
Kód zdroja 72e	2 000,00 €	2 000,00 €	257,16 €	12,86%
Kód zdroja 131I	0,00 €	0,00 €	5 191,74 €	-
Kód zdroja 11O1	0,00 €	0,00 €	1 051,55 €	-
B. Prostriedky Európskej únie	0,00 €	0,00 €	0,00 €	0,00%
II. Výdavky kapitoly celkom (A + B + C)	**10 120 423,00 €**	**21 316 947,94 €**	**20 908 220,89 €**	**98,08%**
A. Výdavky spolu bez prostriedkov podľa § 17 ods. 4 zákona č. 523/2004 Z. z. a prostriedkov Európskej únie, z toho	10 118 423,00 €	14 892 418,33 €	14 485 567,52 €	97,27%
A.1 Prostriedky štátneho rozpočtu (zdroj 111)	10 118 423,00 €	10 695 702,22 €	10 290 845,39 €	96,21%
Kód zdroja 131H	0,00 €	2 039 196,97 €	2 037 202,99 €	100,00%
Kód zdroja 131I	0,00 €	50 000,00 €	50 000,00 €	100,00%
A.2 Prostriedky na spolufinancovanie	0,00 €	2 107 519,14 €	2 107 519,14 €	100,00%
Kód zdroja 3AA2		1 133 387,56 €	1 133 387,56 €	100,00%
Kód zdroja 3AA3		974 131,58 €	974 131,58 €	100,00%
A.3 Mzdy, platy, služobné príjmy a ostatné osobné vyrovnania (610), (kód zdroja 111)	5 413 246,00 €	5 970 879,00 €	5 748 209,13 €**	96,27%
- z toho aparát ústredného orgánu	5 413 246,00 €	5 970 879,00 €	5 748 209,13 €**	96,27%
Počet zamestnancov rozpočtovej organizácie podľa prílohy k uzneseniu vlády SR č. 667/2010	241 osôb	241 osôb	210 osôb*	87,14%
- z toho: aparát ústredného orgánu	241 osôb	241 osôb	210 osôb*	87,14%
A.4 Kapitálové výdavky (700) (bez prostriedkov na spolufinancovanie) z toho:	0,00 €	2 181 346,97 €	2 179 340,73 €	99,91%
Kód zdroja 111	0,00 €	92 150,00 €	92 137,74 €	99,99%
Kód zdroja 131H	0,00 €	2 039 196,97 €	2 037 202,99 €	99,90%
Kód zdroja 131I	0,00 €	50 000,00 €	50 000,00 €	100,00%
B. Prostriedky podľa § 17 ods. 4 zákona č. 523/2004 Z. z., v zmysle ktorého je rozpočtová organizácia oprávnená čerpať tento limit do výšky rozpočtových príjmov skutočne prijatých a je oprávnená prekročiť limit výdavkov z dôvodu dosiahnutia vyšších ako rozpočtovaných príjmov	2 000,00 €	2 000,00 €	123,76 €	6,19%
C. Prostriedky Európskej únie	0,00 €	6 422 529,61 €	6 422 529,61 €	100,00%
D. Výdavky štátneho rozpočtu na realizáciu programov vlády SR a časti programov vlády SR	10 120 423,00 €	21 316 947,94 €	20 908 220,89 €	98,08%
0D9 Bezpečnosť informácií	9 535 585,00 €	20 888 437,57 €	20 489 181,98 €	98,09%
0EK0U Informačné technológie financované zo štátneho rozpočtu – NBÚ	584 838,00 €	428 510,37 €	419 038,91 €	97,79%
E. Systemizácia policajtov v štátnej službe	216 osôb	216 osôb	187 osôb*	86,57%
Objem finančných prostriedkov v štátnej službe	4 880 555,00 €	5 368 611,00 €	5 290 579,27**	98,55%

* evidenčný počet zamestnancov k 31. decembru 2019, ** vrátane CyberExchange

Záväzné ukazovatele rozpočtu úradu boli v roku 2019 dodržané. Úrad pri hospodárení s finančnými prostriedkami dodržiaval zásady hospodárnosti, efektívnosti a účelnosti pri dodržiavaní legislatívnych predpisov najmä zákona č. 523/2004 Z. z. o rozpočtových pravidlách verejnej správy, zákona č. 357/2015 Z. z. o finančnej kontrole a audite, zákona č. 343/2015 o verejnom obstarávaní, uznesení vlády Slovenskej republiky a metodických pokynov a usmernení Ministerstva financií Slovenskej republiky.

ROZPOČET NA ROK 2020

Zákon č. 468/2019 Z. z. o štátnom rozpočte na rok 2020 bol v Národnej rade Slovenskej republiky schválený 3. decembra 2019. V nadväznosti na bod C.3 uznesenia vlády SR č. 500 zo dňa 14. októbra 2019 k návrhu rozpočtu verejnej správy na roky 2020 až 2022 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 2020.

Výdavky úradu na rok 2020 sú rozpočtované v celkovej sume 11 381 182,00 eur, z toho 11 096 344,00 eur v rámci programu 0D9 – Bezpečnosť informácií a 284 838,00 eur v rámci medzirezortného podprogramu 0EK0U – Informačné technológie financované zo štátneho rozpočtu – NBÚ. 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 zo všeobecne záväzných právnych predpisov a zo záväzkov SR voči EÚ a NATO.

5. KONTROLA A AUDIT

Kontrolná a audítorská činnosť je kontrolovanými subjektmi neraz vnímaná ako nepríjemná a represívna, má však aj preventívny a edukačný význam. Poskytuje tiež cenné poznatky a spätnú väzbu o stave dodržiavania všeobecne záväzných právnych predpisov a prispieva k výraznému zlepšovaniu legislatívnej činnosti úradu..

Úrad v roku 2019 pokračoval v kontrolnej činnosti štátnych orgánov a podnikateľov. V oblasti **ochrany utajovaných skutočností** vykonal tri **plánované a jednu mimoriadnu kontrolu,** všetky v štátnych orgánoch. Kontrolné skupiny sa zameriavali najmä na komplexnosť prijatých ochranných opatrení a ich koordináciu naprieč jednotlivými oblasťami bezpečnosti. Nedostatky boli zistené v troch kontrolovaných subjektoch. Spolu bolo zistených pätnásť kontrolných zistení, z toho bolo päť v oblasti administratívnej bezpečnosti, štyri v oblasti fyzickej bezpečnosti a objektovej bezpečnosti, štyri v oblasti bezpečnosti technických prostriedkov a po jednom nedostatku v oblasti priemyselnej bezpečnosti a šifrovej ochrany informácií.

Tabuľka č. 12: Prehľad kontrolnej činnosti úradu v roku 2019

Kontrolovaný subjekt	Počet kontrol		Oblasť	
	Plánované	Mimoriadne	Utajované skutočnosti	Dôveryhodné služby
Štátny orgán	3	1	4	0
Podnikateľ	0	0	0	0

Kontrolná činnosť bola vykonávaná komplexne a zameriavala sa na všetky oblasti bezpečnosti a ich vzájomnú previazanosť v systéme zabezpečenia ochrany utajovaných skutočností kontrolovaného subjektu. Vo všeobecnosti je možné konštatovať, že v porovnaní s predchádzajúcim obdobím **došlo k nárastu počtu kontrolných zistení.**

METODICKÁ ČINNOSŤ

V priebehu roka 2019 bol úrad mnohokrát oslovený štátnymi orgánmi, podnikateľmi, ale aj fyzickými osobami so žiadosťou o **metodické usmernenia** za všetky oblasti, ktoré patria do jeho gescie. Otázky sa najčastejšie týkali oblasti ochrany utajovaných skutočností, nasledovala oblasť kybernetickej bezpečnosti a dôveryhodných služieb. Prehľad je uvedený v tabuľke č. 13.

Tabuľka č. 13: Prehľad metodickej činnosti úradu v roku 2019

Oblasť / Počet	Utajované skutočnosti *						Kybernetická bezpečnosť	Dôveryhodné služby
	PB	AB	PrB	FOB	BTP	PS		
Čiastkovo	22	13	15	9	7	24	23	9
Podľa oblasti	90						23	9
Spolu	**122**							

** **PB** – personálna bezpečnosť, **AB** – administratívna bezpečnosť, **PrB** – priemyselná bezpečnosť, **FOB** – fyzická bezpečnosť a objektová bezpečnosť, **BTP** – bezpečnosť technických prostriedkov, **PS** – prierezové stanoviská*

VNÚTORNÁ KONTROLA A AUDIT

Vnútorný kontrolný orgán úradu v roku 2019 vykonal **deväť vnútorných kontrol.** Štyri vykonané kontroly sa týkali vecného plnenia úloh z uznesení vlády. Ostatné kontroly boli zamerané najmä na kontrolu ochrany utajovaných skutočností za oblasť bezpečnosti technických prostriedkov, kontrolu stavu požiarnej ochrany, kontrolu stavu BOZP, kontrolu dodržiavania času služby príslušníkov úradu a finančnú kontrolu na mieste. Okrem jedného prípadu malého významu nebolo pri kontrolách zistené porušenie všeobecne záväzných právnych predpisov.

V roku 2019 boli útvarom vnútorného auditu vykonané **štyri vnútorné audity.** Boli zamerané na overenie a zhodnotenie evidencie a vymáhania pohľadávok, procesu verejného obstarávania, vynakladania verejných prostriedkov na zahraničné služobné cesty a finančných dopadov vyplývajúcich z práceneschopnosti príslušníkov a zamestnancov úradu na rozpočet a osobitný účet úradu. Vykonanými vnútornými auditmi bol v povinnej osobe zistený jeden nedostatok nízkej závažnosti, nesystémový a finančne nevyčísliteľný.

SŤAŽNOSTI A PETÍCIE

V roku 2019 nebola úradu doručená žiadna sťažnosť ani petícia.

6. ZÁVERY A PRIORITY NA ROK 2020

Rok 2019 bol bohatý na udalosti, ktoré mali bezprostredný vplyv na postavenie, fungovanie a vnímanie úradu. Aktivity úradu zahŕňali plnenie širokého spektra úloh, viaceré z nich budú rozvinuté alebo dokončené v ďalších rokoch.

V roku 2019 nevznikli mimoriadne okolnosti, ktoré by narušali systém ochrany utajovaných skutočností v Slovenskej republike. V septembri sa uskutočnila inšpekcia Rady EÚ, ktorej predbežné neoficiálne závery potvrdili **vysokú úroveň zabezpečenia utajovaných skutočností,** vhodnosť nastavenia systému a pôsobenia jeho jednotlivých prvkov. Nevyskytli sa ani žiadne podstatné problémy, ktoré by obmedzili funkčnosť siete utajovanej komunikácie najvyšších ústavných činiteľov a ďalších vládnych predstaviteľov. **Bezpečnosť vládneho spojenia** nebola ohrozená a komunikácia sa uskutočňovala prostredníctvom certifikovaných technických prostriedkov a certifikovaných šifrových prostriedkov.

Úrad pokračoval v zavádzaní **vhodných legislatívnych podmienok,** ktorými bolo potrebné reagovať na vývojové trendy a na problémy, ktoré sa vyskytli v aplikačnej praxi. Pokračovalo aj budovanie **inštitucionálneho rámca,** posilňovanie **personálnych kapacít** úradu, implementácia **najnovších riešení a najlepších skúseností.**

Personálny stav úradu smeruje k ustáleniu jednotlivých rolí, hoci v prípade niektorých pozícií je veľkou výzvou priamo ich obsadiť **kvalifikovanými odborníkmi.**

V roku **2019 úrad spolupracoval s bezpečnostnými orgánmi EÚ a NATO** vo všetkých oblastiach svojej pôsobnosti. Vyvíjal aktívne kroky smerujúce k **podpore regionálnej spolupráce a rozvoju bilaterálnych partnerstiev** umožňujúcich výmenu skúseností, formuláciu spoločných stanovísk a koordináciu postupov pri presadzovaní spoločných záujmov. Úrad zabezpečoval **medzinárodnú výmenu utajovaných skutočností**. Elektronizácia registrov zahraničných utajovaných skutočností a ich online prepojenie s registrami orgánov verejnej moci umožňovala bezpečnú a zároveň **rýchlejšiu a flexibilnejšiu evidenciu a elektronickú distribúciu** utajovaných skutočností.

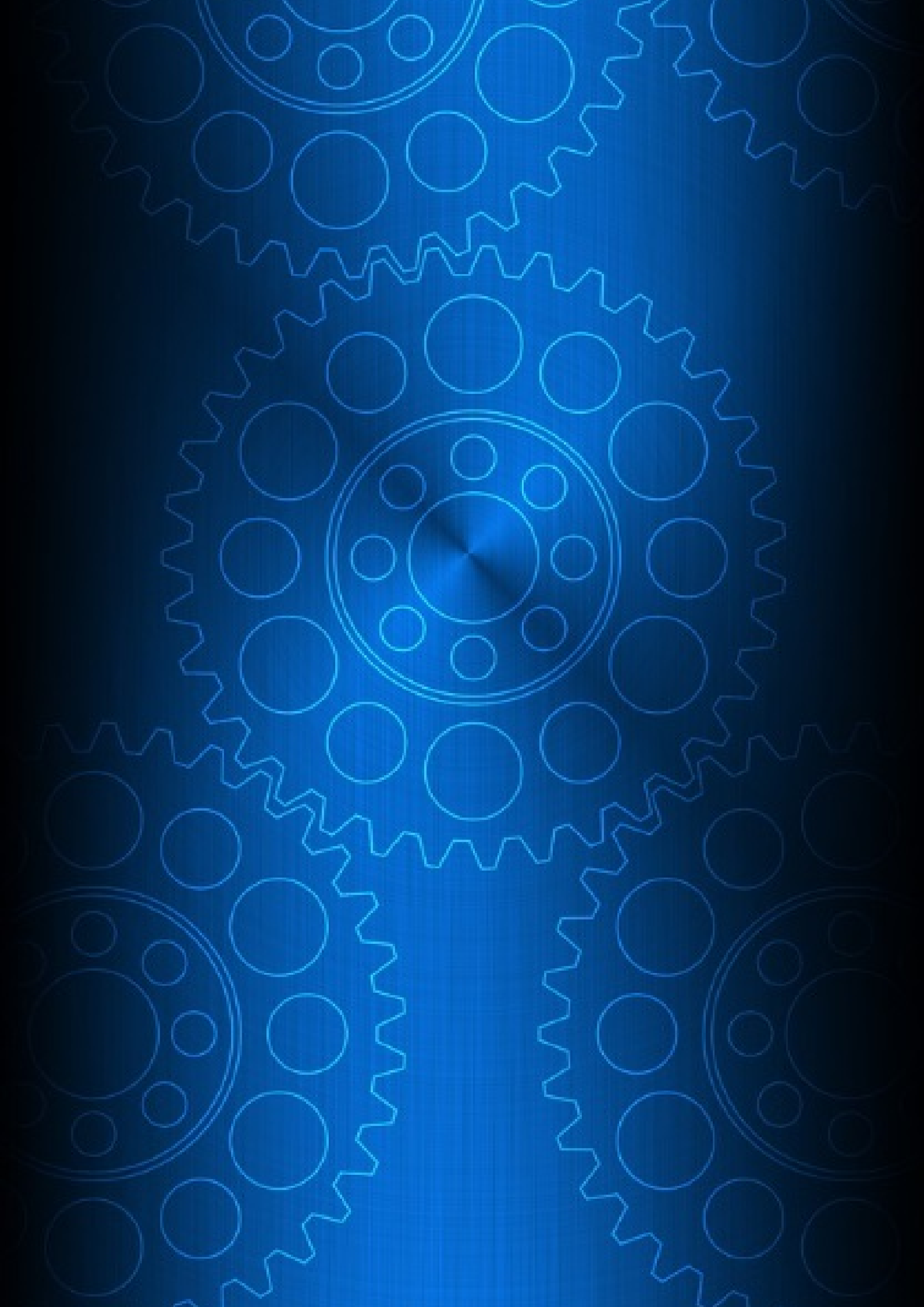
V oblasti kybernetickej bezpečnosti úrad v roku 2019 odpovedal na narastajúcu intenzitu a dynamiku hrozieb. Kybernetické útoky sa vyznačovali používaním **nových alebo inovovaných techník a nasadzovaním nových útočných vektorov.** Okrem štátnych aktérov a štátom sponzorovaných skupín, ktoré podnikali špionážne aktivity, pokúšali sa manipulovať verejnú mienku či ovplyvňovať výsledky demokratických procesov, pôsobia v kybernetickom priestore aj jednotlivci, pre ktorých sú kybernetické útoky osobnou výzvou, no najmä zdrojom príjmu.

Úrad 1. septembra 2019 zriadil **Národné centrum kybernetickej bezpečnosti SK-CERT (NCKB),** ktoré 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 záujme udržateľnosti plnenia úloh úradu a v perspektíve napredovania úradu v ďalšom období bola sformulovaná **Stratégia rozvoja Národného bezpečnostného úradu v rokoch 2019 – 2026.** Materiál sumarizuje sústavu rozvojových priorít úradu a definuje strategické ciele v oblasti posilňovania identity úradu, budovania personálnych kapacít, zvyšovania odbornosti vykonávaných činností, optimalizácie vnútorných procesov a rozvoja vonkajších vzťahov. Ciele sa odvíjajú od predstavy želaného stavu v budúcnosti a sú rozpracované do konkrétnych aktivít umožňujúcich ich realizáciu zavádzaním opatrení do praxe.

V súlade s rozvojovými zámermi úrad v roku 2019 zaviedol model **programového a projektového riadenia tímov,** ktoré zabezpečujú **plnenie prierezových medziútvarových úloh.** Zaoberajú sa najmä prípravou a realizáciou projektov spolufinancovaných z európskych fondov. K najdôležitejším projektom, ktorých realizácia prebieha, prípadne sa pripravuje, patrí projekt **Národného systému riadenia incidentov** kybernetickej bezpečnosti vo verejnej správe, projekt na vybudovanie **Centra simulácie, výskumu a výuky** kybernetických hrozieb a kybernetickej bezpečnosti, projekt **Certifikácie kybernetickej bezpečnosti,** projekt **Elektronizácie služieb úradu v oblasti ochrany utajovaných skutočností** a projekt **Zavádzania a podpory manažérstva kvality** vo verejnej správe. Každý z projektov má vysoké ambície prispieť k zefektívneniu uplatňovaných procesov, pripraviť kvalifikovaných odborníkov a zabezpečiť najmodernejšie technické vybavenie. Jednotlivé projekty budú ukončené v priebehu rokov 2020 a 2021.

Úrad v roku 2019 spracoval vlastný **Protikorupčný program** a prijal **Etický kódex.** Oba dokumenty sú nástrojom pozitívnej motivácie pracovníkov úradu posilnením ich vedomia, že pracujú v etickom prostredí s jasnými pravidlami platnými pre všetkých. Úrad má ambíciu zaviesť v roku 2020 systém riadenia korupčných rizík podľa STN ISO 37001 Systémy manažérstva proti korupcii a v súbehu s nastaveným vnútorným systémom oznamovania protispoločenskej činnosti vytvárať, udržiavať, preskúmavať a zlepšovať systém manažérstva proti korupcii.



Pôsobnosť Národného bezpečnostného úradu sa datuje od roku 2001. Patrí mu postavenie ústredného orgánu štátnej správy pre oblasť ochrany utajovaných skutočností, šifrovú službu, kybernetickú bezpečnosť a dôveryhodné služby.

Národný bezpečnostný úrad, ako súčasť bezpečnostného systému Slovenskej republiky, vykonáva bezpečnostné previerky osôb a podnikateľov, zabezpečuje bezpečné vládne spojenie, je orgánom dohadu pre dôveryhodné služby a plní úlohu národnej jednotky na riešenie kybernetických bezpečnostných incidentov.

Vo vzťahu k zahraničiu je Národný bezpečnostný úrad kontaktným bodom a národnou autoritou v oblastiach svojej pôsobnosti.

Od roku 2019 Národný bezpečnostný úrad v rámci svojej organizačnej štruktúry prevádzkuje Národné centrum kybernetickej bezpečnosti SK-CERT.

Národný bezpečnostný úrad
Budatínska 30, 851 06
Bratislava

podatelna@nbu.gov.sk
media@nbu.gov.sk
www.nbu.gov.sk