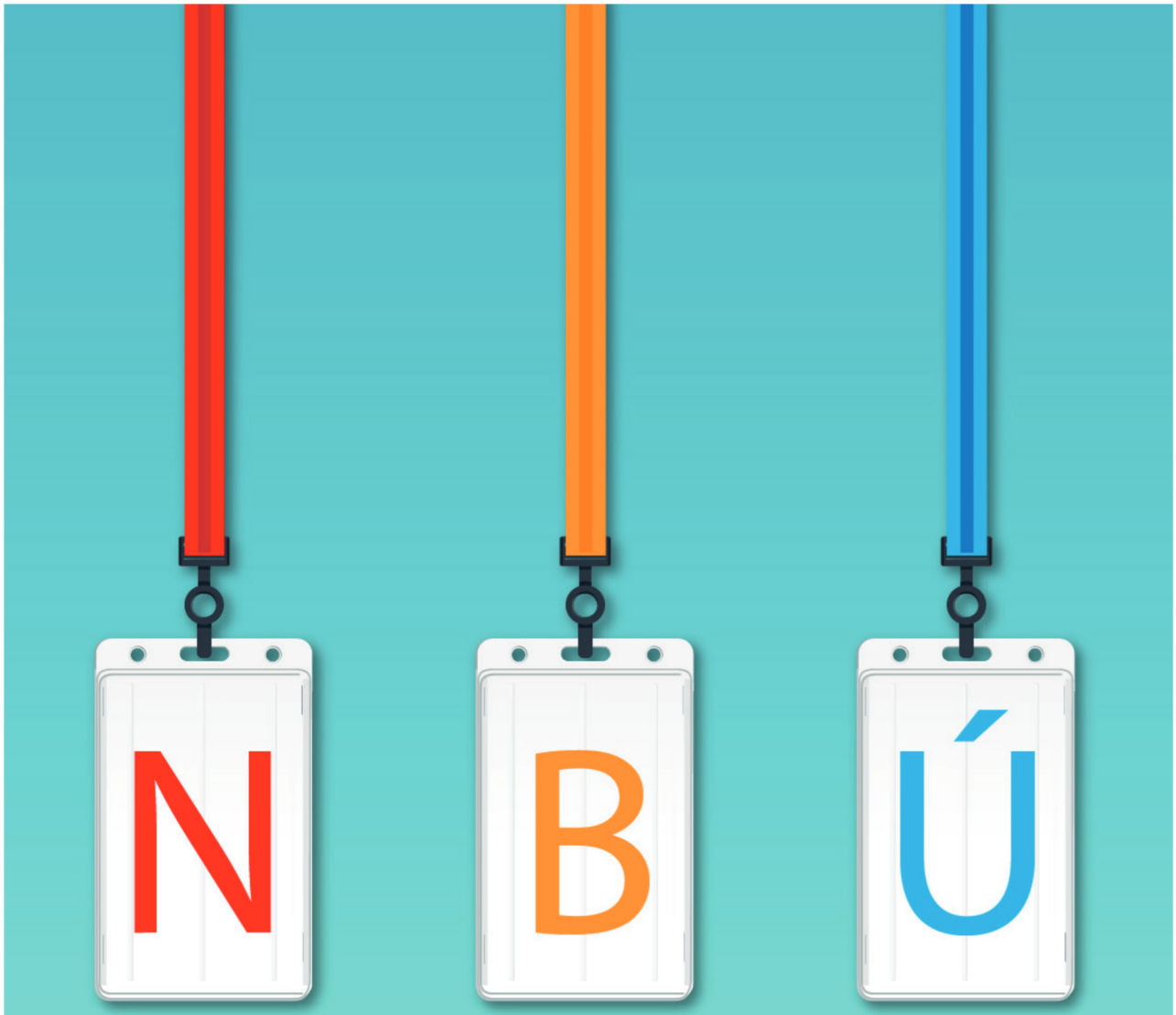
NÁRODNÝ
BEZPEČNOSTNÝ
ÚRAD

SPRÁVA O ČINNOSTI V ROKU 2020

Obsah



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 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.

NBÚ 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; 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 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 utajovaných skutočností v Slovenskej republike a podieľa sa na ochrane zahraničných utajovaných skutočností.

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

Plní úlohu garanta 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 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.

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 o ochrane utajovaných skutočností č. 215/2004, 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 o dôveryhodných službách 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.

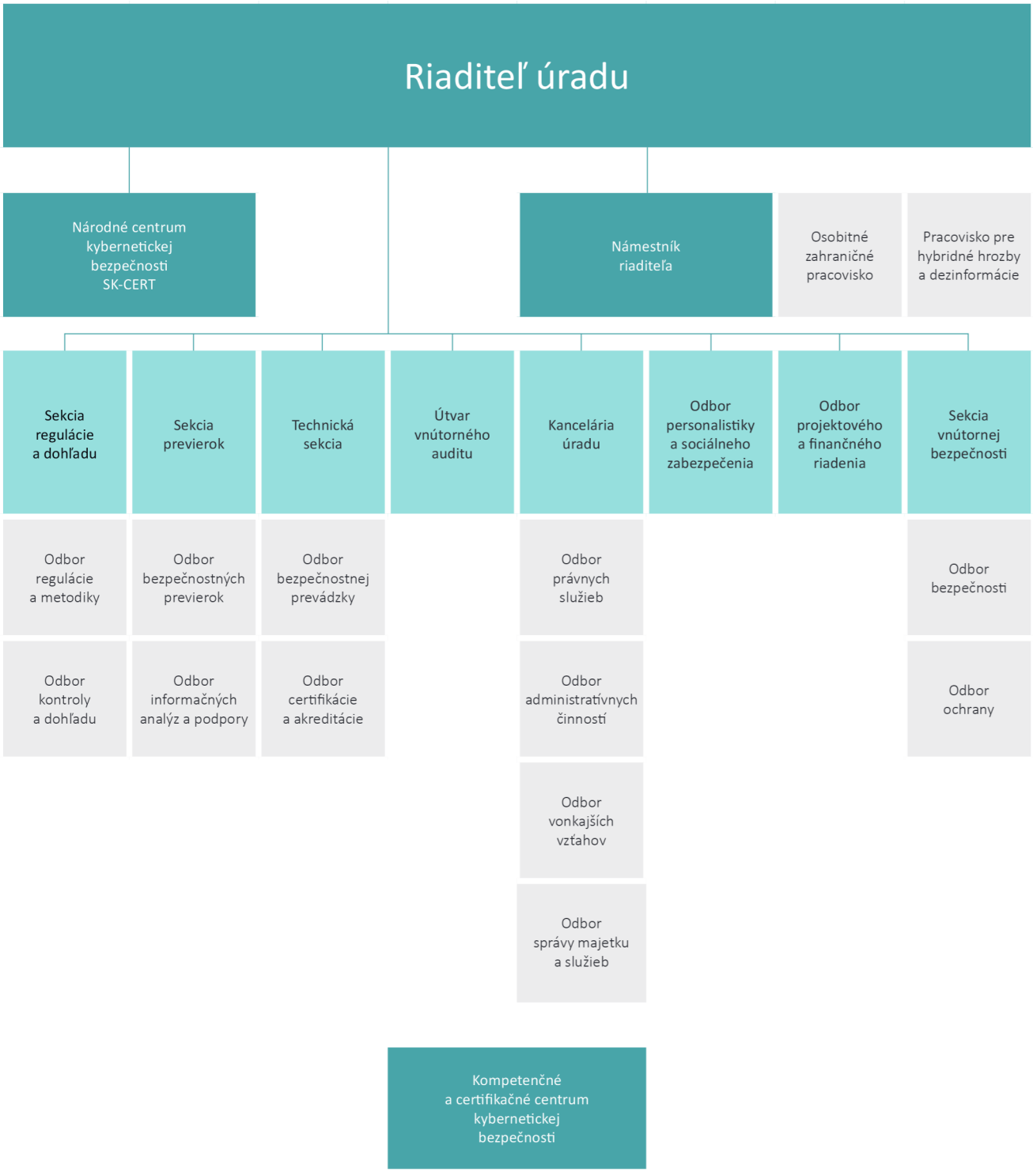
VEDENIE ÚRADU

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 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. V roku 2020 pod neho patrí aj Pracovisko pre hybridné hrozby a dezinformácie, ktoré zabezpečuje úlohy v oblasti boja proti hybridným hrozbám a šíreniu dezinformácií.

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.

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.

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 úradu v zahraničí.

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.

ĽUDSKÉ ZDROJE

ĽUDSKÉ ZDROJE

Celkový počet pracovníkov úradu bol v uplynulých rokoch 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.

2019

100 mužov

118 žien

195 príslušníkov

23 zamestnancov

2020

104 mužov

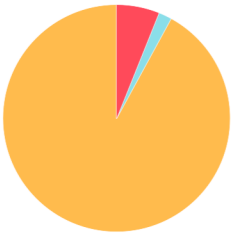
121 žien

202 príslušníkov

23 zamestnancov

Príslušníci v štátnej službe

2019



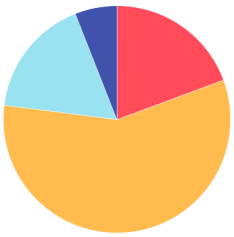
- **92 %** stála štátna služba
- **6 %** prípravná štátna služba
- **2 %** dočasná štátna služba

2020

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

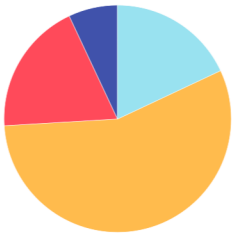
Vek

2019



- **58 %** 35 až 49 rokov
- **19 %** mladší ako 34 rokov
- **17 %** 50 až 59 rokov
- **6 %** nad 60 rokov

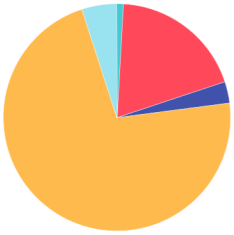
2020



- **56 %** 35 až 49 rokov
- **19 %** 50 až 59 rokov
- **18 %** mladší ako 34 rokov
- **7 %** nad 60 rokov

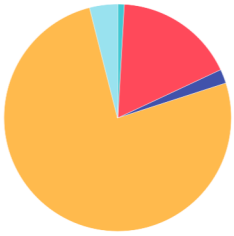
Vzdelanie

2019



- **72 %** vysokoškolské vzdelanie II. stupňa
- **19 %** úplné stredné vzdelanie
- **5 %** vysokoškolské vzdelanie III. stupňa
- **3 %** vysokoškolské vzdelanie I. stupňa
- **1 %** základné vzdelanie

2020



- **76 %** vysokoškolské vzdelanie II. stupňa
- **17 %** úplné stredné vzdelanie
- **4 %** vysokoškolské vzdelanie III. stupňa
- **2 %** vysokoškolské vzdelanie I. stupňa
- **1 %** 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. Z dôvodu pandémie COVID-19 bola veľká časť výuky vrátane záverečných skúšok vykonávaná dištančne online formou.

Príslušníci aj zamestnanci absolvovali vlani štandardné vstupné a pravidelné školenia bezpečnosti a ochrany zdravia pri práci a takisto ochrany pred požiarmi. Novinkou bolo školenie zamerané na prevenciu proti terorizmu a inštitútu aktívneho strelca.

Limitované bolo udržiavanie a zvyšovanie fyzickej kondície, pretože väčšinu roka bola telocvičňa úradu uzatvorená pre pandémiu.

AKTUALIZÁCIA PROTIKORUPČNÉHO PROGRAMU

NBÚ v roku 2020 aktualizoval svoj existujúci Protikorupčný program. Opäť má ambíciu monitorovať a hodnotiť nastavenie protikorupčného systému úradu s cieľom odstraňovať systémové zlyhania súvisiace s korupciou. Program je zverejnený na webovom sídle úradu.

OPATRENIE V OBLASTI PREVENCIE KORUPCIE

Na jeseň 2020 riaditeľ úradu na účely vytvorenia, implementovania, udržiavania, preskúmavania a zlepšovania systému riadenia protikorupčných činností na úrade a na ustanovenie zásad prevencie korupcie na úrade, práv a povinností príslušníkov a zamestnancov úradu pri uplatňovaní týchto zásad a postup pri ich uplatňovaní ustanovil formou interného predpisu systém riadenia korupčných rizík v súlade s požiadavkami STN ISO 37001 Systém manažérstva proti korupcii.

Podozrenia z korupcie príslušníkov a zamestnancov úradu môžu občania oznamovať cez protikorupčný e-mail na webovom sídle úradu.

PANDEMICKÝ PLÁN ÚRADU

V septembri 2020 vydal úrad Pandemický plán, aby zabezpečil preventívne a krízové opatrenia v prípade prepuknutia epidémie akútnych respiračných ochorení. Plán sa zameriava najmä na obmedzenie šírenia infekcie na úrade a zaručuje plnenie úloh úradu.

Plán rešpektuje opatrenia a odporúčania vydané Úradom verejného zdravotníctva Slovenskej republiky a inými relevantnými subjektmi.

LEGISLATÍVA

LEGISLATÍVA

Sekcia regulácie a dohľadu pracovala minulý rok na viacerých väčších legislatívnych zmenách. Výsledky niektorých legislatívnych procesov sa premietnu až v roku 2021. Kontinuálne však útvar pripravoval viaceré novely zákonov:

- príprava novely zákona č. 272/2016 o dôveryhodných službách pre elektronické transakcie na vnútornom trhu – cieľom je dosiahnuť odstránenie problémov z aplikačnej praxe. Ide najmä o úpravu spôsobu oznámenia o zámere poskytovať, zmeniť alebo ukončiť kvalifikované dôveryhodné služby, zároveň sa dopĺňajú povinnosti spoliehajúcej sa strany.

Novela upravuje aj proces certifikácie aj úpravu sankcií. Navrhuje upraviť systém mandátneho certifikátu a zoznamu oprávnení s prihliadnutím na existujúcu všeobecnú právnu úpravu spôsobu výkonu verejnej moci v elektronickej podobe upravenej v zákone o e-Governmente. Zákon bude predložený do legislatívneho procesu v priebehu roka 2021.

- príprava novely zákona č. 215/2004 o ochrane utajovaných skutočností – predmetom novely zákona je dosiahnuť odstránenie problémov vyplývajúcich z aplikačnej praxe, predovšetkým pri vykonávaní bezpečnostných previerok. Zákon bude predložený do legislatívneho procesu v roku 2021.

- 12. decembra 2020 bol v Zbierke zákonov vyhlásený zákon č. 364/2020, ktorým sa mení a dopĺňa zákon č. 395/2002 o archívoch a registratúrach. Mení a dopĺňa niektoré zákony, ktorými bol novelizovaný zákon č. 215/2004 o ochrane utajovaných skutočností.

Novelou sa umožnilo, aby ústredné orgány štátnej správy, v pôsobnosti ktorých vznikajú archívne dokumenty obsahujúce utajované skutočnosti, mohli tieto archívne dokumenty do zrušenia utajenia ukladať v centrálnom úložisku utajovaných skutočností, ktoré zriadi Národný bezpečnostný úrad.

Splnila sa tým aj povinnosť vedúceho zabezpečiť prehodnotenie stupňa utajenia utajovaných skutočností najmenej raz za päť rokov. Prax ukázala, že napriek povinnosti vedúceho (t. j. štatutárneho orgánu) prehodnocovať stupne utajenia, nie je táto povinnosť riadne plnená a k tejto činnosti dochádzalo iba pri vyraďovacom konaní.

- 1. januára 2021 nadobudol účinnosť zákon č. 423/2020 v súvislosti s reformou súdnictva. Takisto pozmenil a doplnil zákona č. 215/2004 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.

- po dôkladnej príprave a konzultáciách s odbornou verejnosťou predložil úrad do medzirezortného pripomienkového konania v zmysle uznesenia vlády Slovenskej republiky č. 547/2020 legislatívny návrh zákona č. 69/2018 o kybernetickej bezpečnosti.

Cieľom navrhovaného zákona je posilnenie právomocí príslušných vnútroštátnych orgánov a precizovanie niektorých definícií. Zavádza sa legislatívne vymedzenie inštitútu „blokovania“.

Novelou sa špecifikuje pôsobnosť úradu v súvislosti s plnením úloh vnútroštátneho orgánu pre certifikáciu kybernetickej bezpečnosti s odkazom na nariadenie EÚ č. 2019/881.

Upravuje sa postavenie audítora kybernetickej bezpečnosti a zavádza sa zoznam audítorov kybernetickej bezpečnosti a zoznam právnických osôb, prostredníctvom ktorých je možné realizovať audity kybernetickej bezpečnosti. Dochádza k implementácii Európskeho toolboxu kybernetickej bezpečnosti 5G sietí (EU Toolbox), zavedením všeobecnej úpravy namiesto definovania konkrétnej 5G („internet piatej generácie“) pre účely ďalšej praxe.

Zavádza sa povinnosť úradu vypracovávať každoročnú správu o ochrane osobných údajov v spojitosti s kybernetickými bezpečnostnými incidentmi a ich riešením. Ďalej dochádza k zakotveniu postavenia manažéra kybernetickej bezpečnosti, špecifikovaniu bezpečnostných opatrení a niektorých sankcií.

Do návrhu bola zapracovaná aj požiadavka z praxe – upravuje sa predĺženie lehoty z pôvodných šesť na dvanásť mesiacov na prijatie a dodržiavanie bezpečnostných opatrení v spravovaných a prevádzkovaných sieťach a informačných systémoch a vedenie príslušnej dokumentácie, pričom lehota plynie prevádzkovateľovi základnej služby od doručenia oznámenia o jeho zaradení do registra prevádzkovateľov základných služieb.

Úrad na základe získaných poznatkov a z dôvodu dopytu jednotlivých prevádzkovateľov základnej služby v návrhu zaviedol inštitút automatizovaného zasielania systémových informácií zo sietí a informačných systémov. Ide o zasielanie takých údajov, ktoré sú potrebné pri riešení kybernetického bezpečnostného incidentu. Materiál bude predmetom rokovania Národnej rady Slovenskej republiky v roku 2021.

- v novembri 2020 predložil Národný bezpečnostný úrad na medzirezortné pripomienkové konanie Národnú stratégiu kybernetickej bezpečnosti na roky 2021 až 2025. Úloha mu vyplynula z uznesenia vlády Slovenskej republiky 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 bude nasledovať príprava a predloženie akčného plánu realizácie stratégie, ktorý stanoví konkrétne časové, vecné, ale aj finančné kritéria rozvoja kybernetickej bezpečnosti na Slovensku. Akčný plán realizácie stratégie bude obsahovať aj úlohy pre jednotlivé ústredné orgány štátnej správy v medziach ich kompetencií a prípadné vplyvy, ktoré nová alebo upravená legislatíva prinesie.

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

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 8 podnetov, 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 a vec odložil záznamom, lebo nebol spáchaný priestupok podľa zákona o ochrane utajovaných skutočností.

OCHRANA UTAJOVANÝCH SKUTOČNOSTÍ

OCHRANA UTAJOVANÝCH SKUTOČNOSTÍ

S výnimkou globálnej pandémie nevznikli v roku 2020 **žiadne mimoriadne udalosti a okolnosti**, ktoré by narúšali systém zabezpečenia ochrany utajovaných skutočností. NBÚ kontinuálne pokračoval v optimalizácii previerkového procesu, zintenzívnil spoluprácu s partnerskými organizáciami a výsledkom je jeho efektívnejší a dynamickejší výkon.

PERSONÁLNA BEZPEČNOSŤ

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

Sekcia previerok minulý rok vydala 4612 osvedčení na oboznamovanie sa s utajovanými skutočnosťami stupňov Dôverné, Tajné a Prísne tajné; z toho 2425 pre príslušníkov a zamestnancov ministerstva obrany.

	2019	2020
Dôverné	**2 166**	**1 924**
pre MO SR	730	377
Tajné	**1 807**	**2 409**
pre MO SR	1351	1915
Prísne tajné	**295**	**279**
pre MO SR	167	133
SPOLU	**4 268**	**4 612**

V roku 2020 vydal úrad 42 rozhodnutí a fyzické osoby podali 12 odvolaní proti rozhodnutiu úradu. V jednom prípade rozhodol v autoremedúre.

Výbor Národnej rady Slovenskej republiky na preskúmavanie rozhodnutí Národného bezpečnostného úradu rozhodoval o 8 odvolaniach. Vo všetkých prípadoch ich zamietol. K 31.12.2020 boli 3 odvolania v odvolacom procese.

Navrhované osoby podali proti rozhodnutiu jednu žalobu na Najvyšší súd SR, ktorá je v procese rozhodovania. Okrem uvedeného najvyšší súd v roku 2020 rozhodoval v jednom konaní, v ktorom bola žaloba podaná v predchádzajúcom období. V uvedenom prípade zrušil rozhodnutie výboru, ktorý následne zrušil rozhodnutie úradu.

	2019	2020
Rozhodnutia úradu	**28**	**42**
Odvolania	**14**	**12**
Odvolania – autoremedúra	0	1
Odvolania zamietnuté výborom	13	8
Rozhodnutia zrušené výborom	0	1
Podané žaloby na najvyššom súde	1	1

Vo vzťahu k utajovaným skutočnostiam postupovaným NATO a EÚ vydal úrad navrhovaným osobám 4227 certifikátov, z toho 2041 certifikátov NATO a 2186 certifikátov EÚ.

Z celkového počtu certifikátov NATO úrad vydal 32 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 90 potvrdení o priemyselnej bezpečnosti, z toho 5 potvrdení stupňa utajenia Vyhradené, 66 potvrdení stupňa utajenia Dôverné, 17 potvrdení stupňa utajenia Tajné a 2 potvrdenia stupňa utajenia Prísne tajné.

Stupeň utajenia	2019	2020
Vyhradené	10	5
Dôverné	76	66
Tajné	22	17
Prísne tajné	1	2
Spolu	**109**	**90**

Úrad vydal 17 rozhodnutí, odvolanie proti nim podali štyria podnikatelia.

V jednom prípade rozhodol úrad v autoremedúre a o troch odvolaniach rozhodoval výbor, ktorý odvolania podnikateľov zamietol. Ku koncu roka nebolo žiadne odvolanie v odvolacom procese.

Proti rozhodnutiu výboru bola na najvyšší súd podaná jedna žaloba, ktorá je v procese rozhodovania. Okrem uvedeného najvyšší súd v roku 2020 rozhodoval v jednom konaní, v ktorom bola žaloba podaná v predchádzajúcom období a žalobu zamietol.

	2019	2020
Rozhodnutia úradu	**23**	**17**
Odvolania	**5**	**4**
Odvolania – autoremedúra	2	1
Odvolania zamietnuté výborom	2	3
Rozhodnutia zrušené výborom	0	0
Podané žaloby na najvyššom súde	0	1

Vo vzťahu k utajovaným skutočnostiam NATO a EÚ vydal úrad podnikateľom 15 certifikátov NATO a 11 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 2020 úrad uzatvoril 4 zmluvy a 6 dodatkov k uzatvoreným zmluvám.

ADMINISTRATÍVNA BEZPEČNOSŤ

V roku 2020 úrad prijal a odoslal 4 381 utajovaných písomností.

Nadobudnutím účinnosti vyhlášky 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. Zároveň prišlo aj k prepojeniu na zákon č. 305/2013 o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci.

Stupeň utajenia	2019	2020
Vyhradené	3 655	3 561
Dôverné	247	807
Tajné	7	13
Prísne tajné	0	0
Spolu	**3 909**	**4 381**

FYZICKÁ BEZPEČNOSŤ A OBJEKTOVÁ BEZPEČNOSŤ

Úrad v roku 2020 posudzoval opatrenia fyzickej bezpečnosti a objektovej bezpečnosti na ochranu utajovaných skutočností, a to v rámci realizovaných bezpečnostných previerok podnikateľov. Vykonaných bolo 40 posúdení (žiadosti podané v roku 2019 – 8 a žiadosti podané v roku 2020 – 32).

V roku 2020 úrad vydal 40 certifikátov mechanických zábranných prostriedkov (MZP) a technických zabezpečovacích prostriedkov (TZP).

	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

V roku 2020 v oblasti bezpečnosti technických prostriedkov (TP) vydal úrad 60 certifikátov a 17 dodatkov:

AKREDITÁCIA KOMUNIKAČNÝCH A INFORMAČNÝCH SYSTÉMOV

V roku 2020 úrad vykonal 2 akreditácie komunikačných a informačných systémov DEKMS a NS WAN v súlade s Bezpečnostnou politikou NATO C-(2002)49 a 1 akreditáciu komunikačného a informačného systému FADO EU v súlade s Rozhodnutím rady (2013/488/EÚ).

OCHRANA PRED NEŽIADUCIM ELEKTROMAGNETICKÝM VYŽAROVANÍM

Na zabezpečenie ochrany utajovaných skutočností pred únikom cez nežiaduce elektromagnetické vyžarovanie NBÚ vykonával zónové merania priestorov a merania technických prostriedkov a prostriedkov šifrovej ochrany informácií v špecializovanom TEMPEST laboratóriu.

Dovedna urobili 724 meraní zariadení (TP a PŠOI) a 10 zónových meraní priestorov, na základe ktorých bolo kategorizovaných 146 komponentov zariadení TP a 65 miestností. V danom období bola prijatá 1 žiadosť o vykonanie meraní tieneného stanu a zároveň bolo na základe žiadosti nevybavenej v roku 2019 vykonané meranie tienenej komory.

Na základe týchto žiadostí bolo vykonaných celkovo 18 meraní útlmu tienenej komory a tieneného stanu. V roku 2020 boli prijaté aj 2 žiadosti o vykonanie technických bezpečnostných prehliadok priestorov a 1 žiadosť o pravidelné vykonávanie technických bezpečnostných prehliadok služobných motorových vozidiel, na základe ktorých bola vykonaná prehliadka 20 miestností a pravidelne vykonávané prehliadky služobných motorových vozidiel.

ŠIFROVÁ OCHRANA INFORMÁCIÍ

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 2020 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.

Počas roka 2020 pokračoval úrad v priebežnej distribúcii technických prostriedkov použiteľných na bezpečnú výmenu informácií medzi vládnymi inštitúciami v režime stupňa utajenia Vyhradené, Dôverné a Tajné. V rámci zabezpečenia 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 národnej a medzinárodnej spolupráci úrad zabezpečoval funkciu Národnej distribučnej autority, ktorá je vstupným a kontaktným bodom Slovenskej republiky pri výmene a distribúcii šifrového materiálu a šifrovacích zariadení.

ŠIFROVÉ A TECHNICKÉ PROSTRIEDKY

Úrad v roku 2020 vydal 3 certifikáty (1x vyhradené a 2x dôverné) prostriedkov šifrovej ochrany informácií (PŠOI) a 6 dodatkov k certifikátu PŠOI.

DÔVERYHODNÉ SLUŽBY

DÔVERYHODNÉ SLUŽBY

V roku 2020 úrad dostal 1 žiadosť o certifikáciu bezpečného produktu pre kvalifikovaný elektronický podpis a 1 žiadosť o predĺženie platnosti certifikátu, avšak tieto konania boli zastavené z dôvodu nedodania zákonom požadovanej dokumentácie.

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 2020 úrad vydal úrad usmernenia napr. k použitiu certifikovaných zariadení na vyhotovenie kvalifikovaných elektronických podpisov, najmä certifikovaných v krajine Európskej únie, zverejnených v zozname zariadení certifikovaných Európskou úniou.

DÔVERYHODNÝ ZOZNAM

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

V priebehu roka 2020 úrad publikoval 10 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 2020 bolo na základe žiadostí štátnych orgánov a orgánov územnej samosprávy do zoznamu zapísaných 18 nových oprávnení. V priebehu roka úrad publikoval 14 verzií zoznamu oprávnení. Jeho aktuálna verzia bola vždy doplnená archívom predchádzajúcich verzií.

NOVÉ DÔVERYHODNÉ SLUŽBY

Úrad prijal oznámenie od dvoch kvalifikovaných poskytovateľov o zámere poskytovať kvalifikovanú dôveryhodnú službu. Oznámenia boli poskytovatelia povinní predložiť so záverečnou správou o posúdení zhody. Celkovo bolo udelených šesť kvalifikovaných štatútov na kvalifikovanú dôveryhodnú službu.

Úrad v roku 2020 posúdil a vyhovel siedmim žiadostiam kvalifikovaných poskytovateľov dôveryhodných služieb o rozšírenie existujúcich kvalifikovaných služieb o službu OCSP (Online Certificate Status Protocol) a šiestim žiadostiam na službu vydávania kvalifikovaných elektronických časových pečiatok.

Zároveň boli v roku 2020 kvalifikovanými poskytovateľmi dôveryhodných služieb predložené orgánu dohľadu dve 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.

DÔVERYHODNÁ INFRAŠTRUKTÚRA

Úrad prevádzkuje v dôveryhodnej infraštruktúrye 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.

KCA NBÚ v roku 2020 po ukončení CA Disig prevzala povinnosť poskytovať OCSP odpovede na zrušené a exspirované certifikáty vydané CA Disig.

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 2021.

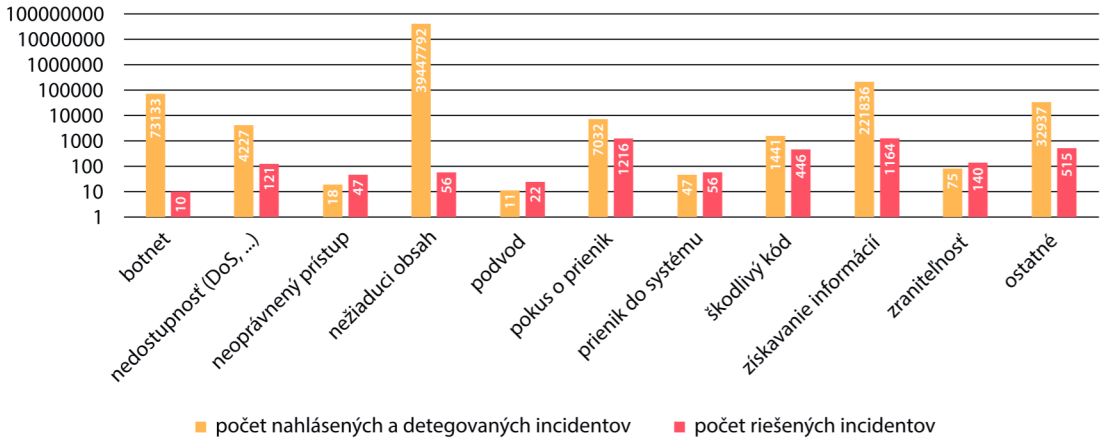
KYBERNETICKÁ BEZPEČNOSŤ

KYBERNETICKÁ BEZPEČNOSŤ

Národné centrum kybernetickej bezpečnosti SK-CERT v priebehu roka 2020 monitorovalo slovenský kybernetický priestor a kontinuálne zbieralo informácie o kybernetických bezpečnostných incidentoch.

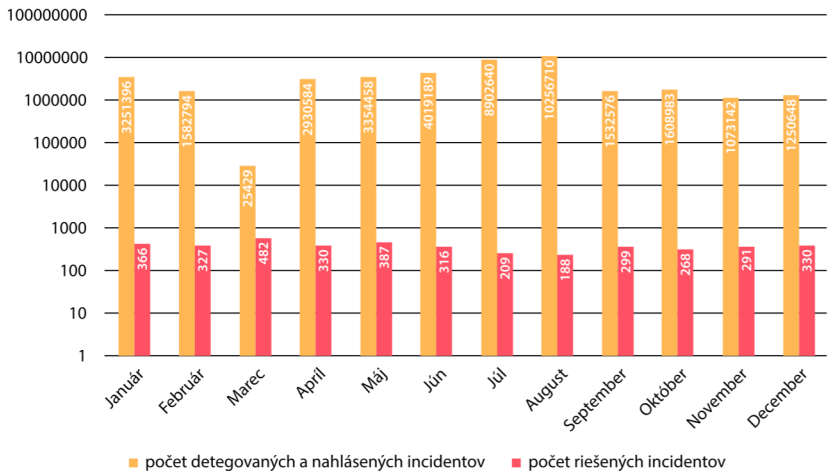
Zdrojom údajov bola vlastná detekcia, povinné a dobrovoľné hlásenia prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb a informácie od partnerov a partnerských organizácií.

Na základe získaných dát možno vytvoriť ucelený pohľad na počet nahlásených, detegovaných a riešených incidentov podľa jednotlivých kategórií. Najviac detegovaných a nahlásených incidentov bolo v kategórii nežiaduci obsah, najviac riešených incidentov bolo v kategórii pokus o prienik.



INCIDENTY NA ČASOVEJ OSI

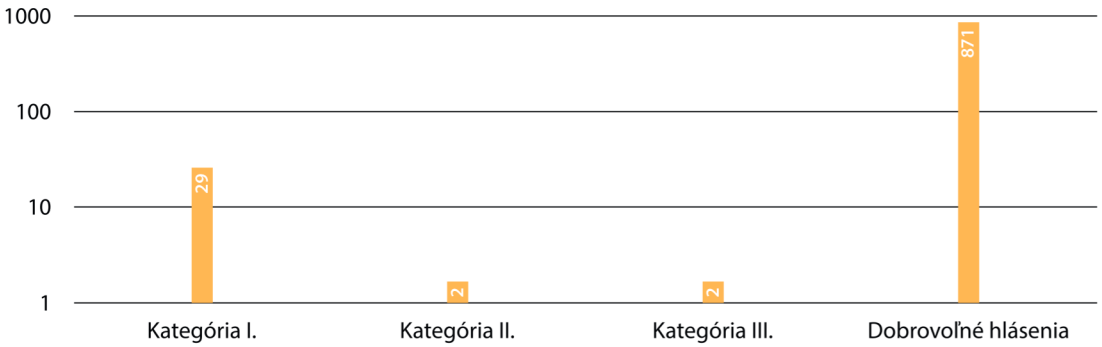
V roku 2020 bolo najviac incidentov detegovaných a nahlásených v auguste, najviac riešených v marci. Vstupy do tejto štatistiky pochádzajú zo zdrojov Národného centra kybernetickej bezpečnosti SK-CERT a od jeho CSIRT partnerov na Slovensku.



POVINNÉ A DOBROVOĽNÉ HLÁSENIA INCIDENTOV

Prevádzkovatelia základných služieb a poskytovatelia digitálnych služieb majú zo zákona o kybernetickej bezpečnosti dňom zápisu povinnosť hlásiť úradu každý závažný kybernetický bezpečnostný incident.

V roku 2020 došlo k nárastu hlásených incidentov podľa zákona, hlavne v kategórii dobrovoľných hlásení. V grafe nižšie sú uvedené podrobné počty incidentov v kategórii povinné a dobrovoľné hlásenia.



ČASY PANDÉMIE

Národné centrum kybernetickej bezpečnosti SK-CERT zaznamenalo prvý útok súvisiaci s COVID-19 v priebehu marca 2020. Len medzi marcom a aprílom bolo zaznamenaných a riešených ďalších 10 incidentov. Počas roka centrum evidovalo 24 súvisiacich incidentov.

Kybernetický priestor významne ovplyvnili aj karanténne opatrenia. Spoločnosti neboli pripravené na presun svojich zamestnancov do domácností, čo znamenalo opustenie často dôkladne zabezpečeného perimetra a vytvorenie nových nedostatočne pripravených vstupov do systémov spoločnosti. Útočníkom to často zjednodušilo pokusy získať dáta spoločností.

Významným cieľom útočníkov sa stal sektor zdravotníctva. Útočníci zameraní na krádež dát sa pokúšali získať dáta súvisiace s výrobou vakcíny na ochorenie COVID-19. Útok zaznamenala Európska lieková agentúra (EMA), kde sa útočníkom podarilo získať dáta o vakcíne spoločností Pfizer/BioNTech. Útoky boli realizované aj na vývojára vakcín AstraZeneca a na ďalšie farmaceutické spoločnosti v Nemecku, Kanade, Francúzsku, Indii, Južnej Kórei a USA.

Útoky sa nevyhli rôznym nemocniciam, pričom išlo hlavne o ransomvérové ataky. Nedostatok a preťaženosť zdravotníckych zariadení a stredísk zvyšovali šancu, že zdravotnícke zariadenie zaplatí výkupné, a to popri veľmi cenných zdravotníckych dátach lákalo kybernetických útočníkov.

Útoky zaznamenali desiatky nemocníc a laboratórií najmä v USA. V Európe sa cieľom úspešného útoku stala Brnenská nemocnica, ktorá bola nútená presunúť pacientov do inej nemocnice. V Nemecku sa ransomvérový útok skončil smrťou pacienta.

Ransomvérový útok prebehol aj na najväčšieho nemeckého prevádzkovateľa súkromných nemocníc Fresenius. Cieľom sa stali aj londýnske laboratóriá Hammersmith Medicines Research, ktoré pracovali na výskume koronavírusu.

Podvodníci skúšali profitovať masívnym vykupovaním zdravotníckych pomôcok a ich následným predávaním za násobné ceny. Vznikol veľký počet webstránok s podvodným obsahom zdieľajúcich hoaxy o koronavíruse a vakcinácií. Ďalej vznikali falošné internetové obchody – snažili sa vylákať peniaze od zúfalých občanov trpiacich nedostatkom dezinfekčných prostriedkov, respirátorov a rúšok.

CSIRT

K 31. decembru 2020 existujú na Slovensku podľa zákonom stanovených sektorov dve akreditované sektorové CSIRT jednotky – CSIRT.sk pre sektor „Verejná správa“, podsektor „Informačné systémy verejnej správy“ a Centrum pre kybernetickú obranu Slovenskej republiky, ktoré pôsobí v oblasti kybernetickej obrany.

CSIRT.sk na základe zmluvy poskytuje svoje služby sektoru Bankovníctva. Národné centrum kybernetickej bezpečnosti SK-CERT poskytuje svoje služby na základe zmluvy s Ministerstvom hospodárstva sektorom Energetiky a Priemyslu aj sektoru Zdravotníctvo.

V roku 2020 neprišlo k vzniku nových sektorových jednotiek CSIRT a takisto neboli uzavreté zmluvy s existujúcimi CSIRT jednotkami a ústrednými orgánmi, zodpovednými za jednotlivé sektory.

PRÍPRAVA NÁRODNEJ STRATÉGIE KYBERNETICKEJ BEZPEČNOSTI

Národný bezpečnostný úrad v roku 2020 spustil prípravu Národnej stratégie kybernetickej bezpečnosti na roky 2021 až 2025. Príprava tohto koncepčného materiálu bola podmienená legislatívnou požiadavkou, ale aj potrebou nadviazať na predchádzajúci strategický materiál, ktorým bola Koncepcia kybernetickej bezpečnosti na roky 2015 až 2020.

Národný bezpečnostný úrad na účel prípravy stratégie vytvoril pracovnú skupinu, ktorá participovala na výslednom návrhu. Na vládu bol predložený koncom decembra 2021 a neskôr ho vládny kabinet prijal.

Národná stratégia kybernetickej bezpečnosti má ambíciu zakotviť smerovanie Slovenskej republiky v oblasti kybernetickej bezpečnosti. V návrhu sú popísané princípy, na ktorých stojí systém riadenia kybernetickej bezpečnosti, ako aj hrozby, ktoré vplývajú na procesy a činnosti v oblasti kybernetickej bezpečnosti a majú významný dopad na bezpečnosť štátu, ako aj jeho obyvateľov. Ako reakciu na tieto hrozby určila strategické ciele, na ktoré je potrebné sa zamerať:

- 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

PRACOVISKO PRE HYBRIDNÉ HROZBY A DEZINFORMÁCIE

NBÚ zriadil Pracovisko pre hybridné hrozby a dezinformácie (PHHD) ako druhý ústredný orgán štátnej správy.

Vzniklo bez navýšenia rozpočtu, prispieva svojím vznikom, štatútom a činnosťou k budovaniu a modernizácií bezpečnostného systému Slovenskej republiky. Tento krok jednoznačne zvýraznil záujem úradu progresívne a aktívne pristupovať k prehodnocovaniu jeho vývoja.

PHHD je súčasťou niekoľkých národných iniciatív, ktoré aktívne prispievajú k príprave strategických dokumentov a aktivít vo svojej oblasti pôsobenia. Od svojho vzniku v júli 2020 aktívne upevňuje a rozvíja svoje pôsobenia na rôznych medzinárodných platformách a fórach, najnovšia aktivita je participácia v Hybrid CoE Expert Pools a projekte Hybrid CoE Horizon 2020 Pan-European Network for Countering Hybrid Threats EU-HYBNET, obe na pôde pôsobnosti Európskeho centra výnimočnosti pre hybridné hrozby v Helsinkách.

Na národnej úrovni sa PHHD podieľalo na príprave a realizácii e-learningového vzdelávacieho programu v oblasti hybridných hrozieb. Vzdelávací kurz hybridne.sk je dostupný pre každého príslušníka NBÚ a bol ponúknutý ako vzdelávacia aktivita NBÚ v roku 2020.

PHHD je participujúcim lektorským partnerom vzdelávacej aktivity GLOBSEC, ktorá je zameraná na šírenie povedomia v oblasti hybridných hrozieb. Vzdelávacie školenia boli vo všetkých VÚC a boli zamerané na zamestnancov krízových štábov okresných a krajských miest.

Príslušníci PHHD sa lektorsky zúčastnili na štyroch školeniach. V súčasnosti je pracovisko členom Medzirezortnej pracovnej skupiny pre Rozvoj koordinovaného mechanizmu SR v boji proti informačným operáciám, Koordinačnej platformy proti hybridným hrozbám KOPLA.

Od septembra je PHHD súčasťou projektu spoločnosti STRATPOL a Slovenského inštitútu pre bezpečnostnú politiku SSPI, ktoré sa venujú problematike a auditu bezpečnostného fungovania SK v oblasti hybridných hrozieb. PHHD bolo aktívnym členom analyticko-operačnej skupiny počas operácie Spoločná zodpovednosť.

EURÓPSKA LEGISLATÍVA

Do platnosti vstúpilo Nariadenie 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).

Cieľom tohto nariadenia je stanoviť ciele, úlohy a organizačné aspekty agentúry ENISA a zaviesť rámec európskych systémov certifikácie kybernetickej bezpečnosti na zabezpečenie primeranej úrovne kybernetickej bezpečnosti produktov informačných a komunikačných technológií (IKT), ich služieb a procesov, ale aj na predídenie fragmentáciám vnútorného trhu z hľadiska systémov certifikácie kybernetickej bezpečnosti v EÚ.

Účelom európskych systémov certifikácie kybernetickej bezpečnosti by malo byť, že sa zabezpečí, aby produkty, služby a procesy IKT, ktoré boli certifikované takýmto systémom, spĺňali uvedené požiadavky s cieľom chrániť dostupnosť, pravosť, integritu a dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich funkcií či služieb, ktoré tieto produkty, služby a procesy poskytujú alebo sprístupňujú, a to počas ich celého životného cyklu.

NARIADENIE O SIETI NÁRODNÝCH KOORDINAČNÝCH CENTIER

Európska komisia finalizuje prípravu Nariadenia Európskeho parlamentu a Rady, ktorým sa zriaďuje Európske centrum priemyselných, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti a sieť národných koordinačných centier.

Hlavným dôvodom iniciatívy je strategický záujem Únie zachovať a rozvíjať kapacity kybernetickej bezpečnosti s cieľom zabezpečiť jednotný digitálny jednotný trh, chrániť kritické siete a informačné systémy a poskytovať kľúčové služby v tejto oblasti.

Európske centrum odvetvových, technologických a výskumných kompetencií kybernetickej bezpečnosti – European Cybersecurity Competence Centre (ECCC) bude pracovať aj na podpore výskumu s cieľom uľahčiť a urýchliť procesy normalizácie a certifikácie – najmä v oblasti systémov certifikácie kybernetickej bezpečnosti v zmysle európskeho Aktu o kybernetickej bezpečnosti.

Úlohy národného koordinačného centra v SR plní Kompetenčné a certifikačné centrum kybernetickej bezpečnosti (KCCKB).

NOVELIZÁCIA SMERNICE NIS

Európska komisia zverejnila v decembri 2020 návrh na preskúmanie 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 Únii pod označením „Smernica NIS2“.

Cieľom bude aktualizovať súčasnú smernicu NIS, hoci táto smernica sa v členských štátoch začala uplatňovať až od 9. mája 2018. Súčasná verzia obsahuje cielené pravidlá (napr. povinnosť oznamovať porušenie) pre prevádzkovateľov základných služieb (poskytovatelia v oblasti energetiky, dopravy, bankovníctva a financií, zdravotníctva, dodávok vody a digitálnej infraštruktúry) a poskytovateľov digitálnych služieb (najmä poskytovatelia online trhoviska, služieb internetových vyhľadávačov a služieb cloud computingu). Členské štáty boli tiež povinné zriadiť tím pre riešenie počítačových bezpečnostných incidentov (tzv. CSIRT- computer security incident response team) a príslušný vnútroštátny orgán.

Cieľom je aj zrušenie rozdielu medzi prevádzkovateľmi základných služieb a poskytovateľmi digitálnych služieb a preskúmať nový prístup ku klasifikácii založený na dôležitosti služby. To by umožnilo ľahší režim pre služby, ktoré sú kategorizované ako „dôležité“, a nie „základné“.

Návrh posilňuje bezpečnostné požiadavky na spoločnosti, na ktoré sa vzťahujú predmetné pravidlá, a to zavedením princípu riadenia rizík (technické a organizačné opatrenia) a zároveň poskytuje minimálny zoznam základných bezpečnostných prvkov, ktoré sa musia uplatniť. Uvedené si bude vyžadovať normatívnejší prístup, ako sa aktuálne uplatňuje podľa súčasnej smernice NIS.

Návrh zavádza presnejšie požiadavky na hlásenie incidentov, vrátane obsahu hlásení a časových harmonogramov hlásenia (v niektorých prípadoch do 24 hodín). Cieľom smernice NIS2 je okrem vyššie uvedeného aj nahradiť konkrétne bezpečnostné požiadavky na poskytovateľov elektronických komunikačných sietí a služieb v Európskom kódexe pre elektronické komunikácie a na poskytovateľov dôveryhodných služieb podľa nariadenia (EÚ) č. 910/2014.

KOMPETENČNÉ A CERTIFIKAČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI

Základným poslaním Kompetenčného a certifikačného centra kybernetickej bezpečnosti (KCCKB) je vo verejnom záujme napomáhať k plneniu odborných úloh Národného bezpečnostného úradu ako zriaďovateľa v oblasti kybernetickej bezpečnosti, ochrany utajovaných skutočností, šifrovej ochrany a dôveryhodných služieb.

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

KCCKB plní aj činnosti súvisiace s ochranou utajovaných skutočností, kybernetickou bezpečnosti a dôveryhodných služieb podľa pokynov zriaďovateľa, plní úlohy orgánu posudzovania zhody, certifikuje audítorov, manažérov kybernetickej bezpečnosti, integrované systémy manažérstva kvality a ďalšie.

Realizuje audity kybernetickej bezpečnosti u prevádzkovateľa základnej služby s cieľom potvrdiť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených zákonom.

S cieľom posilniť a podporovať slovenskú ekonomiku v oblasti kybernetickej bezpečnosti vyplývajú kompetenčnému centru činnosti, ktoré sú v priamej súvislosti s pripravovaným Nariadením Európskeho parlamentu a Rady, ktorým sa zriaďuje Európske centrum priemyselných, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti a sieť národných koordinačných centier.

AUDITY KYBERNETICKEJ BEZPEČNOSTI

Prevádzkovateľ základnej služby má povinnosť vykonať audit kybernetickej bezpečnosti, čím preverí účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených zákonom. Audit je potrebné vykonať do dvoch rokov odo dňa zaradenia subjektu do registra prevádzkovateľov základných služieb a zároveň po každej zmene, ktorá má významný vplyv na bezpečnostné opatrenia. Auditom sa identifikujú nedostatky kybernetickej bezpečnosti a cieľom je odporúčať opatrenia na ich odstránenie a nápravu.

Úrad môže kedykoľvek nariadiť vykonanie auditu kybernetickej bezpečnosti u prevádzkovateľa základnej služby, resp. požiadať orgán posudzovania zhody, aby vykonal takýto audit u prevádzkovateľa základnej služby s cieľom potvrdiť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených týmto zákonom.

Kompetenčné centrum získalo v máji 2020 akreditáciu od Slovenskej národnej akreditačnej služby ako vnútroštátneho akreditačného orgánu SR.

To znamená, že aktuálny počet disponibilných certifikovaných audítorov v Slovenskej republike je 40. Certifikácie naďalej prebiehajú, Kompetenčné centrum vykonáva približne jednu certifikačnú skúšku mesačne s úspešnosťou 3-5 uchádzačov. Optimálny cieľový počet certifikovaných audítorov, ktorý by zodpovedal prácnosti a rozsahu auditov a očakávaným potrebám na výkon auditu u PZS približne 100.

Úrad v uplynulom období nariadil vykonanie dvoch auditov kybernetickej bezpečnosti – v Národnej agentúre pre sieťové a elektronické služby (NASES) a Národnom centre zdravotníckych informácií (NCZI).

MEDZINÁRODNÁ SPOLUPRÁCA

MEDZINÁRODNÁ SPOLUPRÁCA

Napriek okolnostiam pandémie úrad udržal intenzívnu spoluprácu s bezpečnostnými orgánmi EÚ a NATO a s ďalšími medzinárodnými organizáciami vo všetkých oblastiach svojej pôsobnosti na vysokej úrovni.

NBÚ vyvíjal aktívne kroky k podpore regionálnej spolupráce a rozvoju bilaterálnych partnerstiev na výmenu skúseností, formuláciu jednotných stanovísk a koordináciu postupov pri presadzovaní spoločných záujmov. Pracovisko Centrálneho registra úradu zabezpečovalo medzinárodnú výmenu a ochranu utajovaných skutočností.

PÔSOBENIE V EURÓPSKEJ ÚNII

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

Pandémia mala značný vplyv na realizáciu osobných pracovných stretnutí v jednotlivých pracovných platformách, preto sa rokovania presunuli spoza okrúhleho stola do virtuálneho priestoru. 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 zasadnutí Bezpečnostného výboru Rady EÚ (CSC), ako poradného orgánu Generálneho sekretariátu Rady EÚ pri príprave politík bezpečnosti a ochrany utajovaných skutočností EÚ.

Diskusie v CSC 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).

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 aj do Expertného bezpečnostného výboru pre globálny navigačný satelitný systém (GNSS SB) a Bezpečnostného akreditačného panela Európskej GNSS agentúry (GSA) pri budovaní satelitného systému Galileo (SAB).

Program Galileo je európskou iniciatívou za najmodernejší globálny navigačný satelitný systém poskytujúci vysoko presnú a zaručenú službu globálneho určovania polohy pod civilnou kontrolou. Plne nasadený systém bude tvoriť 30 satelitov a pozemná infraštruktúra. V roku 2020 bol predstavený aplikačný plán pre nasadenie druhej generácie (G2G) satelitov, ktoré by mali byť k dispozícii do roku 2025. Nová generácia satelitnej technológie zlepší už v súčasnosti excelentnú presnosť určovania polohy s minimálnou odchýlkou.

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, ako aj aktualizácii medzinárodných zmlúv v oblasti EUCI.

V celkovom pohľade reflektovala agenda ochrany EUCI v roku 2020 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 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. V procese schvaľovania tohto nariadenia je úrad pripravený na odbornú diskusiu.

V oblasti kybernetickej bezpečnosti rezonovali viaceré témy. Úrad úspešne reprezentoval Slovenskú republiku v platformách Blue OLEx 2020 (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 incidentu alebo krízy) s cieľom budovať pevnejší vzťah v komunite kybernetickej bezpečnosti.

Európska únia zriadila koncom roka Európske centrum odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti a sieť národných koordinačných centier. Zástupcovia vlád členských štátov vybrali za sídlo inštitúcie Bukurešť. 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), ktoré okrem iného plní aj úlohy národného odvetvového, technologického a výskumného centra v oblasti kybernetickej bezpečnosti.

V nelegislatívnej oblasti rok 2020 priniesol úspešnú implementáciu opatrení 5G toolbox (súbor opatrení určených na riešenie rizík v oblasti kybernetickej bezpečnosti 5G sietí). Komisia koncom roka k odporúčaniam publikovala správu, v ktorej analyzuje dôsledky opatrení. Úrad sa podieľal na Záveroch Rady o kybernetickej bezpečnosti pripojených zariadení. Dokument konštatuje, že zariadenia budú hrať kľúčovú rolu pri ďalšom formovaní digitálnej budúcnosti Európy.

Novou oblasťou sa stalo aplikovanie reštriktívnych opatrení v oblasti kybernetickej bezpečnosti. 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 ako kľúčový prvok formovania digitálnej budúcnosti Európy, Plánu 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.

NBÚ aktívne pôsobil v Európskej organizácii pre kybernetickú bezpečnosť (ECSO). V organizačnej štruktúre je 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 NATO

Rok 2020 bol pre Bezpečnostný úrad NATO (NOS) aj spojencov a partnerov NATO prelomový. Bezpečnostnému výboru NATO pre tvorbu bezpečnostných politík (SC SP) sa po niekoľkoročnej snahe podarilo zavŕšiť proces rozsiahleho revidovania základného dokumentu bezpečnostnej politiky NATO Bezpečnosť v Organizáciu Severoatlantickej zmluvy C-M(2002)49-REV1.

Stanovuje základné princípy a minimálne štandardy pre manipuláciu a ochranu utajovaných skutočností NATO. Úrad sa aktívne podieľal na revidovaní normy aj Direktívy o personálnej bezpečnosti, Direktívy o administratívnej bezpečnosti, Direktívy o fyzickej bezpečnosti a na príprave novej direktívy a podporného dokumentu k problematike ochrany utajovaných skutočností NATO vo vzťahu k nečlenským entitám NATO.

Koncom januára 2020 vykonal NOS inšpekciu ochrany utajovaných skutočností NATO na Slovensku. Úrad ako hlavný gestor ochrany utajovaných skutočností na Slovensku bol nielen subjektom inšpekcie, ale podieľal sa aj na koordinovaní a zabezpečovaní celej návštevy.

Inšpektori NOS hodnotili stav ochrany utajovaných skutočností NATO na Slovensku veľmi pozitívne a na veľmi vysokej úrovni. V záveroch Inšpekčnej bezpečnostnej správy o bezpečnostných opatreniach na ochranu utajovaných skutočností NATO v Slovenskej republike boli formulované odporúčania na odstránenie nedostatkov vyplývajúcich z hodnotiacej návštevy. Všetky kontrolované subjekty boli o výsledkoch informované a dostali požiadavku na dôsledné dodržiavanie odporúčaní.

Spoločné aliančné cvičenie NATO Able Staff 2020 sa tesne pred jeho novembrovým začiatkom zrušilo pre pandémiu a termín sa presunul na prelom februára a marca 2021.

Cvičenie má preveriť komunikáciu pri jadrovom plánovaní, precvičenie použiteľných opatrení systému krízovej odozvy aliancie, zdokonalenie konzultácií, realizovanie praktického výcviku personálu v centrále NATO, v Hlavnom veliteľstve spojeneckých síl v Európe (SHAPE) a v národných ústrediach.

REGIONÁLNA SPOLUPRÁCA

Národný bezpečnostný úrad dlhodobo považuje regionálnu spoluprácu za dôležitú prioritu. V roku 2020 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 Platform). Opäť sa v nej darilo nachádzať spoločné a zjednocujúce názory na aktuálne európske témy.

Každoročné zasadnutie platformy sa odohralo vo virtuálnom priestore. Hlavnými témami boli spoločné vyhlásenie k revidovanej smernici NIS 2, zdieľanie skúsenosti počas pandémie z oblasti kybernetickej bezpečnosti, posledná aktualizácia k prijímaným opatreniam k bezpečnosti 5G sietí aj certifikácia kybernetickej bezpečnosti. Maďarský inšpektor ozbrojených síl predstavil kybernetickú obranu štátu a projekt „MeliCERT facility“. V roku 2021 platforme predsedá Poľsko a v roku 2022 Slovensko.

BILATERÁLNE PARTNERSTVÁ

Úrad napriek celosvetovej pandemickej situácii aj v roku 2020 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 pod.

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

Začiatkom roka pokračovalo medzirezortné pripomienkové konanie k dohode medzi slovenskou a maltskou vládou o vzájomnej ochrane utajovaných skutočností.
V rovnakom čase rokoval úrad o novej dohode medzi vládou SR a USA o bezpečnostných opatreniach na ochranu utajovaných skutočností. V októbri 2020 bolo ďalšie kolo rokovaní k pripomienkam na oboch stranách. Americká strana sa mala v júni 2020 zúčastniť na bezpečnostnej hodnotiacej návšteve na Slovensku. Pre pandémiu ale musia obe strany nájsť vhodnú alternatívu.

Pred vypuknutím pandémie privítal riaditeľ NBÚ delegáciu Severného Macedónska. Témou boli problematika vzájomnej ochrany a výmeny utajovaných informácií, zdieľanie praktických skúsenosti v otázkach ochrany utajovaných skutočností a dát v podmienkach EÚ aj skúsenosti SR s prístupom do EÚ. Delegácia sa venovala aj témam ochrany kritickej digitálnej infraštruktúry, kybernetickej bezpečnosti a fungovaniu Národného centra kybernetickej bezpečnosti SK-CERT.

Začiatkom septembra 2020 absolvoval návštevu Slovenskej republiky zástupca námestníka ministra zahraničných vecí USA pre európske záležitosti Matthew Boyse. Na oficiálnom prijatí u riaditeľa úradu ho sprevádzala veľvyslankyňa USA na Slovensku Bridget A. Brinková a politický tajomník Jonathan Herzog.

Hlavnou témou rozhovoru bolo legislatívne ukotvenie problematiky bezpečnosti 5G sietí na Slovensku. Riaditeľ úradu informoval amerických partnerov o iniciatíve Slovenska v uzavretí spoločnej deklarácie o bezpečnosti 5G technológií, na vypracovaní ktorej úrad aktívne spolupracoval. Spoločné vyhlásenie SR a USA k bezpečnosti sietí piatej generácie podpísali v októbri vo Washingtone ministri zahraničných vecí oboch krajín.

V súvislosti s dlhodobým úsilím Rumunska o pridelenie Európskeho centra odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti a siete národných koordinačných centier navštívil úrad špeciálny vyslanec rumunskej vlády Alexander Nazare, ktorého sprevádzala rumunská veľvyslankyňa na Slovensku Steluta Arhireová.

Delegácia predstavila koncepciu kandidatúry a detaily fungovania centra v horizonte desaťročia. Úrad rumunským partnerom potvrdil podporu. Aj vďaka hlasu Slovenska sa po zavŕšení legislatívneho procesu sídlom centra stane Bukurešť.

VÝMENA ZAHRANIČNÝCH INFORMÁCIÍ

Elektronizácia registrov zahraničných utajovaných skutočností prostredníctvom online prepojenia s registrami utajovaných skutočností orgánov verejnej moci umožňuje bezpečnú, rýchlejšiu a flexibilnejšiu evidenciu a elektronickú distribúciu utajovaných skutočností. V roku 2020 úrad jednotlivým registrom utajovaných skutočností, zriadenými orgánmi verejnej moci, poskytol metodickú pomoc pri elektronickej evidencii utajovaných skutočností.

Pracovisko centrálneho registra spracovalo 4 222 utajovaných skutočností NATO a 1 353 utajovaných skutočností EÚ. Úrad sprostredkoval aj výmenu 152 utajovaných skutočností cudzej moci. Na úrade od roku 2010 pôsobí vytvorený register utajovaných skutočností NATO ATOMAL. V roku 2020 v ňom neboli zaevidované žiadne ATOMAL utajované písomnosti.

Stupeň utajenia	2019	2020
NATO Restricted	4 870	1 754
EU Restricted	2 374	802
Cudzia moc Vyhradené	53	83
NATO Confidential	1 847	1 089
EU Confidential	1 131	364
Cudzia moc Dôverné	62	66
NATO Secret	2 491	1 379
EU Secret	430	186
Cudzia moc Tajné	14	2
NATO Top Secret	0	0
EU Top Secret	0	1
Cudzia moc Prísne tajné	16	1
NATO spolu	**9 208**	**4 222**
EU spolu	**3 935**	**1 353**
Cudzia moc spolu	**145**	**152**

HOSPODÁRENIE

HOSPODÁRENIE

ROZPIS ZÁVÄZNÝCH UKAZOVATEĽOV ROZPOČTU

Rozpis záväzných ukazovateľov rozpočtu kapitoly 41 Národný bezpečnostný úrad na rok 2020, vplyv rozpočtových opatrení na výšku rozpočtu a porovnanie čerpania rozpočtových prostriedkov k upravenému rozpočtu k 31. decembru 2020.

Ukazovatele	Schválený rozpis	Upravený rozpočet	Skutočnosť	Plnenie k upr. rozpočtu
I. Príjmy kapitoly	**16 900,00**	**14 296,05**	**12 460,08**	**87,16 %**
A. Záväzný ukazovateľ	**14 900,00**	**12 296,05**	**12 313,85**	**100,15 %**
B. Prostriedky Európskej únie	0,00	0,00	0,00	-
II. Výdavky kapitoly celkom (A + B+ C)	**11 381 182,00**	**15 043 525,61**	**14 132 042,87**	**93,94 %**
A. Výdavky spolu bez prostriedkov podľa § 17 ods. 4 zákona č. 523/2004 Z. z. a prostriedkov Európskej únie	11 379 182,00	12 796 947,88	11 887 318,91	92,89 %
z toho:				
A.1. prostriedky štátneho rozpočtu kód zdroja 111	11 379 182,00 11 379 182,00	10 060 401,57 11 685 677,00	11 150 918,83 10 776 194,26	92,46 % 92,22 %
A.2. prostriedky na spolufinancovanie 3AA2 3AA3	0,00	736 546,31 396 101,94 340 444,37	736 546,31 396 101,94 340 444,37	100,00 % 100,00 % 100,00 %
A.3. mzdy, platy, služ. príj. a ost. os. vyrovnania (610), (kód zdroja 111 + 11H)	6 562 036,00	6 558 796,00	5 847 363,17	89,15 %
z toho: mzdy, platy, služ. príjmy a ost. os. vyrovnania aparátu ústred.orgánu (kód zdroja 111 + 11H)	6 562 036,00	6 558 796,00	5 847 363,17	89,15 %
Počet zamestnancov rozp. org. podľa prílohy č. 1 k uznes. vlády SR č. 500/2019	241 osôb	240 osôb	214 osôb*	89,17 %
z toho: aparát ústredného orgánu	241 osôb	240 osôb	214 osôb*	89,17 %
A.4. kapitálové výdavky (700) (bez prostriedkov na spolufinancovanie) z toho: kód zdroja 111 kód zdroja 131I kód zdroja 131J	0,00 0,00	405 792,57 31 068,00 257 231,16 117 493,41	405 792,57 31 068,00 257 231,16 117 493,41	100,00 % 100,00 % 100,00 % 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 rozpočtovaných príjmov skutočne prijatých a je oprávnená prekročiť limit výdavkov z dôvodu dosiahnutia vyšších ako rozpočtovaných príjmov.	2 000,00	2 000,00	146,23 %	7,31 %
C. Prostriedky Európskej únie 3AA1	0,00	2 244 577,73 2 244 577,73	2 244 577,73 2 244 577,73	100,00 % 100,00 %
D. Výdavky štátneho rozpočtu na realizáciu programov vlády SR a časti programov vlády SR 0D9 Bezpečnosť informácií 0EK0U Informačné technológie financované zo štátneho rozpočtu – NBÚ	11 381 182,00 11 096 344,00 284 838,00	15 043 525,61 14 775 687,61 267 838,00	14 132 042,87 13.865 864,70 266 178,17	93,04 % 93,84 % 99,38 %
E. Systemizácia policajtov v štátnej službe	216 osôb 5 905 472,00	216 osôb 5 905 472,00	192 osôb* 5 394 490,32	88,89 % 91,35 %

Úrad dodržal záväzné ukazovatele rozpočtu úradu v roku 2020. Pri hospodárení s finančnými prostriedkami sa opieral o zásady hospodárnosti, efektívnosti a účelnosti pri dodržiavaní legislatívnych predpisov najmä zákona č. 523/2004 o rozpočtových pravidlách verejnej správy, zákona č. 357/2015 o finančnej kontrole a audite, zákona č. 343/2015 o verejnom obstarávaní, uznesení vlády Slovenskej republiky a metodických pokynov a usmernení Ministerstva financií Slovenskej republiky.

ROZPOČET NA ROK 2021

Zákonom č. 425/2020 o štátnom rozpočte na rok 2021 boli schválené záväzné ukazovatele štátneho rozpočtu jednotlivých kapitol na rok 2021. V nadväznosti na bod C.1 uznesenia vlády SR č. 649 zo dňa 14. októbra 2020 k návrhu rozpočtu verejnej správy na roky 2021 až 2023 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 NBÚ oznámené záväzné ukazovatele štátneho rozpočtu na rok 2021.

Výdavky úradu pre rok 2021 sú rozpočtované v programe 0D9 – Bezpečnosť informácií a medzirezortného podprogramu 0EK0U – Informačné technológie financované zo štátneho rozpočtu – NBÚ v celkovej sume 12 730 671,00 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 zo všeobecne záväzných právnych predpisov a zo záväzkov SR voči EÚ a NATO.

KONTROLA A AUDIT

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 2020 pokračoval v kontrolnej činnosti štátnych orgánov a podnikateľov. V oblasti ochrany utajovaných skutočností vykonal 10 plánovaných a jednu mimoriadnu kontrolu; ďalej jednu kontrolu nad dodržiavaním ustanovení zákona o dôveryhodných službách.

Deväť kontrol bolo v štátnych orgánoch, tri v podnikateľských subjektoch.

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

Nedostatky boli zistené v ôsmich kontrolovaných subjektoch. Spolu bolo zistených 36 kontrolných zistení:

- 8 v oblasti administratívnej bezpečnosti
- 22 v oblasti fyzickej bezpečnosti a objektovej bezpečnosti
- 4 v oblasti bezpečnosti technických prostriedkov
- 1 nedostatok v oblasti priemyselnej bezpečnosti
- 1 nedostatok v oblasti šifrovej ochrany informácií

Z celkového počtu plánovaných kontrol na rok 2020 presunuli kontrolóri 8 z nich na rok 2021. Dôvodom boli opatrenia súvisiace s pandémiou ochorenia COVID-19. Napríklad v mesiacoch marec až jún a september až október nebolo vôbec možné vykonávať kontroly, prípadne iba v obmedzenom režime.

Kontrolovaný subjekt	Počet kontrol		Oblasť	
	Plánované	Mimoriadne	Utajované skutočnosti	Dôveryhodné služby
Štátny orgán	8	1	9	0
Podnikateľ	3	0	2	1

V oblasti kybernetickej bezpečnosti boli úradu doručené tri záverečné správy o výsledku auditu u prevádzkovateľov základných služieb.

Národný bezpečnostný úrad vlani nariadil dva mimoriadne audity kybernetickej bezpečnosti v Národnej agentúre pre sieťové a elektronické služby (NASES) a v Národnom centre zdravotníckych informácií (NCZI).

METODICKÁ ČINNOSŤ

V roku 2020 oslovili úrad desiatky štátnych orgánov, podnikateľov, ale aj fyzických osôb so žiadosťou o metodické usmernenia vo všetkých oblastiach jeho vecnej pôsobnosti. Otázky sa najčastejšie týkali oblasti ochrany utajovaných skutočností, kybernetickej bezpečnosti a dôveryhodných služieb.

Oblasť	Utajované skutočnosti*							
Počet	**PB**	**AB**	**PrB**	**FOB**	**BTP**	**PS**	**Kybernetická bezpečnosť**	**Dôveryhodné služby**
Štátny orgán	33	40	12	11	2	38	32	11
Spolu						**179**		

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

VNÚTORNÁ KONTROLA

Sekcia vnútornej bezpečnosti v roku 2020 vykonala 13 ukončených vnútorných kontrol.

Štyri sa týkali vecného plnenia uznesení vlády, ostatné boli zamerané na kontrolu ochrany utajovaných skutočností za oblasť fyzickej a objektovej bezpečnosti, dodržiavania stanoveného času služby príslušníkov a zamestnancov úradu, dočasnej neschopnosti na výkon štátnej služby pre chorobu alebo úraz a poskytovanie služobného voľna (vrátane štatistického zistenia).

Vnútorná kontrola sa venovala aj dodržiavaniu povinností z interných predpisov v oblasti prevádzky služobných motorových vozidiel, zabezpečeniu stravovania, výdavkom za ubytovanie pri tuzemskej a zahraničnej služobnej ceste.

Kontroly v osobnom kontakte s príslušníkom alebo zamestnancom (napr. vyšetrenie na zistenie alkoholu v krvi) neboli vykonané pre pandemické opatrenia.

Okrem banálnych prípadov nezistila sekcia vnútornej bezpečnosti pri kontrolách žiadne porušenie všeobecne záväzných predpisov.

VNÚTORNÝ AUDIT

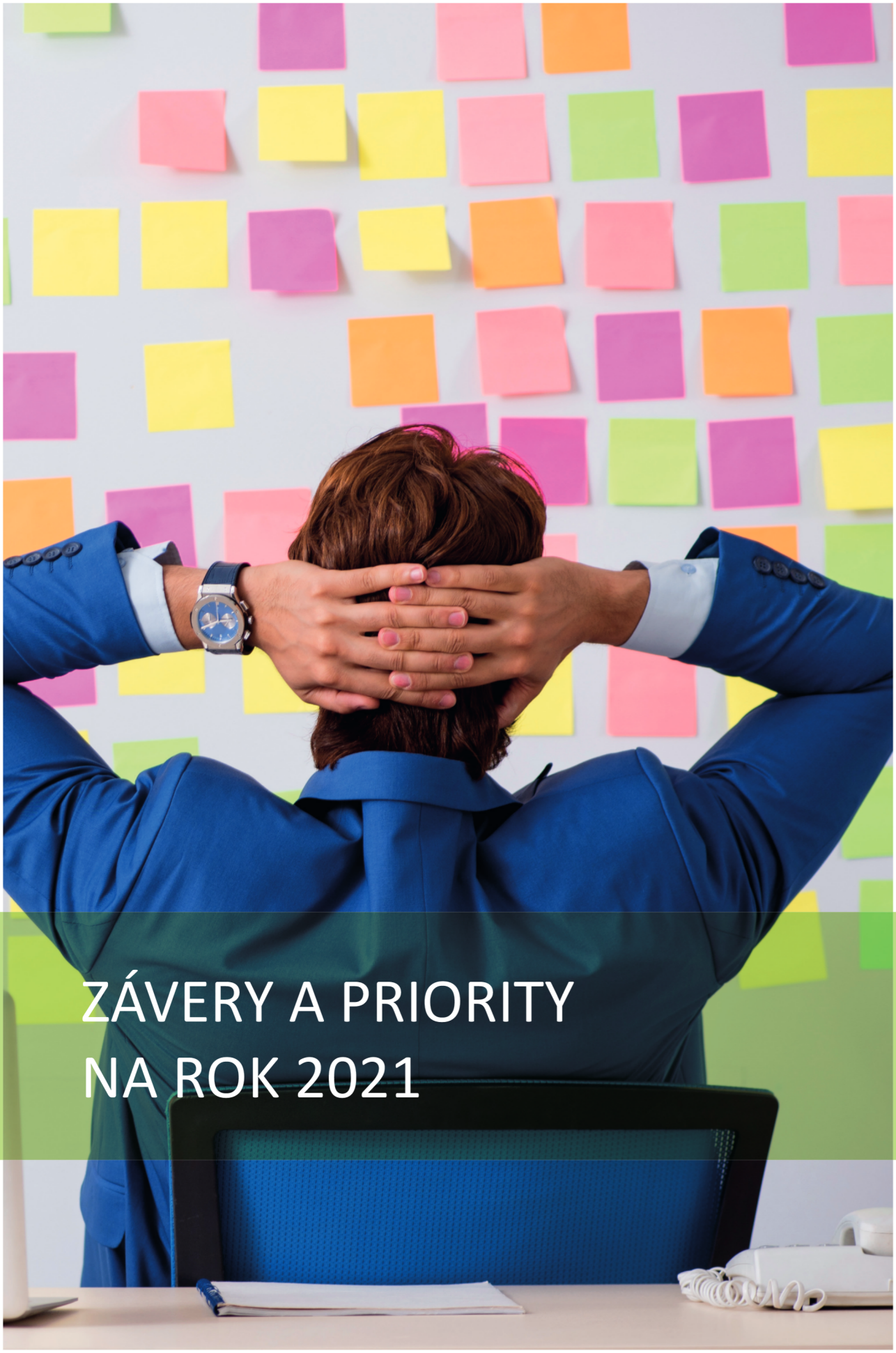
V roku 2020 boli útvarom vnútorného auditu vykonané 3 vnútorné audity.

Zamerali sa na overenie a zhodnotenie vykonania inventarizácie v rokoch 2018 až 2019, plnenia prijatých opatrení na základe správy z vnútorného auditu a plnenia záväzných rozpočtových ukazovateľov NBÚ v rokoch 2018 a 2019.

Vykonanými vnútornými auditmi nebol v povinnej osobe zistený nedostatok.

SŤAŽNOSTI A PETÍCIE

Úradu boli doručené 3 sťažnosti, ktoré úrad prešetrením a prekontrolovaním vyhodnotil ako neopodstatnené. NBÚ nebola doručená žiadna petícia.



ZÁVERY A PRIORITY NA ROK 2021

ZÁVERY A PRIORITY NA ROK 2021

Dlhodobé priority Národného bezpečnostného úradu sa nemenia. Budeme ďalej **upevňovať postavenie úradu v bezpečnostnom systéme Slovenska**, posilňovať služobnú a pracovnú disciplínu jeho pracovníkov a prispievať k obrazu NBÚ ako **modernej** a **transparentnej inštitúcie**, ktorá podporuje informatizáciu spoločnosti, odbúravanie byrokracie a boj proti korupcii.

Úrad bude kontinuálne optimalizovať riadenie ľudských zdrojov, efektivitu prijímania nových odborníkov a ich neustále vzdelávanie; svoje interné procesy, hospodárenie aj projektové riadenie.

Národný bezpečnostný úrad bude pokračovať v zbere a analýze informácií z aplikačnej praxe, zohľadňovať požiadavky z medzinárodných dohôd a legislatívy Európskej únie, ale bude vychádzať aj zo spätnej väzby odbornej verejnosti pri tvorbe a úprave zákonov a predpisov pre lepší výkon štátnej správy. Naším cieľom je presadiť alebo pripraviť novely zákonov o dôveryhodných službách, kybernetickej bezpečnosti a ochrane utajovaných skutočností (aj s vyhláškami k fyzickej a objektovej bezpečnosti).

Úrad bude ďalej rozvíjať svoje spôsobilosti v oblasti certifikácie mechanických zabezpečovacích, technických zabezpečovacích aj technických prostriedkoch či prostriedkoch šifrovej ochrany informácií. V aktivitách akreditácie certifikačných laboratórií, v súlade s požiadavkami Common Criteria Recognition Arrangement, môže úradu napomôcť projekt Cybersecurity Certification Slovakia, ktorého implementácia sa začala na jeseň 2020.

NBÚ v uplynulom roku verejne deklaroval svoju ambíciu zefektívniť výkon a kvalitu bezpečnostných previerok, čo sa mu v praxi darilo napriek zásadným komplikáciám počas globálnej pandémie.

K prioritám pre rok 2021 patrí aj projekt Elektronické služby spracovania bezpečnostných spisov Národného bezpečnostného úradu. Projekt je zameraný na vytvorenie informačných systémov pre elektronizáciu služieb NBÚ v oblasti ochrany utajovaných skutočností a interných procesov súvisiacich s bezpečnostnými previerkami fyzických osôb a podnikateľov.

Minulý rok úrad začal proces prípravy súťažných podkladov, realizácie verejného obstarávania a projektu Vybudovanie novej Fyzickej a objektovej bezpečnosti NBÚ.

Vláda prijala tento rok Národnú stratégiu kybernetickej bezpečnosti na roky 2021 až 2025, iba nedávno sme odoslali znenie jeho akčného plánu do medzirezortného pripomienkového konania znenie. Ešte v tomto roku odštartuje implementácia priorít v tejto oblasti v podmienkach Slovenskej republiky aj medzinárodnej spolupráce.

NBÚ neustále pracuje na rozvoji expertov z Národného centra kybernetickej bezpečnosti SK-CERT: ich špeciálnym vzdelávaním a odbornými cvičeniami aj na medzinárodnej úrovni.

Po celosvetovej pandémii sa výrazne menia javy a trendy v kybernetickej bezpečnosti. Rizikom sú virtuálne súkromné siete (VPN) a online stretnutia, ktoré potenciálnym útočníkom poskytujú možnosť dostať sa k citlivým informáciám alebo priamo preniknúť do sietí spoločností.

Národné centrum kybernetickej bezpečnosti očakáva pokračovanie trendu rozsiahlych phishingových kampaní, odborníci dlhodobo považujú za jednu z najväčších hrozieb ransomvérové útoky. Na vzostupe budú aj kybernetické útoky sofistikovanou formou umelej inteligencie. NBÚ bude vytrvalo pracovať s partnermi na šírení osvety, rozvoji prevencie aj riešení problémov v tejto oblasti.

podatelna@nbu.gov.sk

+421 2 6869 1111

www.nbu.gov.sk