NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Príloha č. 2

Ročná monitorovacia správa k 31. 12. 2019

Programová štruktúra

0D9 – BEZPEČNOSŤ INFORMÁCIÍ

Zámer: **Informácie chránené v súlade so zákonom o ochrane utajovaných informácií, zákonom o dôveryhodných službách a budovanie spôsobilosti kybernetickej bezpečnosti**
Gestor: **sekcia ekonomiky a prevádzky**
Zodpovedný: **riaditeľ sekcie ekonomiky a prevádzky**

Komentár:

Jednotlivé ciele programu 0D9 – Bezpečnosť informácií v nadväznosti na zámer programu „Informácie chránené v súlade so zákonom o ochrane utajovaných informácií, zákonom o dôveryhodných službách a budovanie spôsobilosti kybernetickej bezpečnosti“ boli v priebehu roka 2019 plnené na požadovanej úrovni. Plnenie programu na jednotlivých úrovniach podprogramov a prvkov ovplyvňujú najmä kvalita a stabilita legislatívneho prostredia, kvantita a stupeň utajenia utajovaných informácií, ktoré vzhľadom na záujem Slovenskej republiky treba chrániť pred neoprávnenou manipuláciou, reálne hrozby a riziká, odborná spôsobilosť zamestnancov, bezpečnostná spoľahlivosť navrhovaných osôb a podnikateľov, súčinnosť orgánov pri poskytovaní informácií pri vykonávaní bezpečnostných previerok a i. Napriek tomu porovnaním plánovaných a dosiahnutých výsledkov možno konštatovať, že výsledky zabezpečujú plnenie zámeru programu. V nadväznosti na stanovené ciele merateľné ukazovatele sú vhodne zvolené a nepredpokladajú sa riziká a odchýlky od rozpočtových zámerov. Ciele sa plnia na základe existujúcich kapacít Národného bezpečnostného úradu v súlade so zásadami efektívnosti a hospodárnosti. Gestori jednotlivých podprogramov a prvkov jednotlivé ciele k 31. 12. 2019 plnia.

Vypracoval: plk. Ing. Anna Friesseová
Schválil: plk. Mgr. Jana Lukáčová

Cieľ 1: *Zaistiť spôsobilosť osôb na ochranu utajovaných informácií*
Gestor: *sekcia previerok*
Zodpovedný: *riaditeľ sekcie previerok*

Názov ukazovateľa		**Rok 2017**	**Rok 2018**	**Rok 2019**	**Rok 2020**	**Rok 2021**
Kvalitné a včasne ukončené previerky personálnej a priemyselnej bezpečnosti	Plán	áno/nie	áno/nie	áno/nie	áno/nie	áno/nie
	Skutočnosť	áno	áno	áno	–	–

Plnenie cieľa:

Hodnotený cieľ sleduje zámer programu „Informácie chránené v súlade so zákonom o ochrane utajovaných informácií, zákonom o dôveryhodných službách a budovanie spôsobilosti kybernetickej bezpečnosti“, vychádza z úlohy úradu zabezpečiť spôsobilosť osôb na ochranu utajovaných informácií v orgánoch verejnej moci a u podnikateľov na požadovanej úrovni dostatočným počtom oprávnených osôb a podnikateľov s platným potvrdením o priemyselnej bezpečnosti, s cieľom minimalizovať riziko postúpenia utajovaných skutočností osobám alebo podnikateľom, ktorých bezpečnostná spoľahlivosť nebola posúdená podľa príslušných právnych predpisov. Dosiahnutie stanoveného cieľa je možné hodnotiť ako efektívne a hospodárne. Na jeho realizácii sa podieľali príslušníci plnením úloh na požadovanej kvantitatívnej a kvalitatívnej úrovni.

Cieľovými skupinami sú navrhované osoby a podnikatelia. Stanovený ukazovateľ nadväzuje na cieľ a monitoruje jeho plnenie, pričom sleduje kvalitné a včasné ukončenie bezpečnostných previerok navrhovaných osôb a podnikateľov.

Od 01. 01. 2019 do 31. 12. 2019 prijal úrad 4 529 žiadostí o vykonanie bezpečnostnej previerky navrhovanej osoby a 100 žiadostí o vydanie potvrdenia o priemyselnej bezpečnosti. Z počtu prijatých žiadostí o vykonanie bezpečnostnej previerky navrhovanej osoby bolo v hodnotenom období ukončených 3 604 bezpečnostných previerok. Z počtu prijatých žiadostí o vydanie potvrdenia o priemyselnej bezpečnosti bolo v hodnotenom období ukončených 58 bezpečnostných previerok. Spolu bolo prijatých 4 629 žiadostí o bezpečnostnú previerku, z toho ukončených bolo 3 662 bezpečnostných previerok.

Vyššie uvedené žiadosti boli vybavované a bezpečnostné previerky ukončené vzhľadom na zákonom stanovené lehoty na rozhodnutie o bezpečnostnej previerke navrhovanej osoby (úrad je povinný rozhodnúť o bezpečnostnej previerke II. stupňa do troch mesiacov od začatia konania, o bezpečnostnej previerke III. stupňa do štyroch mesiacov od začatia konania, o bezpečnostnej previerke IV. stupňa do šiestich mesiacov od začatia konania, a ak nemožno vzhľadom na povahu veci rozhodnúť v uvedených lehotách, môže ich predĺžiť najviac o tri mesiace) a vzhľadom na zákonom stanovené lehoty na vydanie potvrdenia o priemyselnej bezpečnosti (úrad je povinný rozhodnúť o bezpečnostnej previerke pre stupeň utajenia Vyhradené alebo Dôverné do štyroch mesiacov po podaní žiadosti, pre stupeň utajenia Tajné alebo Prísne tajné do siedmich mesiacov po podaní žiadosti, a ak nemožno vzhľadom na povahu veci rozhodnúť v uvedených lehotách, môže ich úrad predĺžiť najviac o tri mesiace).

Možno konštatovať, že v hodnotenom období vzhľadom na vyššie uvedené zákonom stanovené lehoty boli bezpečnostné previerky navrhovaných osôb a bezpečnostné previerky podnikateľov ukončené kvalitne a včas a podarilo sa dosiahnuť reálnu hodnotu ukazovateľa „áno“. Plnenie stanoveného cieľa ovplyvňujú najmä kvalita a stabilita legislatívneho prostredia, kvantita a stupeň utajenia utajovaných skutočností, ktoré vzhľadom na záujem SR treba chrániť pred neoprávnenou manipuláciou, reálne hrozby a riziká, odborná spôsobilosť zamestnancov, bezpečnostná spoľahlivosť navrhovaných osôb a podnikateľov, súčinnosť orgánov pri poskytovaní informácií pri vykonávaní bezpečnostných previerok, plnenie zákonom stanovených povinností navrhovanou osobou v priebehu bezpečnostnej previerky, úroveň bezpečnostného povedomia, personálna stabilita vo vedúcich funkciách v orgánoch verejnej moci a u podnikateľov, ekonomická stabilita podnikateľov, fluktuácia zamestnancov a mnoho ďalších faktorov, ovplyvňujúcich počet žiadostí, priebeh a výsledok bezpečnostných previerok navrhovaných osôb a podnikateľov.

Zdroj získavania údajov: interný
Vypracoval: pplk. JUDr. Zuzana Gavorníková
Schválil: plk. JUDr. Marek Barta

Cieľ 2: Zaistiť technickú spôsobilosť na ochranu utajovaných informácií
Gestor: technická sekcia
Zodpovedný: riaditeľ technickej sekcie

Názov ukazovateľa		**Rok 2017**	**Rok 2018**	**Rok 2019**	**Rok 2020**	**Rok 2021**
Zaistená technická spôsobilosť na ochranu UI	Plán	áno/nie	áno/nie	áno/nie	áno/nie	áno/nie
	Skutočnosť	áno	áno	áno	–	–

Plnenie cieľa:

Jednou z oblastí zaručujúcich technickú spôsobilosť ochrany utajovaných informácií pred ich únikom prostredníctvom *nežiaduceho elektromagnetického vyžarovania* (ďalej len „NEV“) sú merania NEV *technických prostriedkov* (ďalej len „TP“) a *prostriedkov šifrovej ochrany informácií* (ďalej len „PŠOI“) , ako aj zónové merania chránených priestorov, v ktorých budú tieto umiestnené. Merania NEV zariadení TP a PŠOI sa vykonávajú na úrade v TEMPEST laboratóriu, zónové merania chránených

priestorov sa vykonávajú mobilnou meracou aparatúrou. Merania sa vykonávajú na základe žiadostí od orgánov verejnej moci alebo podnikateľov, ktorí budú spracovávať utajované skutočnosti na TP alebo na PŠOI, prípadne ako súčasť procesu certifikácie.

Na vybavenie žiadosti môže byť potrebné zmerať niekoľko zariadení TP, PŠOI alebo priestorov. Výstupom plnenia cieľa sú protokoly, stanoviská a inštalačné záznamy, ktoré sú podkladmi k certifikácii TP alebo PŠOI.

V roku 2019 bolo prijatých 59 žiadostí o stanovisko k certifikácii TP, vykonanie meraní NEV zariadení TP a o vykonanie zónových meraní priestorov, z ktorých bolo vybavených 54. Na základe doručených žiadostí bolo vykonaných 876 meraní zariadení TP a PŠOI a 47 zónových meraní priestorov, na základe ktorých bolo kategorizovaných 241 zariadení TP a 31 priestorov. V roku 2019 bola prijatá 1 žiadosť o vykonanie meraní tienených komôr, na základe ktorej bolo vykonaných 6 meraní útlmu tienenej komory.

Porovnaním plánovaných a dosiahnutých výsledkov možno konštatovať, že výsledky zabezpečujú plnenie stanoveného cieľa, merateľný ukazovateľ je vhodne zvolený a nepredpokladajú sa riziká a odchýlky od rozpočtových zámerov. Cieľ sa plní na základe existujúcich kapacít úradu v súlade so zásadami efektívnosti a hospodárnosti. Výkon meraní NEV je v súlade s potrebami cieľovej skupiny. Avšak vzhľadom na prudký rozvoj nových technológií a tiež inštaláciu zložitých zariadení je žiaduce obstaranie zariadení na vysoko odborné činnosti (napr. zariadenia na vykonávanie špeciálnych analýz elektromagnetických signálov, systém na meranie akustickej nepriezvučnosti atď.). Tiež budú potrebné finančné prostriedky na údržbu, obmenu a pravidelnú kalibráciu techniky a na špeciálne školenia príslušníkov úradu.

Vytvorenie optimálnych podmienok technickej spôsobilosti na ochranu utajovaných informácií je zabezpečované aj akreditáciou komunikačných a informačných systémov pre manipuláciu utajovaných informácií SR, NATO a EÚ, ako aj certifikáciou prostriedkov potrebných na ochranu utajovaných informácií pre rôzne stupne utajenia. V roku 2019 úrad vykonal 2 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, akreditoval 3 systémy pre EÚ v súlade s Rozhodnutím rady (2013/488/EÚ) a 1 systém v súlade s Bezpečnostnou politikou NATO C-M(2002)49. V roku 2019 bolo certifikovaných 164 prostriedkov potrebných na ochranu utajovaných informácií a bolo vydaných 25 dodatkov k už certifikovaným prostriedkom potrebných na ochranu utajovaných informácií.

Zdroj získavania údajov: interný
Vypracoval: pplk. Mgr. Ivan Chrenko
Schválil: pplk. Ing. Bibiána Magáthová, PhD.

Cieľ 3: *Zabezpečiť efektívny systém pre poskytovanie dôveryhodných služieb pre elektronické transakcie na vnútornom trhu v súlade s platným zákonom o dôveryhodných službách*
Gestor: *technická sekcia, odbor bezpečnostnej prevádzky*
Zodpovedný: *riaditeľ odboru bezpečnostnej prevádzky*

Názov ukazovateľa		**Rok 2017**	**Rok 2018**	**Rok 2019**	**Rok 2020**	**Rok 2021**
Efektívny systém pre poskytovanie dôveryhodných služieb	Plán	áno/nie	áno/nie	áno/nie	áno/nie	áno/nie
	Skutočnosť	áno	áno	áno	–	–

Plnenie cieľa:

Zavedenie a zabezpečenie efektívneho systému pre poskytovanie dôveryhodných služieb pre elektronické transakcie na vnútornom trhu v súlade s platným zákonom o dôveryhodných službách je naplnením záväzkov Slovenskej republiky voči Európskej únii v oblasti dohľadu nad poskytovateľmi kvalifikovaných dôveryhodných služieb vyplývajúcich z nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES (ďalej len „nariadenie o eIDAS“) a zároveň plnení

zákonom stanovenej úlohy poskytovať kvalifikované dôveryhodné služby orgánom verejnej moci (do 31. 7. 2019). Stanovený cieľ možno hodnotiť ako relevantný.

Systém v Slovenskej republike (vychádzajúc z nariadenia eIDAS) je založený na PKI infraštruktúre, pričom Národný bezpečnostný úrad je v pozícii tzv. dozorného orgánu. Okrem neho v súčasnosti v prostredí SR pôsobia štyria tzv. poskytovatelia kvalifikovaných dôveryhodných služieb (dva komerčné subjekty a dva štátne).

Sledovaný cieľ možno rozdeliť do dvoch oblastí. Jednou je budovanie efektívneho systému v rámci SR pre poskytovanie kvalifikovaných dôveryhodných služieb ako takých (tzv. národná dôveryhodná infraštruktúra).

Druhým je poskytovanie kvalifikovaných dôveryhodných služieb úradom pre orgány verejnej moci podľa § 11 ods. 2 zákona o dôveryhodných službách. Hodnotený cieľ je vhodne stanovený, je plne aktuálny a prispôsobený skutočným potrebám, ktoré vychádzajú z požiadaviek kladených na Národný bezpečnostný úrad zo zákona o dôveryhodných službách a z nariadenia eIDAS.

Cieľ možno charakterizovať ako strednodobý až dlhodobý a výsledkom jeho plnenia je zabezpečenie tzv. dôveryhodnej národnej infraštruktúry a zároveň z pozície poskytovateľa bezpečné a kvalitné poskytovanie kvalifikovaných dôveryhodných služieb.

Obzvlášť významným prínosom v sledovanom období bola modernizácia koreňovej infraštruktúry a úspešná implementácia projektu poskytovania kvalifikovaných dôveryhodných služieb pre orgány verejnej moci. Očakávané kladné zmeny, ktoré sú výsledkom zavedenia spomínanej služby, sa prejavili okamžite, čo sa odzrkadlilo enormným nárastom počtu žiadostí o poskytovanie kvalifikovaných dôveryhodných služieb, pričom sme v sledovanom období zaznamenali veľký záujem o dané služby zo strany orgánov verejnej moci, čím sa enormne zvýšil objem vydaných certifikátov a vyhotovených časových pečiatok. Čo sa týka trvácnosti zmien, nestanú sa zastaranými v krátkom časovom období a ich charakter bude závisieť od legislatívnych, normatívnych a technických zmien. V sledovanom období došlo k legislatívnej zmene, na základe ktorej k 1. augustu 2019 prišlo k prechodu kompetencií za poskytovanie kvalifikovaných dôveryhodných služieb pre orgány verejnej moci na inú organizáciu (Národná agentúra pre sieťové a elektronické služby). Kompetencia úradu ako orgánu dohľadu podľa článku 17 nariadenia eIDAS ostala nezmenená.

Merateľný ukazovateľ je stanovený vhodne, nadväzuje na cieľ a odráža jeho plnenie. K termínu zhodnocovania plnenia cieľov sa časový plán plní. V rámci procesu plnenia cieľa sa podarilo dosiahnuť kvantifikovaný výstup zhodný s plánovaným. Dosiahnuté výstupy a výsledky zabezpečujú plnenie zámeru programu v plnej miere.

Plnenie cieľa je hodnotené ako efektívne a hospodárne, nakoľko značnú časť činností zabezpečovali príslušníci odboru bezpečnostnej prevádzky, napriek skutočnosti, že sa jedná o vysoko odborné činnosti v oblasti informačných technológií so zameraním na problematiku infraštruktúry verejného kľúča (PKI).

Zdroj získavania údajov: interné zdroje
Vypracoval: mjr. Mgr. Zuzana Halásová, PhD.
Schválil: pplk. Ing. Bibiána Magáthová, PhD.

Cieľ 4 Zabezpečiť otvorený, bezpečný a chránený národný kybernetický priestor
Gestor: Národné centrum kybernetickej bezpečnosti SK-CERT
Zodpovedný: riaditeľ Národného centra kybernetickej bezpečnosti SK-CERT

Názov ukazovateľa		**Rok 2017**	**Rok 2018**	**Rok 2019**	**Rok 2020**	**Rok 2021**
Zvýšená bezpečnosť kybernetického priestoru	Plán	áno/nie	áno/nie	áno/nie	áno/nie	áno/nie
	Skutočnosť	áno	áno	áno	–	–

Plnenie cieľa:

Národná jednotka SK-CERT bola dňom 1. septembra 2019 transformovaná na Národné centrum kybernetickej bezpečnosti SK-CERT, ktoré naďalej rozvíja svoju pôsobnosť a spôsobilosť pri zabezpečovaní otvoreného, bezpečného a chráneného národného kybernetického priestoru. SK-CERT kontinuálne rozvíja svoje interné nástroje a systémy slúžiace na detekciu kybernetických bezpečnostných incidentov a rozposielanie adresných varovaní.

Zdroj získavania údajov: interný
Vypracoval: pplk. Mgr. Beáta Kalininová
Schválil: plk. Mgr. Rastislav Janota

0D901 – OCHRANA UTAJOVANÝCH INFORMÁCIÍ

Zámer: Optimálne podmienky ochrany utajovaných informácií
Gestor: sekcia previerok
Zodpovedný: riaditeľ sekcie previerok

Komentár:

Cieľom ochrany utajovaných informácií je dosiahnutie ich bezpečnosti vytvorením systémových opatrení v jednotlivých oblastiach bezpečnosti.

Plnenie stanovených cieľov v rámci jednotlivých prvkov podprogramu ochrana utajovaných informácií, spôsobilosť osôb na ochranu utajovaných informácií, technická spôsobilosť na ochranu utajovaných informácií a spôsobilosť na ochranu zahraničných utajovaných informácií, pozitívne vplýva na vytváranie vhodných podmienok v jednotlivých oblastiach bezpečnosti (personálna bezpečnosť, priemyselná bezpečnosť, administratívna bezpečnosť, fyzická bezpečnosť a objektová bezpečnosť, bezpečnosť technických prostriedkov), pričom sleduje zámer podprogramu zabezpečiť „optimálne podmienky ochrany utajovaných informácií“.

Cieľom prvku spôsobilosť osôb na ochranu utajovaných informácií v hodnotenom období je zabezpečenie optimálnych podmienok ochrany utajovaných informácií v orgánoch verejnej moci a u podnikateľov dostatočným počtom oprávnených osôb, pričom na zvýšenie úrovne ochrany utajovaných informácií pozitívne vplývajú vykonávané kontroly ochrany utajovaných informácií a zvyšovanie bezpečnostného povedomia vykonávaním skúšok bezpečnostných zamestnancov a preškolením osôb v rôznych oblastiach bezpečnosti.

Výstupom cieľov prvku technická spôsobilosť na ochranu utajovaných informácií je dosiahnutie maximálnej technickej spôsobilosti na ochranu utajovaných informácií. Dosiahnutý výsledok je v plnej miere naplnením potrieb cieľovej skupiny v oblasti akreditácie systémov potrebných na ochranu utajovaných informácií, a tiež v oblasti certifikácii zariadení a prostriedkov potrebných na ochranu utajovaných informácií.

Prvok spôsobilosť na ochranu zahraničných utajovaných informácií je zameraný na vytvorenie podmienok na ochranu utajovaných skutočností poskytnutých a prijatých v rámci medzinárodnej spolupráce, s cieľom zabezpečiť potrebnú úroveň ochrany utajovaných skutočností Slovenskej republiky postupovaných cudzej moci a utajovaných skutočností cudzej moci postupovaných Slovenskej republike.

Na realizácii jednotlivých cieľov prvkov podprogramu sa podieľali príslušníci útvarov úradu.

Vo vzťahu k dosiahnutiu stanovených cieľov v rámci prvkov podprogramu možno kritériá efektívnosti a hospodárnosti hodnotiť ako primerané. Odrazom je plnenie úloh v požadovanej kvalite a kvantite. Účelom hodnotenia je zistiť, či je predmetný podprogram konzistentný s potrebami a úlohami úradu.

Vypracoval: pplk. JUDr. Zuzana Gavorníková
Schválil: plk. JUDr. Marek Barta

0D90101 Spôsobilosť osôb na ochranu utajovaných informácií
Gestor: sekcia previerok
Zodpovedný: riaditeľ sekcie previerok

Komentár:

Dosiahnuté výsledky plnenia jednotlivých cieľov v rámci prvku v hodnotenom období mali priamy vplyv na skvalitnenie stavu a dosiahnutie požadovanej úrovne ochrany utajovaných informácií v orgánoch verejnej moci a u podnikateľov.

Prostredníctvom pravidelného vykonávania kontrol dodržiavania ustanovení zákona o ochrane utajovaných skutočností úrad zisťoval stav ochrany utajovaných informácií (upozorňoval cieľové skupiny na vzniknuté nedostatky, príčiny ich vzniku), čím sa v budúcnosti môže predchádzať ich opakovaniu a tým pozitívne vplývať na zvyšovanie úrovne zabezpečenia ochrany utajovaných informácií.

Vzhľadom na dôležitosť záujmu štátu na ochrane utajovaných informácií zákon umožní prístup k utajovaným informáciám iba vymedzenému okruhu osôb, na ktoré však kladie určité požiadavky. Špecifikuje podmienky, ktoré musí spĺňať oprávnená osoba a podnikateľ počas celej doby prístupu k utajovaným informáciám. Splnenie podmienok pre prístup k utajovaným informáciám zisťoval úrad bezpečnostnou previerkou fyzickej osoby a bezpečnostnou previerkou podnikateľa, pričom cieľom bolo vybaviť všetky žiadosti o vykonanie bezpečnostnej previerky v zákonom stanovených lehotách.

Vykonávaním skúšok bezpečnostných zamestnancov a preškolení v jednotlivých oblastiach bezpečnosti úrad sledoval cieľ zabezpečiť zvyšovanie bezpečnostného povedomia bezpečnostných zamestnancov v jednotlivých orgánoch verejnej moci a podnikateľov.

Vypracoval: pplk. JUDr. Zuzana Gavorníková
Schválil: plk. JUDr. Marek Barta

Cieľ 1 Vykonať kontrolu dodržiavania ustanovení zákona o ochrane utajovaných informácií
Gestor: odbor regulácie a dohľadu
Zodpovedný: riaditeľ odboru regulácie a dohľadu

Názov ukazovateľa		**Rok 2015**	**Rok 2016**	**Rok 2017**	**Rok 2018**	**Rok 2019**	**Rok 2020**	**Rok 2021**
% vykonaných kontrol OUI z ročného plánu kontrol OUI	Plán	100	100	100	100	100	100	100
	Skutočnosť	100	100	100	100	100	–	–

Plnenie cieľa:

V pláne vonkajších kontrol na rok 2019 boli schválené 4 kontroly ochrany utajovaných skutočností.

V novembri 2019 bola jedna plánovaná kontrola ochrany utajovaných skutočností z plánu vonkajších kontrol na rok 2019 vypustená. Možno teda konštatovať, že vonkajšie kontroly ochrany utajovaných skutočností boli podľa schváleného plánu vonkajších kontrol na rok 2019 vykonané v plnom rozsahu.

Zdroj získavania údajov: Počet vykonaných vonkajších kontrol, Plán vonkajších kontrol na rok 2019
Vypracoval: por. Mgr. Veronika Vanyová
Schválil: plk. Ing. JUDr. Alexandra Kaľavská Dianišková

Cieľ 2: Zabezpečiť spôsobilosť osôb na ochranu utajovaných informácií
Gestor: sekcia previerok
Zodpovedný: riaditeľ sekcie previerok

Názov ukazovateľa		**Rok 2015**	**Rok 2016**	**Rok 2017**	**Rok 2018**	**Rok 2019**	**Rok 2020**	**Rok 2021**
% vybavených žiadostí o vykonanie bezpečnostnej previerky v zákonnej lehote	Plán	100	100	100	100	99	97	97
	Skutočnosť	99,77	98,83	99,83	99,06	98,96	–	–

Plnenie cieľa:

Vzhľadom na zákonom stanovené lehoty na rozhodnutie o bezpečnostnej previerke príslušného stupňa a na zákonom stanovené lehoty na vydanie potvrdenia o priemyselnej bezpečnosti príslušného stupňa mal úrad od 01. 01. 2019 do 31. 12. 2019 vybaviť 4 528 žiadostí o vykonanie bezpečnostnej previerky. V hodnotenom období bolo vybavených 4 481 žiadostí, čo predstavuje 98,96 % vybavených žiadostí. Percento vybavených žiadostí z počtu prijatých žiadostí, ktoré možno vybaviť vzhľadom na zákonom stanovené lehoty vyjadruje plnenie stanoveného cieľa.

Formulácia cieľa zabezpečiť spôsobilosť fyzických osôb a právnických osôb na ochranu utajovaných informácií, korešponduje so skutočnými potrebami úradu, pričom hodnotený cieľ je stanovený v nadväznosti na zámer podprogramu tak, aby boli zabezpečené optimálne podmienky ochrany utajovaných informácií osobami spôsobilými na ich ochranu.

Stanovený cieľ je merateľný a kvantifikovateľný vhodným merateľným ukazovateľom výsledku, pričom obsahuje konkrétnu cieľovú hodnotu, t. j. 99 % vybavených žiadostí.

Na plnení cieľa sa podieľali príslušníci vybavovaním žiadostí o vykonanie bezpečnostnej previerky a žiadostí o vydanie potvrdenia o priemyselnej bezpečnosti na požadovanej kvantitatívnej a kvalitatívnej úrovni.

Pri plnení cieľa sa kládol dôraz na účelnosť vynakladania finančných prostriedkov z hľadiska množstva, kvality a času v súlade so zásadou racionálneho hospodárenia. Počas hodnoteného obdobia sa formovali podmienky na ochranu utajovaných skutočností v rámci procesov vytvárania vhodných organizačných, legislatívnych a technických podmienok.

Cieľovými skupinami sú navrhované osoby a podnikatelia. Stanovený cieľ sleduje zámer vybaviť v hodnotenom období všetky žiadosti o vykonanie bezpečnostnej previerky navrhovanej osoby a žiadosti o vydanie potvrdenia o priemyselnej bezpečnosti podnikateľa tak, aby boli bezpečnostné previerky vykonané v zákonom stanovenej lehote kvalitne a v čo najkratších lehotách.

Plnenie stanoveného cieľa v priebehu hodnoteného obdobia by mohla ovplyvniť najmä kvalita a stabilita legislatívneho prostredia, kvantita a stupeň utajenia utajovaných skutočností, ktoré vzhľadom na záujem SR treba chrániť pred neoprávnenou manipuláciou, neúplnosť podkladových materiálov z dôvodu nedostatočnej súčinnosti štátnych orgánov a právnických osôb, nerealizovanie niektorých procesných úkonov navrhovanými osobami resp. ich nerealizovanie v stanovených termínoch, neúmerný nárast počtu žiadostí, napr. z dôvodu novej právnej úpravy, uplynutia doby platnosti veľkého počtu osvedčení, fluktuácia príslušníkov, nedostatočný personálny alebo materiálny substrát atď.

Na základe analýzy vykonanej v súvislosti s vyhodnocovaním cieľa možno konštatovať, že 47 žiadostí o vykonanie bezpečnostnej previerky navrhovanej osoby a o vydanie potvrdenia o priemyselnej bezpečnosti podnikateľa nebolo možné vybaviť v zákonom stanovených lehotách. Výšku percenta v hodnotenom období ovplyvnili najmä faktory, ako nesplnenie si zákonom stanovených povinností navrhovanou osobou v priebehu bezpečnostnej previerky, nedodržanie lehoty zo strany štátnych orgánov a iných právnických osôb poskytujúcich informácie potrebné na vykonanie bezpečnostnej previerky, nedodržanie lehoty zo strany štátneho orgánu na predloženie materiálov spolu s vyhodnotením a návrhom na spôsob ukončenia bezpečnostnej previerky a poskytnutie

informácií v iných než zákonom stanovených lehotách príslušným partnerským bezpečnostným orgánom. Udržateľnosť cieľa v budúcnosti závisí od vyššie uvedených faktorov.

Zdroj získavania údajov: interný
Vypracoval: pplk. JUDr. Zuzana Gavorníková
Schválil: plk. JUDr. Marek Barta

Cieľ 3 Zvýšenie bezpečnostného povedomia
Gestor: kancelária úradu
Zodpovedný: riaditeľ kancelárie úradu

Názov ukazovateľa		**Rok 2017**	**Rok 2018**	**Rok 2019**	**Rok 2020**	**Rok 2021**
% vykonaných skúšok a preškolení z požadovaného počtu	Plán	100	100	100	100	100
	Skutočnosť	100	100	100	–	–

Plnenie cieľa:

Odbor vonkajších vzťahov kancelárie úradu v rámci zvyšovania bezpečnostného povedomia vykonáva skúšky bezpečnostného zamestnanca a preškolenia osôb v rôznych oblastiach bezpečnosti. V roku 2019 bol úrad požiadaný o vykonanie 258 skúšok bezpečnostného zamestnanca. Skúšku bezpečnostného zamestnanca vykonalo 246 uchádzačov úspešne a 12 boli neúspešní. Z celkového počtu uchádzačov, na ktorých bola zaslaná žiadosť o vykonanie skúšky bezpečnostného zamestnanca, odbor vonkajších vzťahov kancelárie úradu pozval všetkých 258 uchádzačov.

V tomto období odbor vonkajších vzťahov zverejnil na webovom sídle úradu rôzne témy preškolení, na ktoré sa mohli záujemcovia prihlásiť. Vykonaných bolo celkovo 37 preškolení, ktorých sa zúčastnilo 655 osôb.

V súvislosti s vykonávaním skúšok bezpečnostného zamestnanca a preškoľovania osôb v oblastiach bezpečnosti možno konštatovať ich pozitívny vplyv na zvýšenie úrovne zabezpečenia ochrany utajovaných skutočností v orgánoch verejnej moci a u podnikateľov.

Zdroj získavania údajov: interný
Vypracoval: pplk. JUDr. Andrea Senková
Schválil: plk. Mgr. Marián Kramár

0D90102 Technická spôsobilosť na ochranu utajovaných informácií
Gestor: technická sekcia
Zodpovedný: riaditeľ technickej sekcie

Komentár:

Ciele boli stanovené v súlade požiadavkami platnej legislatívy SR (najmä zákona č. 215/2004 o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov, vrátane súvisiacich vyhlášok) a s požiadavkami vyplývajúcimi z predpisov NATO a EÚ. Výstupom cieľa je zabezpečenie plnenia zámeru dosiahnuť maximálnu technickú spôsobilosť na ochranu utajovaných informácií, pričom dosiahnutý výsledok je v plnej miere naplnením potreby cieľovej skupiny v oblasti akreditácie systémov potrebných na ochranu utajovaných informácií, tak i v oblasti certifikácie zariadení a prostriedkov potrebných na ochranu utajovaných informácií. Dosiahnutie stanovených cieľov je možné hodnotiť ako efektívne a hospodárne. Na ich realizácii sa podieľali príslušníci odborných útvarov technickej sekcie. Na základe získaných výsledkov možno konštatovať, že zabezpečenie technickej spôsobilosti na ochranu utajovaných informácií sa plní v súlade so stanovenými cieľmi a pri plnení cieľov „akreditácia systémov potrebných na ochranu utajovaných informácií“ a „certifikácia zariadení a prostriedkov potrebných na ochranu utajovaných informácií“ sa do budúcnosti nepredpokladajú žiadne riziká a odchýlky od rozpočtových zámerov.

Vypracoval: pplk. Mgr. Ivan Chrenko
Schválil: pplk. Ing. Bibiána Magáthová, PhD.

Cieľ 1: Akreditácia systémov potrebných na ochranu utajovaných informácií
Gestor: technická sekcia, odbor certifikácie a akreditácie
Zodpovedný: riaditeľ odboru certifikácie a akreditácie

Názov ukazovateľa		**Rok 2015**	**Rok 2016**	**Rok 2017**	**Rok 2018**	**Rok 2019**	**Rok 2020**	**Rok 2021**
% vybavených žiadostí v zákonom stanovenej lehote	Plán	97	97	97	97	97	97	97
	Skutočnosť	100	100	100	100	100	–	–

Plnenie cieľa:

V roku 2019 úrad vykonal 2 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 3 systémy pre EÚ v súlade s Rozhodnutím rady (2013/488/EÚ) a 1 systém v súlade s Bezpečnostnou politikou NATO CM(2002)49.

V tomto roku boli prijaté ďalšie 2 žiadosti (jedna pre akreditáciu 2 systémov EÚ a druhá pre akreditáciu systému NATO). Nakoľko nebola dodaná kompletná dokumentácia k akreditácii týchto systémov a z dôvodu inšpekcií EÚ a NATO bola akreditácia presunutá do roku 2020, pričom nebude prekročená zákonom stanovená lehota.

Akreditáciou systémov potrebných na ochranu utajovaných informácií sa zabezpečuje vytvorenie optimálnych podmienok technickej spôsobilosti na ochranu utajovaných informácií v komunikačných a informačných systémoch. Porovnaním plánovaných a dosiahnutých výsledkov možno konštatovať, že výsledky zabezpečujú plnenie stanoveného cieľa a do budúcnosti nepredpokladajú žiadne riziká a odchýlky od rozpočtových zámerov.

Zdroj získavania údajov: Údaje na plnenie cieľa 1 sú získavané z interných zdrojov.
Vypracoval: pplk. Mgr. Ivan Chrenko a por. Ing. Tomáš Holienka
Schválil: mjr. Ing. Marek Patsch

Cieľ 2: Certifikácia zariadení a prostriedkov potrebných na ochranu utajovaných informácií
Gestor: technická sekcia, odbor certifikácie a akreditácie
Zodpovedný: riaditeľ odboru certifikácie a akreditácie

Názov ukazovateľa		**Rok 2015**	**Rok 2016**	**Rok 2017**	**Rok 2018**	**Rok 2019**	**Rok 2020**	**Rok 2021**
% vybavených žiadostí v zákonom stanovenej lehote	Plán	97	97	97	97	97	97	97
	Skutočnosť	100	100	100	100	100	–	–

Plnenie cieľa:

Cieľ je stanovený v súlade požiadavkami platnej legislatívy SR a s požiadavkami vyplývajúcimi z predpisov NATO a EÚ. V rámci plnenia cieľa boli podľa zákona č. 215/2004 o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov, certifikované mechanické zábranné prostriedky a technické zabezpečovacie prostriedky (ďalej len „MZP a TZP“), technické prostriedky (ďalej len „TP“) a prostriedky šifrovej ochrany informácii (ďalej len „PŠOI“).

V roku 2019 bolo celkovo prijatých 173 žiadostí o certifikáciu (MZP a TZP 90, TP 83, PŠOI 11) a 25 žiadostí o vydanie dodatku (TP 24, PŠOI 1). Z celkového počtu prijatých žiadostí bolo vybavených 164 žiadostí (MZP a TZP 86, TP 67, PŠOI 11) a 25 dodatkov (TP 24, PŠOI 1). Žiadosti, ktoré spĺňali požadované náležitosti boli všetky vybavené v zákonom stanovenej lehote.

Na základe získaných výsledkov možno konštatovať, že cieľ je stanovený v súlade s potrebami žiadateľov, ktorí zabezpečujú ochranu utajovaných informácií a plní sa na základe existujúcich kapacít úradu v súlade so zásadami efektívnosti a hospodárnosti. Pri plnení cieľa sa nepredpokladajú žiadne riziká a odchýlky od rozpočtových zámerov.

Zdroj získavania údajov: Údaje na plnenie cieľa 2 sú získavané z interných zdrojov.
Vypracoval: pplk. Mgr. Ivan Chrenko
Schválil: mjr. Ing. Marek Patsch

0D90103 Spôsobilosť na ochranu zahraničných utajovaných informácií
Gestor: kancelária úradu
Zodpovedný: riaditeľ kancelárie úradu

Cieľ 1: Poskytovanie služieb centrálneho registra podľa požiadaviek zákona o ochrane utajovaných informácií
Gestor: kancelária úradu, odbor administratívnych činností
Zodpovedný: riaditeľ odboru administratívnych činností

Názov ukazovateľa		**Rok 2015**	**Rok 2016**	**Rok 2017**	**Rok 2018**	**Rok 2019**	**Rok 2020**	**Rok 2021**
% poskytnutých služieb z počtu žiadosti o poskytnutie služby	Plán	91	93	94	97	97	97	97
	Skutočnosť	91	97	98	98	99	–	–

Plnenie cieľa:

V roku 2019 bolo plánované vykonať 97 % poskytnutých služieb.

Dosiahnuté výsledky v období od 01. 01. 2019 do 31. 12. 2019 zabezpečili plnenie zámeru programu. V sledovanom období bolo vykonané plnenie na 99 %.

Zadefinovaný cieľ prvku je prispôsobený skutočným potrebám a plne korešponduje s vývojom potrieb úradu.

Ochrana zahraničných utajovaných informácií sa zabezpečuje splnením osobitných podmienok podľa zákona. Dokladom o splnení zákonných podmienok je úradom vydaný certifikát o bezpečnostnej previerke fyzickej osoby a certifikát podnikateľa o priemyselnej bezpečnosti. Splnením uvedených podmienok vzniká spôsobilosť oboznamovať sa s príslušnými zahraničnými utajovanými informáciami. Pre fyzické prijímanie zahraničných informácií je povinnosťou subjektov zriadiť register utajovaných skutočností. Následne je oprávnený priamo prijímať utajované skutočnosti NATO a EÚ označené stupňom utajenia Vyhradené s ohlasovacou povinnosťou smerom k centrálnemu registru. Celkovo v sledovanom období prijala Slovenská republika 7 298 zahraničných utajovaných skutočností označených stupňom utajenia Vyhradené, z toho 7 212 zaevidovali registre utajovaných skutočností.

Cieľ je merateľný a kvantifikovateľný vhodným merateľným ukazovateľom výsledku, pričom obsahuje konkrétnu cieľovú hodnotu – 99 % poskytnutých služieb z celkového počtu žiadostí o poskytnutie služby v hodnotenom roku.

Cieľovou skupinou sú navrhované osoby, orgány verejnej moci a podnikateľské subjekty. Stanovený cieľ sleduje poskytnúť v hodnotenom období všetky služby tak, aby boli vykonané kvalitne a v najkratších možných lehotách.

Stanovený cieľ vystihuje zámer podprogramu a naďalej ostáva aktuálny. Jeho plnenie ovplyvňuje najmä kvalita a stabilita legislatívneho prostredia, kvantita a stupeň utajenia utajovaných skutočností, ktoré je vzhľadom na záujmy Slovenskej republiky potrebné ochraňovať pred neoprávnenou manipuláciou. Na plnenie cieľa vplýva aj mnoho ďalších faktorov, ktoré ovplyvňujú počty žiadostí o poskytnutie služieb centrálneho registra.

Zdroj získavania údajov: interný
Vypracoval: mjr. Mgr. Dana Ružovičová
Schválil: plk. Mgr. Mária Rejdová

0D903 – RIADENIE A PODPORA PROGRAMOV

Zámer: **Kvalitne fungujúce podporné útvary**
Gestor: **sekcia ekonomiky a prevádzky**
Zodpovedný: **riaditeľ sekcie ekonomiky a prevádzky**

Komentár:

Potreby podmieňujúce existenciu podprogramu v nadväznosti na stanovené ciele jednotlivých podprogramov a prvkov programu 0D9 – Bezpečnosť informácií stále pretrvávajú. Ciele stanovené v tomto podprograme sú plnené kvalitne a včas tak, aby sa odborným útvarom zabezpečili kvalitné podmienky na dosahovanie zámeru programu. Merateľné ukazovatele sú stanovené vhodne, nadväzujú na ciele a odrážajú ich plnenie. Dosiahnuté výstupy a výsledky zabezpečujú plnenie zámeru programu v plnej miere.

Vypracoval: plk. Ing. Anna Friesseová
Schválil: plk. Mgr. Jana Lukáčová

Cieľ 1: *Plnenie úloh pri zabezpečovaní činnosti úradu*
Gestor: *sekcia ekonomiky a prevádzky*
Zodpovedný: *riaditeľ sekcie ekonomiky a prevádzky*

Názov ukazovateľa		**Rok 2015**	**Rok 2016**	**Rok 2017**	**Rok 2018**	**Rok 2019**	**Rok 2020**	**Rok 2021**
Zabezpečenie plnenia stanovených úloh	Plán	áno/nie	áno/nie	áno/nie	áno/nie	áno/nie	áno/nie	áno/nie
	Skutočnosť	Áno	áno	áno	áno	áno	–	–

Plnenie cieľa:

Stanovený cieľ je aktuálny a korešponduje so skutočnými potrebami odborných útvarov. Cieľ bol stanovený v nadväznosti na zámer podprogramu a programu. Plnenie úloh pri zabezpečovaní činnosti úradu jednoznačne podporuje zámer podprogramu, to znamená aby jednotlivé podporné útvary vykonávali svoje činnosti kvalitne tak, aby svojím fungovaním a kvalitou práce zabezpečili odborným útvarom podmienky na dosahovanie zámeru programu. Údaje o plnení príslušného cieľa sú ľahko dostupné v nadväznosti na spätnú väzbu od odborných útvarov s poukázaním na plnenie jednotlivých cieľov v rámci programového rozpočtovania. Úlohy, ktoré sú stanovené podporným útvarom sú plnené v súlade so stanovenými termínmi. Zodpovednosť za plnenie jednotlivých úloh má riaditeľ príslušného útvaru, ktorému plnenie úlohy vyplýva z činnosti útvaru. Cieľ je pritom možné prispôsobiť skutočným potrebám.

Aktivity uskutočnené počas hodnoteného obdobia boli transformované do skutočných výsledkov v súlade s časovým harmonogramom plnenia úloh. Napríklad z návrhov na zahraničné služobné cesty a prijatia boli realizované len skutočne nevyhnutné cesty a prijatia, ktoré bezprostredne súviseli s plnením kľúčových úloh úradu pri súčasnom dodržaní finančnej disciplíny. Vo vzťahu k disponibilným finančným prostriedkom v rámci hodnoteného obdobia podporné útvary maximalizovali výsledky svojej činnosti. V rámci materiálneho zabezpečovania boli vstupy realizované za podmienky najlepšia kvalita/najlepšia cena zodpovedným prístupom a dôsledným uplatňovaním prieskumu trhu. Podporné útvary plnili a zabezpečovali svoje úlohy stanovením požiadavky na kvalitu a k tomu zodpovedajúcu najnižšiu cenu.

Za hodnotené obdobie boli vypracované odborné stanoviská k predkladaným návrhom právnych predpisov. Uvedené stanoviská výrazne prispeli ku skvalitneniu práce odborných útvarov.

Vplyv plnenia úloh podporných útvarov sa v sledovanom období rozšíril aj mimo cieľovú skupinu (cieľovou skupinou v podmienkach úradu sú odborné útvary). Činnosť kancelárie úradu v oblasti medzinárodnej spolupráce, negociácie a prípravy medzinárodných dohôd ako aj plnenie úloh v oblasti legislatívy má významný vplyv na činnosť ostatných rezortov.

Zmeny, ktoré sa dosiahli, resp. ktoré sa očakávajú v budúcnosti, majú dlhodobý charakter a je vysoká pravdepodobnosť, že dosiahnuté výsledky budú udržateľné v dlhodobom časovom horizonte. V súčasnosti nie je predpoklad, že by na udržanie dosiahnutých výsledkov boli potrebné dodatočné finančné zdroje.

Zdroj získavania údajov: interný
Vypracoval: plk. Ing. Anna Friesseová
Schválil: plk. Mgr. Jana Lukáčová

Cieľ 2: Plnenie úloh pri zabezpečení funkčnosti technologických zariadení úradu
Gestor: technická sekcia, odbor bezpečnostnej prevádzky
Zodpovedný: riaditeľ odboru bezpečnostnej prevádzky

Názov ukazovateľa		**Rok 2015**	**Rok 2016**	**Rok 2017**	**Rok 2018**	**Rok 2019**	**Rok 2020**	**Rok 2021**
Zabezpečenie funkčnosti technologických zariadení	Plán	áno/nie	áno/nie	áno/nie	áno/nie	áno/nie	áno/nie	áno/nie
	Skutočnosť	áno	áno	áno	áno	áno	–	–

Plnenie cieľa:

Hlavnou úlohou vyplývajúcou z plnenia cieľa je zabezpečiť funkčnosť technologických zariadení nasadených v rámci komunikačných a informačných systémov, ktoré sú prevádzkované v rámci úradu, realizovať činnosti pri ich správe, udržiavať ich v prevádzkyschopnom stave a rozširovať ich podľa schválených koncepčných zámerov.

Počas roka bola trvale zabezpečovaná funkčnosť technologických zariadení, ktoré tvoria súčasť najmä týchto hlavných systémov úradu:

- správa externého webového sídla úradu,
- správa interného webového sídla úradu,
- správa mailových serverov úradu – vnútorná a vonkajšia pošta úradu,
- technologická správa automatizovaného informačného systému pre správu registratúry,
- technologická správa právneho softvéru ASPI,
- technologická správa elektronického protokolu pre evidenciu utajovaných skutočností,
- technologická správa informačného systému evidencie vystavených a vrátených certifikátov pre NATO a EÚ,
- technologická správa automatizovaného informačného systému pre centrálny register,
- technologická správa serverov informačného systému Previerka,
- technologická správa ekonomického a personálneho informačného systému,
- technologická správa certifikačných autorít úradu
- správa informačného systému Integrovaná báza dát,
- správa sieťovej infraštruktúry úradu,
- administrácia digitálneho multifunkčného systému,
- administrácia liniek a trunkov a optického pripojenia,
- administrácia tarifikačného systému,
- administrácia VPS NBÚ – Brusel (NATO, EÚ),
- správa komunikačno-informačného systému Apeiron.

Prevádzkové nedostatky boli odstraňované vlastnými silami. Identifikované nedostatky technológie úradu bolo navrhnuté riešiť komplexnými projektami (serverovňa, informačný systém pre elektronizáciu služieb NBÚ v oblastiach ochrany utajovaných skutočností a interných procesov – IS OUSIP, infraštruktúra, VoIP).

Projekt VoIP bol začatý v roku 2018 a úspešne odovzdaný do ostrej prevádzky k 01. 04. 2019. Projekt IS OUSIP bol začatý v roku 2018 a ukončený 31. 05. 2019, v súčasnosti prebieha proces certifikácie riešenia. V najbližšom období bude potrebné realizovať projekt serverovne a projekt na obnovu infraštruktúry, aby sa odstránilo zvýšené riziko prevádzkových havárií.

K termínu zhodnocovania plnenia cieľov sa časový plán plní. Dosiahnuté výstupy a výsledky zabezpečujú plnenie zámeru programu. Na základe aktuálnych výsledkov hodnotenia stavu sa konštatuje, že sa ku dňu hodnotenia podarilo dosiahnuť reálnu hodnotu ukazovateľa „áno“.

Zdroj získavania údajov: Prevádzkové záznamy OBPr
Vypracoval: mjr. Mgr. Zuzana Halásová, PhD.
Schválil: pplk. Ing. Bibiána Magáthová, PhD.

0D904 – DÔVERYHODNÉ SLUŽBY

Zámer: **Zabezpečiť optimálne podmienky na poskytovanie dôveryhodných služieb v súlade s platným zákonom o dôveryhodných službách**
Gestor: **technická sekcia**
Zodpovedný: **riaditeľ technickej sekcie**

Komentár:

Systém poskytovania dôveryhodných služieb v Slovenskej republike (vychádzajúc z nariadenia eIDAS) je založený na PKI infraštruktúre, pričom Národný bezpečnostný úrad je v pozícii tzv. dozorného orgánu. Okrem neho v súčasnosti v prostredí SR pôsobia štyria tzv. poskytovatelia kvalifikovaných dôveryhodných služieb (dva komerčné subjekty a dva štátne). V sledovanom období došlo k legislatívnej zmene, na základe ktorej k 1. augustu 2019 prišlo k prechodu kompetencií za poskytovanie kvalifikovaných dôveryhodných služieb pre orgány verejnej moci na inú organizáciu (Národná agentúra pre sieťové a elektronické služby). Kompetencia úradu ako orgánu dohľadu podľa článku 17 nariadenia eIDAS ostala nezmenená. Vonkajšie kontroly kvalifikovaných poskytovateľov dôveryhodných služieb sa v súlade s aktualizovaným plánom vonkajších kontrol na rok 2019 nevykonávali. V súlade s plánom výkonu posudzovania zhody nad kvalifikovanými poskytovateľmi dôveryhodných služieb boli všetky naplánované posúdenia vykonané v plnom rozsahu. Možno konštatovať, že boli zabezpečené optimálne podmienky na poskytovanie dôveryhodných služieb v súlade s platným zákonom o dôveryhodných službách.

Vypracoval: npor. Ing. Michaela Špeťková
Schválil: pplk. Ing. Bibiána Magáthová, PhD.

Cieľ 1: *Zabezpečiť dohľad nad poskytovateľmi dôveryhodných služieb*
Gestor: *odbor regulácie a dohľadu*
Zodpovedný: *riaditeľ odboru regulácie a dohľadu*

Názov ukazovateľa		**Rok 2017**	**Rok 2018**	**Rok 2019**	**Rok 2020**	**Rok 2021**
% vykonaných dohľadov nad poskytovateľmi dôveryhodných služieb	Plán	100	100	100	100	100
	Skutočnosť	100	100	100	–	–

Plnenie cieľa:

V pláne vonkajších kontrol na rok 2019 bola schválená 1 vonkajšia kontrola kvalifikovaného poskytovateľa dôveryhodných služieb. V novembri 2019 bola plánovaná kontrola kvalifikovaného poskytovateľa služieb z plánu vonkajších kontrol na rok 2019 vypustená. Možno teda konštatovať, že vonkajšie kontroly kvalifikovaných poskytovateľov dôveryhodných služieb boli podľa schváleného plánu vonkajších kontrol na rok 2019 vykonané v plnom rozsahu. V pláne výkonu posudzovania zhody nad kvalifikovanými poskytovateľmi dôveryhodných služieb boli na rok 2019 plánované 4 posúdenia, ktoré boli podľa plánu vykonané v plnom rozsahu.

Zdroj získavania údajov: Počet vykonaných vonkajších kontrol, Plán vonkajších kontrol na rok 2019, Posúdenie auditných správ pre certifikačný audit
Vypracoval: por. Mgr. Veronika Vanyová
Schválil: plk. Ing. JUDr. Alexandra Kaľavská Dianišková

0D905 – KYBERNETICKÁ BEZPEČNOSŤ

Zámer: **Zabezpečiť budovanie spôsobilosti na úseku kybernetickej bezpečnosti**
Gestor: **Národné centrum kybernetickej bezpečnosti SK-CERT**
Zodpovedný: **riaditeľ Národného centra kybernetickej bezpečnosti SK-CERT**

Komentár:

Národná jednotka SK-CERT bola dňom 1. septembra 2019 transformovaná na Národné centrum kybernetickej bezpečnosti SK-CERT, ktoré naďalej buduje a rozvíja spôsobilosti v kybernetickom priestore s celoslovenskou pôsobnosťou a zodpovednosťou. Z tejto pozície úrad zabezpečuje služby spojené s riadením bezpečnostných incidentov, odstraňovaním ich následkov a následnou obnovou činnosti informačných systémov v spolupráci s vlastníkmi a prevádzkovateľmi týchto systémov. Medzi ďalšie činnosti SK-CERT patria analytické činnosti, výskum, rozširovanie bezpečnostného povedomia a vzdelávanie v oblasti kybernetickej bezpečnosti.

Vypracoval: pplk. Mgr. Beáta Kalininová
Schválil: plk. Mgr. Rastislav Janota

Cieľ 1: *Vytvoriť optimálne legislatívne podmienky pre kybernetickú bezpečnosť SR*
Gestor: *odbor regulácie a dohľadu*
Zodpovedný: *riaditeľ odboru regulácie a dohľadu*

Názov ukazovateľa		**Rok 2017**	**Rok 2018**	**Rok 2019**	**Rok 2020**	**Rok 2021**
Vytvorenie optimálnych legislatívnych podmienok	Plán	áno/nie	áno/nie	áno/nie	áno/nie	áno/nie
	Skutočnosť	áno	áno	áno	–	–

Plnenie cieľa:

Na úseku kybernetickej bezpečnosti dňa 01. 01. 2019 nadobudla účinnosť Vyhláška, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení. Dňa 01. 01. 2020 nadobudne účinnosť Vyhláška Národného bezpečnostného úradu č. 436/2019 Z. z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora. Možno teda konštatovať, že v roku 2019 boli vytvorené legislatívne podmienky pre kybernetickú bezpečnosť v Slovenskej republike.

Zdroj získavania údajov: www.slov-lex.sk
Vypracoval: por. Mgr. Veronika Vanyová
Schválil: plk. Ing. JUDr. Alexandra Kaľavská Dianišková

Cieľ 2: *Vytvoriť optimálne technické podmienky pre kybernetickú bezpečnosť SR*
Gestor: *Národné centrum kybernetickej bezpečnosti SK-CERT*
Zodpovedný: *riaditeľ Národného centra kybernetickej bezpečnosti SK-CERT*

Názov ukazovateľa		**Rok 2017**	**Rok 2018**	**Rok 2019**	**Rok 2020**	**Rok 2021**
Vytvorenie optimálnych technických podmienok	Plán	áno/nie	áno/nie	áno/nie	áno/nie	áno/nie
	Skutočnosť	áno	áno	áno	-	-

Plnenie cieľa:

Národná jednotka SK-CERT, ktorá bola dňom 1. septembra 2019 transformovaná na Národné centrum kybernetickej bezpečnosti SK-CERT, pokračuje v budovaní modernej infraštruktúry pre vytvorenie optimálnych podmienok vysokej úrovne kybernetickej bezpečnosti nielen na pracovisku SK-CERT ale aj implementáciou najnovších technologických trendov v rámci národného kybernetického priestoru.

Zdroj získavania údajov: interné
Vypracoval: pplk. Mgr. Beáta Kalininová
Schválil: plk. Mgr. Rastislav Janota

0D90501-NP Národný systém riadenia incidentov kybernetickej bezpečnosti vo verejnej správe
Gestor: Národné centrum kybernetickej bezpečnosti SK-CERT
Zodpovedný: riaditeľ Národného centra kybernetickej bezpečnosti SK-CERT

Cieľ 1: Zvýšenie kybernetickej bezpečnosti v spoločnosti
Gestor: Národné centrum kybernetickej bezpečnosti SK-CERT
Zodpovedný: riaditeľ Národného centra kybernetickej bezpečnosti SK-CERT

Názov ukazovateľa		**Rok 2019**	**Rok 2020**
Dodatočný počet informačných systémov verejnej správy s implementovaným nástrojom na rozpoznávanie, monitorovanie a riadenie bezpečnostných incidentov	Plán	0	550
	Skutočnosť	0	–
Počet informačných systémov VS zapojených do centrálneho systému monitorovania bezpečnosti v rámci VS	Plán	0	550
	Skutočnosť	0	–
Počet nasadených nástrojov na rozpoznávanie, monitorovanie a riadenie bezpečnostných incidentov	Plán	0	1
	Skutočnosť	0	–

Plnenie cieľa:

Hlavným cieľom projektu je rozšírenie spôsobilosti v riešení kybernetických bezpečnostných incidentov prostredníctvom vytvorenia siete odborne a technicky vybavených jednotiek pre riešenie kybernetických bezpečnostných incidentov (CSIRT) na celonárodnej úrovni. Ich úlohou bude vykonávanie preventívnych a reaktívnych opatrení v oblasti svojho pôsobenia a poskytovanie relevantných informácií o kybernetických incidentoch SK-CERT. SK-CERT v súčasnosti tento projekt implementuje.

Zdroj získavania údajov: interné
Vypracoval: pplk. Mgr. Beáta Kalininová
Schválil: plk. Mgr. Rastislav Janota

0D90502 Vybudovanie centra simulácie, výskumu a výuky kybernetických hrozieb a kybernetickej bezpečnosti
Gestor: Národné centrum kybernetickej bezpečnosti SK-CERT
Zodpovedný: riaditeľ Národného centra kybernetickej bezpečnosti SK-CERT

Cieľ 1: Vytvorenie podmienok pre simuláciu, výskum a výuku kybernetických hrozieb a kybernetickej bezpečnosti
Gestor: Národné centrum kybernetickej bezpečnosti SK-CERT
Zodpovedný: riaditeľ Národného centra kybernetickej bezpečnosti SK-CERT

Názov ukazovateľa		**Rok 2019**	**Rok 2020**	**Rok 2021**
Počet vybudovaných učební	Plán	0	3	–
	Skutočnosť	0	–	–

Plnenie cieľa:

Projekt Centra simulácie, výskumu a výuky kybernetických hrozieb a kybernetickej bezpečnosti je národným projektom, ktorého cieľom je vytvoriť dostupnú, kvalitnú a širokospektrálnu platformu vzdelávania a tréningu v oblasti kybernetickej bezpečnosti. Vytvorí sa tak priestor na vzdelávanie kvalifikovaných profesionálov najmä v oblasti štátnej a verejnej správy, prevádzkovateľov základných služieb a akademickej obce. Edukácia prostredníctvom centra simulácie, výskumu a výuky kybernetických hrozieb a kybernetickej bezpečnosti týchto cieľových skupín zabezpečí dostatok

kvalifikovaného personálu, ktorý rozumie problematike kybernetickej bezpečnosti a vie pružne reagovať na hrozby v kybernetickom prostredí Slovenskej republiky v prípade regionálnych aj globálnych incidentov.

Zdroj získavania údajov: interné
Vypracoval: pplk. Mgr. Beáta Kalininová
Schválil: plk. Mgr. Rastislav Janota

Cieľ 2: Zvyšovanie povedomia, zručnosti, metodickej a praktickej pripravenosti na kybernetické hrozby
Gestor: Národné centrum kybernetickej bezpečnosti SK-CERT
Zodpovedný: riaditeľ Národného centra kybernetickej bezpečnosti SK-CERT

Názov ukazovateľa		**Rok 2019**	**Rok 2020**	**Rok 2021**
Poskytovanie prostredia pre školenia bežných používateľov, pre tréning zamestnancov IT oddelení a pre arénový kybernetický výcvik špecialistov	Plán	–	–	áno/nie
	Skutočnosť	4	–	–

Plnenie cieľa:

Dôležitou súčasťou neustáleho zvyšovania povedomia, zručnosti, metodickej a praktickej pripravenosti na kybernetické hrozby je aj pravidelný praktický tréning v podobe účasti na kybernetických cvičeniach od procesných a manažérskych až po technické a analytické. Významným úspechom v roku 2019 bolo prvé miesto tímu SK-CERT na medzinárodnom cvičení Cyber Czech. Medzinárodným úspechom bolo aj prizvanie zástupcov SK-CERT ako spoluorganizátora vysokoúrovňového table-top cvičenia BlueOLEx 2019 v Paríži. Novou aktivitou SK-CERT bola realizácia národného table-top cvičenia slúžiaceho na prípravu účastníkov na výnimočné situácie v kybernetickej oblasti, podporu manažérskeho rozhodovania a zlepšenie komunikácie a koordinácie. Národné centrum SK-CERT takisto buduje povedomie prostredníctvom osvetových a informačných výstupov na stránke www.SK-CERT.sk, organizovaním a účasťou na konferenciách zameraných na kybernetickú bezpečnosť a inými činnosťami, ktoré vedú k rozširovaniu vedomostí rôznych skupín obyvateľstva v oblasti kybernetickej bezpečnosti.

Zdroj získavania údajov: interné
Vypracoval: pplk. Mgr. Beáta Kalininová
Schválil: plk. Mgr. Rastislav Janota

0D906 – Manažérstvo kvality

Zámer: Optimalizácia procesov v rámci manažérstva kvality
Gestor: kancelária úradu
Zodpovedný: riaditeľ kancelárie úradu
Komentár:

V septembri roku 2018 uzatvoril Národný bezpečnostný úrad s Úradom pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky Zmluvu o partnerstve k národnému projektu Zavádzanie a podpora manažérstva kvality v organizáciách verejnej správy č. 2018/111/009977/03343, ktorou vyjadrilo vedenie úradu záväzok a záujem trvalo zlepšovať organizáciu. V zmluve sa úrad zaviazal implementovať nástroj komplexného manažérstva kvality – model CAF. Model CAF je aplikačný nástroj, ktorý pomáha organizáciám verejnej správy implementovať manažérstvo kvality s cieľom optimalizovať procesy, a tým zlepšiť výkonnosť organizácií.

Vypracoval: npor. JUDr. Lenka Hábelová, LL.M.
Schválil: kpt. JUDr. Katarína Kvasňovská

Cieľ 1: *Zavedenie a podpora manažérstva kvality v organizácii*
Gestor: *kancelária úradu*
Zodpovedný: *riaditeľ kancelárie úradu*

Názov ukazovateľa		Rok 2019	Rok 2020	Rok 2021
Počet platných certifikátov kvality	Plán	0	0	1
	Skutočnosť	0	–	–

Plnenie cieľa:

Cieľom implementácie modelu CAF je v podmienkach úradu zaviesť systém komplexného manažérstva kvality a prostredníctvom samohodnotenia identifikovať procesy a námety na zlepšenie činnosti, zvýšenie kvality vo všetkých oblastiach pôsobnosti úradu a napokon získanie titulu Efektívny používateľ modelu CAF (06/2021). Časový rámec projektu bol určený od novembra 2019 do júna 2021. Aktivity uskutočnené počas hodnoteného obdobia korešpondujú s časovým harmonogramom plnenia úloh. V rámci plnenia aktivít bolo 2. decembra 2019 uskutočnené školenie manažmentu k modelu CAF, na ktorom sa zúčastnilo 10 vedúcich pracovníkov sekcií a odborov. Bolo precizované personálne obsadenie garanta, metodika a administratívneho pracovníka modelu CAF, ktorí boli do svojich rolí vymenovaní menovacími dekrétmi riaditeľa úradu. Metodik a garant projektu sa 21. až 22. decembra 2019 zúčastnili dvojdňového školenia. V súlade s rozkazom riaditeľa úradu č. 30 z 20. decembra 2019 bol z príslušníkov úradu zriadený CAF tím, v ktorom bolo zohľadnené organizačné usporiadanie úradu.

Zdroj získavania údajov: interný
Vypracoval: npor. JUDr. Lenka Hábelová, LL.M.
Schválil: kpt. JUDr. Katarína Kvasňovská

Programová štruktúra – medzirezortný program
0EK – Informačné technológie financované zo štátneho rozpočtu

Zámer: **Zabezpečiť efektívne využívanie a riadenie výdavkov na informačné technológie financované zo štátneho rozpočtu**
Gestor: **Úrad podpredsedu vlády SR pre investície a informatizáciu**
Zodpovedný: **Úrad podpredsedu vlády SR pre investície a informatizáciu**

0EK0U – Informačné technológie financované zo štátneho rozpočtu – Národný bezpečnostný úrad

Zámer: **Zabezpečiť efektívne využívanie a riadenie výdavkov na informačné technológie financované zo štátneho rozpočtu**
Gestor: **technická sekcia**
Zodpovedný: **riaditeľ technickej sekcie**

Komentár:

Hlavným zámerom 0EKOU je zabezpečiť efektívne využívanie a riadenie výdavkov na informačné technológie financované zo štátneho rozpočtu. Vo všetkých troch prvkoch programu (systémy vnútornej správy, špecializované systémy a podporná infraštruktúra) je možné, z aktuálnych výsledkov hodnotenia stavu konštatovať, že sa ku dňu hodnotenia podarilo dosiahnuť požadovaný zámer a to zabezpečiť efektívne využívanie a riadenie výdavkov na informačné technológie financované zo štátneho rozpočtu.

Vypracoval: mjr. Mgr. Zuzana Halásová, PhD.
Schválil: pplk. Ing. Bibiána Magáthová, PhD.

0EK0U01 Systémy vnútornej správy

Zámer: Zabezpečiť efektívne využívanie a riadenie výdavkov na informačné technológie financované zo štátneho rozpočtu
Gestor: technická sekcia, odbor bezpečnostnej prevádzky
Zodpovedný: riaditeľ odboru bezpečnostnej prevádzky

Cieľ 1: Sledovať a riadiť objem výdavkov na jednotlivé informačné systémy z hľadiska ich implementácie a následných výdavkov na prevádzku a údržbu za účelom ich zefektívnenia

Názov ukazovateľa		**Rok 2017**	**Rok 2018**	**Rok 2019**	**Rok 2020**	**Rok 2021**
Zefektívnené využitie výdavkov zo štátneho rozpočtu na prevádzku a údržbu jednotlivých informačných technológií	Plán	áno/nie	áno/nie	áno/nie	áno/nie	áno/nie
	Skutočnosť	áno	áno	áno	–	–

Plnenie cieľa:

Hlavnou úlohou vyplývajúcou z plnenia cieľa je zabezpečiť efektívne využívanie a riadenie výdavkov na informačné technológie financované zo štátneho rozpočtu v oblasti systémov vnútornej správy. V priebehu roka 2019 prešli niektoré systémy vnútornej správy modernizáciou, čo malo za následok zefektívnenie využitia výdavkov zo štátneho rozpočtu. Na základe aktuálnych výsledkov hodnotenia stavu sa konštatuje, že sa ku dňu hodnotenia podarilo dosiahnuť reálnu hodnotu ukazovateľa „áno“. Technologické zariadenia používané v rámci systémov vnútornej správy, ktoré neboli predmetom modernizácie, sú už morálne opotrebované a možno v budúcnosti očakávať zvýšené prevádzkové náklady spôsobené ich haváriami. V sledovanom období boli výdavky zo štátneho rozpočtu na informačné technológie vynaložené efektívne.

Zdroj získavania údajov: prevádzkové záznamy, finančné kontroly, projektové stretnutia
Vypracoval: mjr. Mgr. Zuzana Halásová, PhD.
Schválil: pplk. Ing. Bibiána Magáthová, PhD.

0EK0U02 Špecializované systémy

Zámer: Zabezpečiť efektívne využívanie a riadenie výdavkov na informačné technológie financované zo štátneho rozpočtu
Gestor: technická sekcia, odbor bezpečnostnej prevádzky
Zodpovedný: riaditeľ odboru bezpečnostnej prevádzky

Cieľ 1: Sledovať a riadiť objem výdavkov na jednotlivé informačné systémy z hľadiska ich implementácie a následných výdavkov na prevádzku a údržbu za účelom ich zefektívnenia

Názov ukazovateľa		**Rok 2017**	**Rok 2018**	**Rok 2019**	**Rok 2020**	**Rok 2021**
Zefektívnené využitie výdavkov zo štátneho rozpočtu na prevádzku a údržbu jednotlivých informačných technológií	Plán	áno/nie	áno/nie	áno/nie	áno/nie	áno/nie
	Skutočnosť	áno	áno	áno	–	–

Plnenie cieľa:

Hlavnou úlohou vyplývajúcou z plnenia cieľa je zabezpečiť efektívne využívanie a riadenie výdavkov na informačné technológie financované zo štátneho rozpočtu v oblasti špecializovaných systémov. Sledovaním objemu výdavkov na prevádzku a údržbu jednotlivých informačných systémov je možné konštatovať, že ku dňu hodnotenia sa podarilo dosiahnuť reálnu hodnotu ukazovateľa „áno“. Aby bola táto hodnota udržateľná aj do budúceho obdobia, je potrebná modernizácia systémov spadajúcich pod prvok 0EKOU02 – Špecializované systémy, nakoľko technologické zariadenia systémov sú morálne zastarané a v budúcnosti možno očakávať zvýšené prevádzkové náklady spôsobené ich haváriami. Na niektorých častiach špecializovaných systémov v súčasnosti prebiehajú modernizačné

a rekonštrukčné práce. Výdavky zo štátneho rozpočtu na informačné technológie boli vynaložené tak, aby sa zamedzilo negatívnym dopadom neriadených nákupov a nákupov mimo plánu obstarávania.

Zdroj získavania údajov: prevádzkové záznamy, projektové stretnutia
Vypracoval: mjr. Mgr. Zuzana Halásová, PhD.
Schválil: pplk. Ing. Bibiána Magáthová, PhD.

0EK0U03 Podporná infraštruktúra
Zámer: Zabezpečiť efektívne využívanie a riadenie výdavkov na informačné technológie financované zo štátneho rozpočtu
Gestor: technická sekcia, odbor bezpečnostnej prevádzky
Zodpovedný: riaditeľ odboru bezpečnostnej prevádzky

Cieľ 1: Sledovať a riadiť objem výdavkov na podpornú infraštruktúru z hľadiska ich implementácie a následných výdavkov na prevádzku a údržbu za účelom ich zefektívnenia

Názov ukazovateľa		**Rok 2017**	**Rok 2018**	**Rok 2019**	**Rok 2020**	**Rok 2021**
Zefektívnené využitie výdavkov zo štátneho rozpočtu na zabezpečenie infraštruktúry na prevádzku jednotlivých informačných systémov	Plán	áno/nie	áno/nie	áno/nie	áno/nie	áno/nie
	Skutočnosť	áno	áno	áno	–	–

Plnenie cieľa:

Hlavnou úlohou vyplývajúcou z plnenia cieľa je zabezpečiť efektívne využívanie a riadenie výdavkov na informačné technológie financované zo štátneho rozpočtu v oblasti podpornej infraštruktúry. V priebehu roka 2019 prešli niektoré informačné systémy modernizáciou, čo malo za následok zefektívnenie využitia výdavkov aj na podpornú infraštruktúru. Na základe aktuálnych výsledkov hodnotenia stavu sa konštatuje, že sa ku dňu hodnotenia podarilo dosiahnuť reálnu hodnotu ukazovateľa „áno“. Aj napriek modernizácii niektorých informačných systémov sa v prevádzke stále nachádzajú technologické zariadenia spadajúce pod prvok 0EKOU03 – Podporná infraštruktúra, ktoré sú morálne zastarané a dlhodobo nevyhovujú požiadavkám na prevádzku a bezpečnosť. Objem výdavkov nebol dostatočný na zabezpečenie plnohodnotnej obmeny prevádzkovej infraštruktúry. V budúcnosti možno očakávať zvýšený počet porúch a prevádzkových havárií, čo bude mať za následok zvýšené prevádzkové náklady.

Zdroj získavania údajov: prevádzkové záznamy, finančné kontroly, projektové stretnutia
Vypracoval: mjr. Mgr. Zuzana Halásová, PhD.
Schválil: pplk. Ing. Bibiána Magáthová, PhD.