NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Príloha č. 3

Ročná monitorovacia správa k 31. 12. 2020

Programová štruktúra NBÚ

0D9 – BEZPEČNOSŤ INFORMÁCIÍ

Zámer: **Informácie chránené v súlade so zákonom o ochrane utajovaných informácií, zákonom o dôveryhodných službách a budovanie spôsobilosti kybernetickej bezpečnosti**
Gestor: **odbor projektového a finančného riadenia**
Zodpovedný: **riaditeľ odboru projektového a finančného riadenia**

Komentár:

V priebehu roka 2020 bolo plnenie jednotlivých cieľov 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“ ovplyvnené kvalitou a stabilitou legislatívneho prostredia, kvantitou a stupňom utajenia utajovaných informácií, reálnymi hrozbami a rizikami v oblasti kybernetickej bezpečnosti, odbornou spôsobilosťou zamestnancov a taktiež bezpečnostnou spoľahlivosťou navrhovaných osôb a podnikateľov. Na plnenie programu mala vplyv aj súčinnosť orgánov pri poskytovaní informácií pri vykonávaní bezpečnostných previerok a v podstatnej miere aj mimoriadna situácia v súvislosti so šírením nového koronavírusu COVID-19 (ďalej len „pandémia COVID-19“). Aj napriek negatívnym vplyvom niektorých faktorov porovnanie plánovaných a dosiahnutých cieľov preukázalo, že plnenie zámeru a cieľov programu bolo zabezpečené na základe existujúcich kapacít Národného bezpečnostného úradu v súlade so zásadami hospodárnosti, efektívnosti, účelnosti a účinnosti. Možno konštatovať, že merateľné ukazovatele jednotlivých stanovených cieľov boli vhodne zvolené a vzhľadom na negatívne účinky pandémie COVID-19 boli ciele jednotlivých podprogramov a prvkov v roku 2020 plnené v najvyššej možnej miere.

Vypracoval: pplk. Ing. Zuzana Halászová
Schválil: mjr. Ing. Mária Szabóová, PhD.

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**	**Rok 2022**
Kvalitné a včasne ukončené previerky personálnej a priemyselnej bezpečnosti	Plán	áno/nie	áno/nie	áno/nie	áno/nie	áno/nie	áno/nie
	skutočnosť	áno	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 01.01.2020 do 31.12.2020 prijal úrad 5313 žiadostí o vykonanie bezpečnostnej previerky navrhovanej osoby a 88 žiadostí o vydanie potvrdenia o priemyselnej bezpečnosti. Z počtu prijatých žiadostí o vykonanie bezpečnostnej previerky navrhovanej osoby bolo v hodnotenom období ukončených 4247 bezpečnostných previerok. Z počtu prijatých žiadostí o vydanie potvrdenia o priemyselnej bezpečnosti bolo v hodnotenom období ukončených 50 bezpečnostných previerok.

Spolu bolo prijatých 5401 žiadostí o bezpečnostnú previerku, z toho ukončených bolo 4297 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:	interné zdroje
Vypracoval:	pplk. Ing. Miroslava Mináriková (z podkladov OBP)
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	Rok 2022
Zaistená technická spôsobilosť na ochranu UI	Plán	áno/nie	áno/nie	áno/nie	áno/nie	áno/nie	áno/nie
	skutočnosť	áno	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 zariadení *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.

K 31.12.2020 bolo prijatých 42 žiadostí o stanovisko k certifikácii TP, vykonanie meraní NEV zariadení TP a o vykonanie zónových meraní priestorov, z ktorých bolo vybavených 40. Na základe doručených žiadostí bolo vykonaných 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 žiadostí bolo vykonaných celkovo 18 meraní útlmu tienenej komory a tieneného stanu. K 31.12.2020 boli prijaté taktiež 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.

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.

Vytvorenie optimálnych podmienok technickej spôsobilosti na ochranu utajovaných informácií je zabezpečované aj akreditáciou komunikačných a informačných systémov pre manipuláciu utajovaných informácií SR (uvoľniteľných pre NATO alebo EÚ), NATO a EÚ, ako aj certifikáciou prostriedkov potrebných na ochranu utajovaných informácií pre rôzne stupne utajenia. K 31.12.2020 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). Z dôvodu nedostupnosti personálu na MO SR (pandémia COVID-19) je akreditácia systému NS VoS presunutá na rok 2021.

K 31.12.2020 bolo certifikovaných 103 prostriedkov potrebných na ochranu utajovaných informácií a bolo vydaných 23 dodatkov k už certifikovaným prostriedkom potrebným na ochranu utajovaných informácií.

Zdroj získavania údajov: interné zdroje

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**	**Rok 2022**
Efektívny systém pre poskytovanie dôveryhodných služieb	Plán	áno/nie	áno/nie	áno/nie	áno/nie	áno/nie	áno/nie
	skutočnosť	áno	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 plnením zákonom stanovej úlohy poskytovať kvalifikované dôveryhodné služby orgánom verejnej moci (do 31.7.2019). Systém v Slovenskej republike (vychádzajúc z nariadenia eIDAS) je založený na PKI infraštruktúre, pričom Národný bezpečnostný úrad je v pozícii tzv. dozorného orgánu. V súvislosti s legislatívnou zmenou prišlo k 1. augustu 2019 k prechodu kompetencií na poskytovanie kvalifikovaných dôveryhodných služieb pre orgány verejnej moci na Národnú agentúru pre sieťové a elektronické služby. Kompetencia úradu ako orgánu dohľadu podľa článku 17 nariadenia eIDAS ostala nezmenená. V pláne vonkajších kontrol na rok 2020 boli schválené 2 vonkajšie kontroly kvalifikovaných poskytovateľov dôveryhodných služieb, z toho bola uskutočnená jedna kontrola. Druhá kontrola nebola uskutočnená z dôvodu nepriaznivej pandemickej situácie a bude zahrnutá do plánu kontrol na rok 2021.

Možno konštatovať, že boli zabezpečené optimálne podmienky na poskytovanie dôveryhodných služieb v súlade s platným zákonom o dôveryhodných službách.

Zdroj získavania údajov: interné zdroje
Vypracoval: plk. Ing. Branislav Šusta
Schválil: pplk. Ing. Bibiána Magáthová, PhD.

Cieľ 4 Zabezpečiť otvorený, bezpečný a chránený národný kybernetický priestor
Gestor: Národná jednotka SK-CERT
Zodpovedný: riaditeľ Národnej jednotky SK-CERT

Názov ukazovateľa		**Rok 2017**	**Rok 2018**	**Rok 2019**	**Rok 2020**	**Rok 2021**	**Rok 2022**
Zvýšená bezpečnosť kybernetického priestoru	Plán	áno/nie	áno/nie	áno/nie	áno/nie	áno/nie	áno/nie
	skutočnosť	áno	áno	áno	áno	-	-

Plnenie cieľa:

Legislatívny základ ochrany kybernetického priestoru v SR tvorí zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti. Národné centrum kybernetickej bezpečnosti SK-CERT (ďalej ako SK-CERT) naďalej rozvíja svoju pôsobnosť a spôsobilosť pri zabezpečovaní otvoreného, bezpečného a chráneného národného kybernetického priestoru. SK-CERT zbiera informácie, rieši a koordinuje riešenie kybernetických bezpečnostných incidentov v národnom kybernetickom priestore. Zdrojom údajov je vlastná detekcia, povinné a dobrovoľné hlásenia prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb a informácie od partnerov a partnerských organizácií. Úrad prostredníctvom SK-CERT reprezentuje Slovenskú republiku na odborných konferenciách, pracovných skupinách a iných aktivitách v oblasti kybernetickej bezpečnosti, na ktorých prezentuje stav kybernetickej bezpečnosti v SR z rôznych hľadísk a takisto čerpá nové poznatky, ktoré následne implementuje v podmienkach SR tak, aby bol zabezpečený otvorený, bezpečný a chránený národný kybernetický priestor. SK-CERT kontinuálne rozvíja svoje interné nástroje a systémy slúžiace na detekciu kybernetických bezpečnostných incidentov a rozposielanie adresných varovaní.

V roku 2020 Národné centrum kybernetickej bezpečnosti SK-CERT a jeho partneri celkovo detegovali 39 788 549 incidentov, z ktorých bolo riešených 3793 incidentov. Väčšina z detegovaných incidentov bola riešená automatizovaným spôsobom, resp. automatizovanými prostriedkami ochrany.

Národné centrum kybernetickej bezpečnosti SK-CERT v roku 2020 vydalo 255 bezpečnostných varovaní a 37 bezpečnostných bulletinov.

Zdroj získavania údajov :	interné zdroje
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.

Vypracoval: pplk. Ing. Miroslava Mináriková
Schválil: plk. JUDr. Marek Barta

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

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

Názov ukazovateľa		Rok 2016	Rok 2017	Rok 2018	Rok 2019	Rok 2020	Rok 2021	Rok 2022
% vykonaných kontrol OUI z ročného plánu kontrol OUI	plán	100	100	100	100	100	100	100
	skutočnosť	100	100	100	100	64,70	-	-

Plnenie cieľa:

V pláne vonkajších kontrol na rok 2020 bolo schválených 17 kontrol ochrany utajovaných skutočností. Celkovo bolo vykonaných 11 kontrol, z toho 10 plánovaných a jedna mimoriadna nad rámec schváleného plánu na Úrade podpredsedu vlády SR pre investície a informatizáciu. Zvyšné kontroly neboli vykonané v stanovenom termíne z dôvodu pandémie COVID-19 a budú zahrnuté do plánu kontrol na rok 2021.

Zdroj získavania údajov: Plán kontrol a vyhodnotenia kontrol 2020, Prehľad kontrol 2020, Prehľad kontrol 2002-2020
Vypracoval: npor. 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 2016	Rok 2017	Rok 2018	Rok 2019	Rok 2020	Rok 2021	Rok 2022
% vybavených žiadostí o vykonanie bezpečnostnej previerky v zákonnej lehote	plán	100	100	100	99	97	97	97
	skutočnosť	98,83	99,83	99,06	98,96	97,5	-	-

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 01.01.2020 do 31.12.2020 vybaviť 4245 žiadostí o vykonanie bezpečnostnej previerky.

V hodnotenom období bolo vybavených 4139 žiadostí, čo predstavuje 97,5 % z počtu prijatých 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. 97,5 % vybavených žiadostí.

Na plnení cieľa sa podieľali príslušníci úradu 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 informácií 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 informácií, 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 106 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, poskytnutie informácií v iných než zákonom stanovených lehotách príslušným zahraničným partnerským bezpečnostným orgánom a pandémia COVID-19.

Udržateľnosť cieľa v budúcnosti závisí od vyššie uvedených faktorov.

Zdroj získavania údajov: interné zdroje
Vypracoval: pplk. Ing. Miroslava Mináriková (z podkladov OBP)
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	Rok 2022
% vykonaných skúšok a preškolení z požadovaného počtu	Plán	100	100	100	100	100	100
	skutočnosť	100	100	100	92,3	-	--

Plnenie cieľa:
V rámci činností zameraných na zvyšovanie bezpečnostného povedomia vykonáva úrad skúšky bezpečnostného zamestnanca a preškolenia osôb v rôznych oblastiach bezpečnosti. V minulosti ich úrad zabezpečoval prezenčnou formou a spravidla boli organizované v sídle úradu. V súvislosti so vznikom a nepriaznivým priebehom pandemickej situácie na jar 2020 bola prezenčná forma v rámci prijatých opatrení v marci 2020 dočasne pozastavená, resp. zrušená.

Vzniknuté okolnosti urýchlili realizáciu transferu týchto aktivít do virtuálneho priestoru a potvrdili opodstatnenosť dlhodobého, širšie koncipovaného zámeru úradu elektronizovať poskytované služby. Od 1. novembra 2020 realizuje úrad skúšky bezpečnostného zamestnanca takmer výhradne dištančne. Skúšky sa vykonávajú formou on-line testu v prostredí samostatnej webovej aplikácie, komunikácia počas skúšky prebieha vo virtuálnej videokonferenčnej miestnosti. Prechod na dištančnú formu preškolení je vo fáze prípravy. Pred nástupom 1. vlny pandémie úrad usporiadal štyri prezenčné preškolenia. Zúčastnilo sa ich 80 osôb.

V roku 2020 prijal úrad 364 žiadostí o vykonanie skúšky bezpečnostného zamestnanca. Na skúšku bolo pozvaných 336 uchádzačov. 214 skúšok bolo vykonaných prezenčnou formou, 122 dištančne. 312 uchádzačov vykonalo skúšku úspešne (207 prezenčne, 105 dištančne), 19 pri skúške neuspeli (traja prezenčne, 16 dištančne). Na skúšku sa nedostavili piati uchádzači. 28 žiadostí o vykonanie skúšky prijatých v roku 2020 bude vybavených začiatkom roka 2021. V roku 2020 bolo vybavených 92,30 % žiadostí o vykonanie skúšky bezpečnostného zamestnanca.

V súvislosti s vykonávaním skúšok bezpečnostného zamestnanca a realizáciou preškoľovania možno konštatovať pozitívny vplyv týchto aktivít na zvyšovanie úrovne zabezpečenia ochrany utajovaných skutočností v orgánoch verejnej moci a u podnikateľov.

Zdroj získavania údajov: interné zdroje
Vypracoval: pplk. JUDr. Andrea Senková
Schválil: kpt. JUDr. Katarína Kvasňovská

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

Komentár:

Ciele boli stanovené v súlade s požiadavkami platnej legislatívy SR (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 bolo zabezpečenie plnenie zámeru dosiahnuť maximálnu technickú spôsobilosť na ochranu utajovaných informácií, pričom dosiahnutý výsledok je v plnej miere naplnením potreby cieľovej skupiny ako 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 naplnení sa podieľali príslušníci odborných útvarov technickej sekcie. Na základe získaných výsledkov možno konštatovať, že zabezpečenie technickej spôsobilosti na ochranu utajovaných informácií sa plnilo v súlade so stanovenými cieľmi.

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 2016**	**Rok 2017**	**Rok 2018**	**Rok 2019**	**Rok 2020**
% vybavených žiadostí v zákonom stanovenej lehote	plán	97	97	97	97	97
	skutočnosť	100	100	100	100	100

Plnenie cieľa:

K 31.12.2020 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). 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 zabezpečili plnenie stanoveného cieľa.

Zdroj získavania údajov: interné zdroje
Vypracoval: pplk. Mgr. Ivan Chrenko a npor. 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 2016**	**Rok 2017**	**Rok 2018**	**Rok 2019**	**Rok 2020**
% vybavených žiadostí v zákonom stanovenej lehote	plán	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 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov certifikované technické prostriedky (ďalej len „TP“), prostriedky šifrovej ochrany informácii (ďalej len „PŠOI“), mechanické zábranné prostriedky a technické zabezpečovacie prostriedky (ďalej len „MZP a TZP“).

K 31.12.2020 bolo celkovo prijatých 112 žiadostí o certifikáciu (TP 67, PŠOI 5, MZP - 13 a TZP -27) a 23 žiadostí o vydanie dodatku k certifikátu (TP 17, PŠOI 6). Z celkového počtu prijatých žiadostí bolo vybavených 103 žiadostí (TP 60, PŠOI 3, MZP – 13 a TZP – 27) a 23 dodatkov (TP 17, PŠOI 6). Žiadosti, ktoré spĺňali požadované náležitosti, boli všetky vybavené v zákonom stanovenej lehote.

	Vyhradené	Dôverné	Tajné	Prísne tajné	Spolu
TP	20	29	11	0	60
PŠOI	1	2	0	0	3
MZP	0	7	4	2	13
TZP	0	10	10	7	27
SPOLU	21	48	25	9	103

Stupne utajenia vydaných certifikátov k 31.12.2020

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.

Zdroj získavania údajov: interné zdroje
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 2016	Rok 2017	Rok 2018	Rok 2019	Rok 2020	Rok 2021	Rok 2022
% poskytnutých služieb z počtu žiadosti o poskytnutie služby	plán	93	94	97	97	97	97	98
	skutočnosť	97	98	98	99	100	-	-

Plnenie cieľa:

Zadefinovaný cieľ je prispôsobený skutočným potrebám, plne korešponduje s identifikovanými problémami a berie do úvahy doposiaľ dosiahnuté výsledky a všeobecný vývoj potrieb úradu. Zároveň reaguje na výzvy danej politiky v oblasti ochrany utajovaných skutočností. Ochrana zahraničných utajovaných informácií sa zabezpečuje splnením osobitných podmienok podľa zákona.

Cieľ je merateľný a kvantifikovateľný vhodným merateľným ukazovateľom výsledku, pričom obsahuje konkrétnu cieľovú hodnotu – percento 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.

Zdroj získavania údajov: interné zdroje
Vypracoval: pplk. Mgr. Daniela Srdošová
Schválil: kpt. JUDr. Katarína Kvasňovská

0D903 – RIADENIE A PODPORA PROGRAMOV

Zámer: Kvalitne fungujúce podporné útvary
Gestor: kancelária úradu
Zodpovedný: riaditeľ kancelárie úradu

Komentár:

Potreba existencie podprogramu v nadväznosti na stanovené ciele jednotlivých podprogramov a prvkov programu 0D9 – Bezpečnosť informácií stále pretrváva. Ciele stanovené v rámci podprogramu sú plnené na požadovanej kvalitatívnej a kvantitatívnej úrovni, riadne a včas. Sú plnené v takom rozsahu, aby odborným útvarom boli poskytnuté a zabezpečené kvalitné podmienky na dosahovanie zámeru programu a to aj napriek nepriaznivému vplyvu pandémie COVID-19. Výstupy a výsledky pri plnení jednotlivých cieľov zabezpečujú plnenie zámeru programu v požadovanom rozsahu a úrovni.

Vypracoval: plk. Mgr. Jana Lukáčová
Schválil: kpt. JUDr. Katarína Kvasňovská

Cieľ 1: Plnenie úloh pri zabezpečovaní činnosti úradu
Gestor: kancelária úradu
Zodpovedný: riaditeľ kancelárie úradu

Názov ukazovateľa		Rok 2016	Rok 2017	Rok 2018	Rok 2019	Rok 2020	Rok 2021	Rok 2022
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 odráža skutočné potreby odborných útvarov. Je možné opätovne deklarovať, že bol stanovený správne a korešponduje so zámerom podprogramu a programu. Napriek skutočnosti, že plnenie daného cieľa bolo negatívne ovplyvňované pandémiou COVID-19, podporné útvary v maximálnej miere vykonávali svoje činnosti. Možno konštatovať, že odborné útvary mali vytvorené kvalitné podmienky na plnenie úloh a dosahovanie zámeru programu. Vykonané aktivity počas celého hodnoteného obdobia boli premietnuté do skutočných výsledkov v súlade s časovým harmonogramom plnenia úloh. V rámci materiálno-technického zabezpečovania napriek obmedzeniam boli vstupy realizované za podmienky najlepšia kvalita/najlepšia cena. Vo výraznej miere pretrváva trend využívania odborných kapacít najmä pri výkone služieb odborne spôsobilými personálnymi kapacitami úradu.

Vplyv pandémie COVID-19 pri plnení úloh podporných útvarov v sledovanom období narúšal štandardné aktivity minimálne.

Naďalej je predpoklad, že dosiahnuté výsledky budú udržateľné aj v dlhodobom časovom horizonte.

Zdroj získavania údajov: interné zdroje
Vypracoval: plk. Mgr. Jana Lukáčová
Schválil: kpt. JUDr. Katarína Kvasňovská

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

Názov ukazovateľa		**Rok 2016**	**Rok 2017**	**Rok 2018**	**Rok 2019**	**Rok 2020**	**Rok 2021**	**Rok 2022**
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). Projekt IS OUSIP bol začatý v roku 2018 a ukončený 31.5.2019. V súčasnosti prebieha proces certifikácie riešenia, ktorý sa z dôvodu všeobecnej pandemickej situácie a personálnych možností plánuje ukončiť v roku 2021. 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 podprogramu. 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: plk. Ing. Branislav Šusta
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. K 1. augustu 2019 prišlo k prechodu kompetencií na 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.

V pláne vonkajších kontrol na rok 2020 boli schválené 2 vonkajšie kontroly kvalifikovaných poskytovateľov dôveryhodných služieb, z toho bola uskutočnená jedna kontrola. Druhá kontrola nebola uskutočnená z dôvodu nepriaznivej pandemickej situácie a bude zahrnutá do plánu kontrol na rok 2021.

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: *sekcia regulácie a dohľadu*
Zodpovedný: *riaditeľ sekcie regulácie a dohľadu*

Názov ukazovateľa		**Rok 2017**	**Rok 2018**	**Rok 2019**	**Rok 2020**	**Rok 2021**	**Rok 2022**
% vykonaných dohľadov nad poskytovateľmi dôveryhodných služieb	Plán	100	100	100	100	100	100
	skutočnosť	100	100	100	50	-	-

Plnenie cieľa:

V pláne vonkajších kontrol na rok 2020 boli schválené 2 vonkajšie kontroly kvalifikovaných poskytovateľov dôveryhodných služieb, z toho bola uskutočnená jedna kontrola. Druhá kontrola nebola uskutočnená z dôvodu nepriaznivej pandemickej situácie a bude zahrnutá do plánu kontrol na rok 2021.

Zdroj získavania údajov: Plán kontrol a vyhodnotenia kontrol 2020, Prehľad kontrol 2020, Prehľad kontrol 2002-2020
Vypracoval: npor. Mgr. Veronika Vanyová
Schválil: plk. Ing. JUDr. Alexandra Kaľavská Dianišková

0D905 – KYBERNETICKÁ BEZPEČNOSŤ

Zámer: Zabezpečiť budovanie spôsobilostí na úseku kybernetickej bezpečnosti
Gestor: Národná jednotka SK-CERT
Zodpovedný: riaditeľ Národnej jednotky SK-CERT

Komentár:

Národné centrum kybernetickej bezpečnosti SK-CERT 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. SK-CERT kontinuálne zlepšuje svoje spôsobilosti a buduje svoje detekčné, analytické a prevádzkové spôsobilosti tak, aby bola zabezpečená ochrana kybernetického priestoru SR a efektívne riešenie kybernetických bezpečnostných incidentov.

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	Rok 2022
Vytvorenie optimálnych legislatívnych podmienok	Plán	áno/nie	áno/nie	áno/nie	áno/nie	áno/nie	áno/nie
	skutočnosť	áno	áno	áno	áno	-	-

Plnenie cieľa:

Na úseku kybernetickej bezpečnosti dňa 01.01.2020 nadobudla účinnosť vyhláška Národného bezpečnostného úradu č. 436/2019 Z. z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora. V novembri 2020 bol predložený na rokovanie vlády SR návrh zákona, ktorým sa mení a dopĺňa zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. V decembri 2020 bola predložená na rokovanie vlády SR Bezpečnostná stratégia kybernetickej bezpečnosti na roky 2021 až 2025 a následne 7. januára 2021 bola schválená.

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

Cieľ 2: Vytvoriť optimálne technické podmienky pre kybernetickú bezpečnosť SR
Gestor: Národná jednotka SK-CERT
Zodpovedný: riaditeľ Národnej jednotky SK-CERT

Názov ukazovateľa		**Rok 2017**	**Rok 2018**	**Rok 2019**	**Rok 2020**	**Rok 2021**	**Rok 2022**
Vytvorenie optimálnych technických podmienok	Plán	áno/nie	áno/nie	áno/nie	áno/nie	áno/nie	áno/nie
	skutočnosť	áno	áno	áno	áno	-	-

Plnenie cieľa:

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.

SK-CERT počas roka 2020 spolupracovalo so svojimi partnermi, najmä v sektore zdravotníctva, rozvíjalo svoje interné personálne a technické kapacity, implementovalo technologické riešenia v oblasti detekcie a riešenia kybernetických bezpečnostných incidentov a poskytovalo podporu svojej konštituencii pri riešení kybernetických bezpečnostných incidentov. Počas roka takisto riešilo viacero závažných zraniteľností, ktoré mali dopad na kybernetický priestor SR.

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

<u>0D90501 – NP: Národný systém riadenia incidentov kybernetickej bezpečnosti vo verejnej správe</u>
Gestor: Národné centrum kybernetickej bezpečnosti SK-CERT
Zodpovedný: riaditeľ SK-CERT

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

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. V rámci projektu „Národný systém riadenia incidentov kybernetickej bezpečnosti vo verejnej správe" bol obstaraný jednotný informačný systém kybernetickej bezpečnosti. Takisto v rámci projektu bola uzatvorená zmluva na školenia, ale vzhľadom na pandemickú situáciu sa školenia v roku 2020 nezrealizovali. Čerpanie školení bolo predĺžené do konca roku 2021.

Zdroj získavania údajov: interné zdroje
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 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 SK-CERT

Názov ukazovateľa		Rok 2019	Rok 2020	Rok 2021
Počet vybudovaných učební	Plán	-	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. Projekt mal byť realizovaný so začiatkom v roku 2020, avšak z dôvodu vládnych zmien a pandémie ochorenia COVID-19 sa schvaľovacie a iné procesy, súvisiace s projektom, spomalili.

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

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

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. Národné

centrum kybernetickej bezpečnosti 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. Nakoľko rok 2020 bol poznačený pandémiou COVID-19, nebolo možné organizovať kybernetické cvičenia a niektoré konferencie. Vo virtuálnom priestore sa uskutočnilo jedno z najväčších kybernetických cvičení NATO Cyber Coalition 2020, ktoré v rámci SR riadilo Národné centrum kybernetickej bezpečnosti SK-CERT a ako účastníkov prizvalo SIS, MIL.CSIRT.SK a CSIRT.SK. Konferencie vo virtuálnom priestore prebiehali kontinuálne počas celého roka, pričom zástupcovia Národného centra kybernetickej bezpečnosti SK-CERT sa zúčastnili (ako účastníci alebo ako spíkri) viac ako 20 konferencií online. V novembri 2020 sa zástupcovia Národného centra kybernetickej bezpečnosti SK-CERT podieľali na organizácii kongresu ITAPA.

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

0D90503 - Optimálne podmienky pre kybernetickú bezpečnosť SR
Gestor: Národné centrum kybernetickej bezpečnosti SK-CERT
Zodpovedný: riaditeľ Národného centra kybernetickej bezpečnosti SK-CERT

Cieľ 1: Vytvoriť optimálne legislatívne podmienky pre kybernetickú bezpečnosť SR
Gestor: sekcia regulácie a dohľadu
Zodpovedný: riaditeľ sekcie regulácie a dohľadu

Názov ukazovateľa		**Rok 2019**	**Rok 2020**	**Rok 2021**
Vytvorenie optimálnych legislatívnych podmienok	plán	áno/nie	áno/nie	áno/nie
	skutočnosť	áno	áno	-

Plnenie cieľa:

V nadväznosti na doplnenie podprogramu 0D905 o dva nové prvky v roku 2019 bol na základe usmernenia MF SR tento podprogram v roku 2020 doplnený o prvok 0D90503, ktorý prebral ciele a ich plnenie z podprogramu 0D905. Doplnenie bolo odsúhlasené listom MF SR č. 009785/2020-441 zo dňa 05.03.2020. V záujme zachovania prehľadnosti a kontinuity plnenia bolo plnenie cieľov presunuté z podprogramu na prvok k 01.07.2020. Na úseku kybernetickej bezpečnosti dňa 01.01.2020 nadobudla účinnosť vyhláška Národného bezpečnostného úradu č. 436/2019 Z. z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora. V novembri 2020 bol predložený na rokovanie vlády SR návrh zákona, ktorým sa mení a dopĺňa zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. V decembri 2020 bola predložená na rokovanie vlády SR Bezpečnostná stratégia kybernetickej bezpečnosti na roky 2021 až 2025 a následne 7. januára 2021 bola schválená.

Zdroj získavania údajov: www.slov-lex.sk
Vypracoval: npor. 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 2019**	**Rok 2020**	**Rok 2021**
Vytvorenie optimálnych technických podmienok	plán	áno/nie	áno/nie	áno/nie
	skutočnosť	áno	áno	

Plnenie cieľa:

V nadväznosti na doplnenie podprogramu 0D905 o dva nové prvky v roku 2019 bol na základe usmernenia MF SR tento podprogram v roku 2020 doplnený o prvok 0D90503, ktorý prebral ciele a ich plnenie z podprogramu 0D905. Doplnenie bolo odsúhlasené listom MF SR č. 009785/2020-441 zo dňa 05.03.2020. V záujme zachovania prehľadnosti a kontinuity plnenia bolo plnenie cieľov presunuté z podprogramu na prvok k 01.07.2020.

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.

SK-CERT počas roka 2020 spolupracovalo so svojimi partnermi, najmä v sektore zdravotníctva, rozvíjalo svoje interné personálne a technické kapacity, implementovalo technologické riešenia v oblasti detekcie a riešenia kybernetických bezpečnostných incidentov a poskytovalo podporu svojej konštituencii pri riešení kybernetických bezpečnostných incidentov. Počas roka takisto riešilo viacero závažných zraniteľností, ktoré mali dopad na kybernetický priestor SR.

Zdroj získavania údajov: interné zdroje
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:

Národný bezpečnostný úrad v septembri 2018 uzatvoril s Úradom pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky Zmluvu o partnerstve k národnému projektu Zavádzanie a podpora manažérstva kvality v organizáciách verejnej správy. Vedenie úradu týmto krokom vyjadrilo záujem a záväzok trvalo zlepšovať organizáciu.

V zmluve sa úrad zaviazal implementovať nástroj komplexného manažérstva kvality, model CAF. Ide o aplikačný nástroj, ktorý pomáha organizáciám verejnej správy implementovať manažérstvo kvality s cieľom optimalizovať procesy, a tým zlepšiť a zvýšiť výkonnosť organizácií.

Rovnaký zámer je aj súčasťou Stratégie rozvoja NBÚ, ktorá bola prijatá v júni 2019. Jedným z jej kľúčových cieľov je zvyšovať výkonnosť úradu hľadaním a nasadzovaním efektívnejších riešení, zavádzaním automatizácie rutinných činností a vytváraním priestoru na znižovanie administratívnej záťaže.

Vypracoval: por. Mgr. Nicol Vitteková
Schválil: kpt. JUDr. Katarína Kvasňovská

0D90601 - Rozvoj manažérstva kvality
Gestor: kancelária úradu
Zodpovedný: riaditeľ kancelárie úradu

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	0	-

Plnenie cieľa:

Cieľom implementácie modelu CAF v podmienkach úradu je zaviesť na úrade systém komplexného manažérstva kvality a prostredníctvom samohodnotenia identifikovať procesy, ktoré je možné optimalizovať, predložiť a realizovať námety na zvýšenie efektivity činnosti úradu a zvýšenie kvality vo všetkých oblastiach jeho pôsobnosti. V neposlednom rade sa s realizáciou projektu spája aj ambícia získať pre úrad, po úspešnom zavŕšení projektu v júli 2021, titul Efektívny používateľ modelu CAF. Aktivity projektu uskutočnené v roku 2020 korešpondujú so schváleným časovým harmonogramom implementácie modelu CAF, ktorý bol rozvrhnutý na obdobie od novembra 2019 do júna 2021.

V dňoch 13. až 14. januára 2020 sa uskutočnilo školenie CAF tímu. Zúčastnilo sa ho 15 príslušníkov úradu. Prostredníctvom dotazníka spokojnosti bola zisťovaná spätná väzba k priebehu a obsahu vzdelávacej aktivity. Od februára do apríla 2020 prebiehala 2. fáza projektu - fáza samohodnotenia. Projektový tím pokračoval v spracúvaní jednotlivých kritérií Samohodnotiacej správy, vlastníci kritérií a členovia CAF tímu priebežne využívali možnosť konzultovať jednotlivé aspekty so školiteľmi.

Po spripomienkovaní textu Samohodnotiacej správy konzultantom sa v máji 2020 prostredníctvom videokonferencie uskutočnil konsenzus míting. 16. júna 2020 bola správa predložená aj na interné pripomienkové konanie. Nasledovalo vysporiadanie pripomienok útvarov úradu, vykonanie formálnych úprav a predloženie výslednej verzie materiálu riaditeľovi úradu. Po schválení dokumentu riaditeľom úradu 30. júna 2020, bola Samohodnotiaca správa zaslaná Úradu pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky.

Pokračovala príprava ďalšej aktivity, tzv. „Posúdenia na mieste“, ktorú 27. júla 2020 vykonali externí posudzovatelia. Tým bola ukončená druhá fáza projektu – fáza samohodnotenia.

V septembri 2020 bola zahájená 3. fáza projektu - Proces zlepšovania. Členovia CAF tímu upriamili pozornosť na tvorbu Akčného plánu zlepšovania (APZ). 10. septembra 2020 prebehli konzultácie k spracovaniu APZ. V dňoch 28 až 29. septembra sa v sídle úradu uskutočnilo za účasti 16 členov tímu školenie Tvorba APZ. Súčasne boli vyhodnotené výstupy z Posúdenia na mieste.

Dňa 6. októbra 2020 bola spracovaná a predložená na interné pripomienkové konanie nultá verzia Akčného plánu zlepšovania. Po vyhodnotení a vysporiadaní pripomienok útvarov úradu bola finálna verzia akčného plánu predložená na schválenie riaditeľovi úradu. Riaditeľ úradu Akčný plán zlepšovania odsúhlasil 10. novembra 2020. V decembri tak mohla začať realizácia schválených aktivít APZ a plánovanie aktivít, ktoré je potrebné realizovať v roku 2021.

Zdroj získavania údajov: interné zdroje
Vypracoval: por. Mgr. Nicol Vitteková
Schválil: kpt. JUDr. Katarína Kvasňovská

0D907 – KOMPETENČNÉ A CERTIFIKAČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI

Zámer: **Zabezpečiť činnosti príspevkovej organizácie Národného bezpečnostného úradu**
Gestor: **Kompetenčné a certifikačné centrum kybernetickej bezpečnosti**
Zodpovedný: **generálny riaditeľ Kompetenčného a certifikačného centra kybernetickej bezpečnosti**

Komentár:

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti (KCCKB) bolo zriadené 1.1.2020 rozhodnutím riaditeľa Národného bezpečnostného úradu o zriadení príspevkovej organizácie podľa § 21 zákona č. 523/2004 Z. z. o rozpočtových pravidlách verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. Základným poslaním KCCKB je vo verejnom záujme napomáhať k plneniu odborných úloh zriaďovateľa v oblasti kybernetickej bezpečnosti, ochrany utajovaných skutočností, šifrovej ochrany a dôveryhodných služieb.

Všetky súvisiace činnosti pri vytvorení KCCKB boli realizované aj za pomoci niektorých útvarov NBÚ na základe kontraktu.

Vypracoval: Ing. Tomáš Hettych, zástupca generálneho riaditeľa
Schválil: Ing. Ivan Makatura, generálny riaditeľ

Cieľ 1: *Plnenie úloh vyplývajúcich z kontraktu*
Gestor: *Kompetenčné a certifikačné centrum kybernetickej bezpečnosti*
Zodpovedný: *generálny riaditeľ Kompetenčného a certifikačného centra kybernetickej bezpečnosti*

Názov ukazovateľa		**Rok 2020**	**Rok 2021**	**Rok 2022**
Zabezpečenie plnenia úloh zadaných zriaďovateľom	Plán	áno/nie	áno/nie	áno/nie
	skutočnosť	áno	-	-

Plnenie cieľa:

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti (ďalej len „KCCKB“) pri plnení úloh zadaných zriaďovateľom v roku 2020 realizovalo široké spektrum aktivít.

V rámci plnenia úloh certifikačného orgánu podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti vydala Slovenská národná akreditačná služba (SNAS) rozhodnutím č. 695/8678/2020/2 dňa 15.4.2020 osvedčenie o akreditácii pre certifikáciu audítorov kybernetickej bezpečnosti. K 31.12.2020 bolo certifikovaných 28 audítorov kybernetickej bezpečnosti. Okrem formálnej certifikácie v akreditovanom režime KCCKB podpísalo zmluvu s Európskou organizáciou kybernetickej bezpečnosti (ECSO) o pristúpení k vydávaniu obchodnej značky „Cybersecurity made in Europe“.

V oblasti zónových meraní a meraní nežiadúceho elektromagnetického vyžarovania KCCKB vytvorilo odbor Riadenia projektov a externej spolupráce.

V rámci plnenia úloh národného odvetvového, technologického a výskumného centra v oblasti kybernetickej bezpečnosti bola formalizovaná spolupráca so Žilinskou univerzitou.

KCCKB kontrahovalo viacerých klientov s požiadavkou na konzultačné činnosti v oblasti ochrany utajovaných skutočností, kybernetickej bezpečnosti a dôveryhodných služieb. Zároveň bol v nadväznosti na plnenie tejto úlohy vytvorený samostatný odbor.

KCCKB zorganizovalo v roku 2020 dva termíny školení na prípravu Audítorov kybernetickej bezpečnosti.

Zdroj získavania údajov:	Interná rozpočtová metodika, RIS, GARIS, informácie z trhu, SNAS
Vypracoval:	Ing. Tomáš Hettych, zástupca generálneho riaditeľa
Schválil:	Ing. Ivan Makatura, generálny riaditeľ

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: **Ministerstvo investícií, regionálneho rozvoja a informatizácie SR**
Zodpovedný: **Ministerstvo investícií, regionálneho rozvoja a informatizácie SR**

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 riadenia 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 :	plk. Ing. Branislav Šusta
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**	**Rok 2022**
Zefektívnené využitie výdavkov zo štátneho rozpočtu na prevádzku a údržbu jednotlivých informačných technológií	plán	áno/nie	áno/nie	áno/nie	áno/nie	áno/nie	áno/nie
	skutočnosť	áno	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 2020 prešli ďalšie systémy vnútornej správy modernizáciou, čo malo za následok zefektívnenie využitia výdavkov zo štátneho rozpočtu. Avšak progres modernizácie bol z dôvodu všeobecnej pandemickej situácie výrazne pomalší oproti pôvodným predpokladom. 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 : plk. Ing. Branislav Šusta
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**	**Rok 2022**
Zefektívnené využitie výdavkov zo štátneho rozpočtu na prevádzku a údržbu jednotlivých informačných technológií	plán	áno/nie	áno/nie	áno/nie	áno/nie	áno/nie	áno/nie
	skutočnosť	áno	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.

Zdroj získavania údajov : prevádzkové záznamy, projektové stretnutia
Vypracoval : plk. Ing. Branislav Šusta
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**	**Rok 2022**
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	áno/nie
	skutočnosť	áno	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 2020 prešli ďalšie informačné systémy modernizáciou, čo malo za následok zefektívnenie využitia výdavkov aj na podpornú infraštruktúru. Avšak progres modernizácie bol z dôvodu všeobecnej pandemickej situácie výrazne pomalší oproti pôvodným predpokladom.

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 :	plk. Ing. Branislav Šusta
Schválil :	pplk. Ing. Bibiána Magáthová, PhD.