



Ročná monitorovacia správa k 31. 12. 2018

Programová štruktúra

OD9 – 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 OD9 – 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 2018 plnené na požadovanej úrovni. Plnenie programu na jednotlivých úrovniach podprogramov a prvkov ovplyvňujú najmä kvalita a stabilita legislatívneho prostredia, kvantita a stupeň utajenia utajovaných skutočností, 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. 2018 splnili.

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
Kvalitné a včasne ukončené previerky personálnej a priemyselnej bezpečnosti	Plán	áno/nie	áno/nie	áno/nie	áno/nie
	skutočnosť	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. 2018 31. 12. 2018 prijal úrad 4 738 žiadostí o vykonanie bezpečnostnej previerky navrhovanej osoby a 98 žiadostí o vydanie potvrdenia o priemyselnej bezpečnosti. Z počtu prijatých žiadostí o vykonanie bezpečnostnej previerky navrhovanej osoby bolo v hodnotenom období ukončených 4 090 bezpečnostných previerok. Z počtu prijatých žiadostí o vydanie potvrdenia o priemyselnej bezpečnosti bolo v hodnotenom období ukončených 51 bezpečnostných previerok.

Spolu bolo prijatých 4 836 žiadostí o bezpečnostnú previerku, z toho ukončených bolo 4 141 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 (z podkladov OBP)

Schválil: pplk. 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
Zaistená technická spôsobilosť na ochranu UI	Plán	áno/nie	áno/nie	áno/nie	áno/nie
	skutočnosť	áno	áno	-	-

Plnenie cieľa :

S cieľom zabezpečenia ochrany utajovaných informácií pred ich únikom prostredníctvom nežiaduceho elektromagnetického vyžarovania (ďalej len „NEV“) sa vykonáva súbor opatrení na zariadeniach technických prostriedkov (ďalej len „TP“), ako aj v priestoroch, kde budú TP umiestnené. Celý proces posudzovania z hľadiska ochrany pred NEV je náročný na prípravu, priebeh a vyhodnotenie meraní. Súbor opatrení zahŕňa najmä zónové merania priestorov, merania NEV prostriedkov šifrovej ochrany informácií (ďalej len „PŠOI“) a merania NEV zariadení TP. Merania NEV zariadení TP a PŠOI sa vykonávajú v špecializovanom TEMPEST laboratóriu v priestoroch NBÚ. Zónové merania priestorov sa vykonávajú mobilnou meracou aparátúrou. 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. V žiadosti sa špecifikujú požiadavky na výkon meraní zariadení TP, PŠOI alebo zónových meraní priestorov. Na vybavenie žiadosti môže byť potrebné zmerať niekoľko zariadení TP, PŠOI alebo priestorov. Výstupom plnenia cieľa sú protokoly, stanoviská a inštalčné záznamy, ktoré sú podkladmi k certifikácii TP alebo PŠOI.

V roku 2018 bolo prijatých 54 žiadostí o stanovisko k certifikácii TP, vykonanie meraní NEV zariadení TP a o vykonanie zónových meraní priestorov, z ktorých bolo vybavených 52. Na základe doručených žiadostí bolo vykonaných 668 meraní zariadení TP a PŠOI a 89 zónových meraní priestorov, na základe ktorých bolo kategorizovaných 153 zariadení TP a 149 priestorov.

Novými funkcionalitami úradu sú vykonávanie technických bezpečnostných prehliadok priestorov určených na ochranu utajovaných informácií na ich ochranu pred únikom odpočúvaním a meranie vlastností tienených komôr. V roku 2018 boli prijaté 2 žiadosti o vykonanie technických bezpečnostných prehliadok (prehliadnuté boli 4 priestory) a 2 žiadosti o vykonanie meraní tienených komôr (zmerané boli 2 tienené 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 2018 boli akreditované 2 komunikačné a informačné systémy pre manipuláciu utajovaných informácií NATO v súlade s Bezpečnostnou politikou NATO C-M(2002)49 a 3 systémy pre EÚ v súlade s Rozhodnutím rady (2013/488/EÚ). V roku



2018 bolo certifikovaných 87 prostriedkov potrebných na ochranu utajovaných informácií. Bola ukončená prevádzka prostriedkov ŠOI ktorým skončili certifikáty (Baranec, Hornád). Na rezortné registre boli distribuované nové prostriedky ŠOI (SINA). Bol vybudovaný segment „D“, „T“ a „T NATO“ pre spracovávanie a prenášanie informácií stupňa utajenia „dôverný“, „tajný“ a „tajný NATO“.

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
Efektívny systém pre poskytovanie dôveryhodných služieb	Plán	áno/nie	áno/nie	áno/nie	áno/nie
	skutočnosť	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 SR voči EÚ 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“). V roku 2018 bola dobudovaná a spustená do prevádzky infraštruktúra kvalifikovaných dôveryhodných služieb. Následne prebehol audit v mesiacoch júl (TSA a vydávanie certifikátov a pečatí) a október (validácia a archivácia). Systém pre poskytovanie dôveryhodných služieb je plne prispôsobený skutočným potrebám, ktoré vychádzajú z požiadaviek kladených na Národný bezpečnostný úrad zo zákona o dôveryhodných službách a z nariadenia eIDAS. K termínu zhodnocovania plnenia cieľov sa časový plán plní.

Zdroj získavania údajov : interný

Vypracoval : mjr. Ing. Peter Garaj
Schválil : pplk. Ing. Bibiána Magáthová

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
Zvýšená bezpečnosť kybernetického priestoru	Plán	áno/nie	áno/nie	áno/nie	áno/nie
	skutočnosť	áno	áno	-	-



Plnenie cieľa :

Národná jednotka SK-CERT ako samostatný útvar Národného bezpečnostného úradu v roku 2018 naďalej rozvíjala svoju pôsobnosť a spôsobilosť pri zabezpečovaní otvoreného, bezpečného a chráneného národného kybernetického priestoru.

Od 1. apríla 2018 vošiel do účinnosti zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov, ktorý vymedzil práva a povinnosti Národného bezpečnostného úradu v oblasti kybernetickej bezpečnosti. Týmto zákonom Slovenská republika transponovala Smernicu Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (ďalej len „smernica NIS“) a ako jeden z mála štátov v Európskej únii v termíne (termín transpozície bol v smernici stanovený do 9. mája 2018).

Zákon určuje úradu postavenie Národnej jednotky CSIRT. Úrad povinnosti národnej jednotky CSIRT vykonáva prostredníctvom samostatného útvaru Národnej jednotky SK-CERT, ktorej úlohou je riešenie kybernetických bezpečnostných incidentov s celoslovenskou pôsobnosťou a zodpovednosťou pri komunikácii a riešení incidentov na národnej aj medzinárodnej úrovni.

Dôležitým krokom pri budovaní Národnej jednotky SK-CERT bolo získanie medzinárodného uznania jednotky a začlenenie národnej jednotky do najdôležitejších medzinárodných organizácií, združujúcich jednotky CSIRT po celom svete. Súčasťou tohto procesu bolo vytvorenie organizačného, personálneho, procesného a technologického rámca jednotky, ktoré boli overené niekoľkými medzinárodnými auditmi, po ktorých získala Národná jednotka SK-CERT akreditovaný status v organizácii **Trusted Introducer** a členstvo v organizácii **FIRST** (Forum of Incident Response Security Teams). Táto skutočnosť, spolu s členstvom v európskej sieti národných jednotiek CSIRT Network, znamená, že Národná jednotka SK-CERT má medzinárodne potvrdené spôsobilosti na riešenie kybernetických bezpečnostných incidentov.

SK-CERT v roku 2018 riešila a koordinovala riešenie kybernetických bezpečnostných incidentov v národnom kybernetickom priestore. Spolupracovala pri tom nie len so zasiahnutými subjektami, ale aj s národnými a medzinárodnými partnermi. Na národnej úrovni sa naďalej podporuje spolupráca s CSIRT.SK, jednotkou, ktorá bola zákonom o kybernetickej bezpečnosti určená za vládnu jednotku CSIRT. Takisto bola naďalej rozvíjaná aj spolupráca s GOV CERT SK, jednotkou, ktorá vykonáva bezpečnostný a prevádzkový monitoring na úrovni siete GOVNET. Nemožno opomenúť, že národná jednotka SK-CERT rozvíja a udržiava spoluprácu a profesionálne vzťahy aj s inými subjektami, akými sú napríklad jednotka CSIRT Ministerstva obrany, Odbor počítačovej kriminality Prezídia policajného zboru, poskytovatelia internetových služieb a súkromné spoločnosti zaoberajúce sa kybernetickou bezpečnosťou.

Národná jednotka SK-CERT pokračovala vo vydávaní distribúcii bezpečnostných bulletinov a varovaní, ktoré obsahovali dôležité informácie z oblasti kybernetickej bezpečnosti, a to najmä informácie o zraniteľnostiach hardvéru a softvéru, závažných incidentoch a hrozbách v národnom a medzinárodnom kybernetickom priestore. Bulletinov a varovaní boli zasielané partnerom prostredníctvom e-mailu a takisto boli zverejňované na webovej stránke www.sk-cert.sk.

Zástupcovia SK-CERT reprezentovali úrad, ako aj Slovenskú republiku na viacerých významných medzinárodných konferenciách v oblasti kybernetickej bezpečnosti. Výsledkom týchto aktivít bolo nielen získavanie vedomostí o nových trendoch kybernetickej bezpečnosti, ale aj nadviazanie profesionálnych vzťahov v medzinárodnej komunite.

Účastou na medzinárodných kybernetických bezpečnostných cvičeniach umožnila pracovníkom SKCERT precvičiť odborné a manažérske spôsobilosti a takisto získať nové skúsenosti v oblasti



kybernetickej bezpečnosti, nových trendov riešenia kybernetických bezpečnostných incidentov a analýzy hrozieb. V roku 2018 SK-CERT absolvoval tieto cvičenia:

- Locked Shield 2018 – najväčšie NATO cvičenie, zamerané na kybernetickú bezpečnosť. Zástupcovia SK-CERT sa zúčastnili tohto cvičenia spolu so zástupcami Ministerstva obrany a CSIRT.SK.
- Cyber Europe 2018 – cvičenie agentúry ENISA, zamerané na technické, procesné a manažérske spôsobilosti jednotlivých zúčastnených členských krajín.
- CyberEx 2018 – cvičenie, zamerané na technické riešenie incidentov, forenznú analýzu a analýzu malvéru
- Cyber Coalition 2018 – cvičenie kybernetickej obrany a bezpečnosti organizované NATO.

Úrad takisto plní úlohu národného kontaktného bodu pre kybernetickú bezpečnosť voči Európskej únii, Severoatlantickej Aliancii (NATO) a Organizácii pre bezpečnosť a spoluprácu v Európe (OBSE), pričom zástupca úradu reprezentujúci Slovenskú republiku je aj členom Management board ENISA. Príslušníci úradu sa aktívne zúčastňujú na zasadnutiach Bezpečnostného výboru NATO pre bezpečnostnú politiku a zasadnutiach Informal Working Group (IWG) OBSE.

Zdroj získavania údajov : interný

Vypracoval : npor. Ing. Mgr. Andrea Pobocik, PhD.

Schválil : plk. Mgr. Rastislav Janota

OD901 – 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: pplk. JUDr. Marek Barta

OD90101 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 informácií 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: pplk. 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 2014	Rok 2015	Rok 2016	Rok 2017	Rok 2018	Rok 2019	Rok 2020
% 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 2018 bolo schválených 10 kontrol ochrany utajovaných skutočností. V septembri 2018 boli dve plánované kontroly ochrany utajovaných skutočností nahradené kontrolou ochrany utajovaných skutočností v podmienkach iného kontrolovaného subjektu, ktorá bola v novembri 2018 z plánu vonkajších kontrol na rok 2018 vypustená. Možno teda konštatovať, že vonkajšie kontroly ochrany utajovaných skutočností boli podľa schváleného plánu vonkajších kontrol na rok 2018 vykonané v plnom rozsahu.

Zdroj získavania údajov: interný

Vypracoval: mjr. JUDr. Martin Šátek, PhD.

Schválil: pplk. Ing. JUDr. Alexandra Dianišková

Cieľ 2: *Zabezpečiť spôsobilosť osôb na ochranu utajovaných informácií*

Gestor: *sekcia previerok*

Zodpovedný: *riaditeľ sekcie previerok*

Názov ukazovateľa		Rok 2014	Rok 2015	Rok 2016	Rok 2017	Rok 2018	Rok 2019	Rok 2020
% vybavených žiadostí o vykonanie bezpečnostnej previerky v zákonnej lehote	plán	100	100	100	100	100	99	97
	skutočnosť	100	99,77	98,83	99,83	99,06	-	-

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. 2018 do 31. 12. 2018 vybaviť 4 999 žiadostí o vykonanie bezpečnostnej previerky.

V hodnotenom období bolo vybavených 4 952 žiadostí, čo predstavuje 99,06 % vybavených žiadostí.

Percentuálne vyjadrenie vybavených žiadostí z počtu prijatých žiadostí, ktoré možno vybaviť vzhľadom na zákonom stanovené lehoty odráža 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. 100 % 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. Vzhľadom na uvedené skutočnosti, úrad nemohol vykonať všetky procesné úkony v zákonom stanovených lehotách, čo bolo dôvodom zníženia percenta vybavených bezpečnostných previerok. Pokles percenta vybavených žiadostí však podstatne neovplyvnil plnenie zámeru podprogramu.

Udržateľnosť cieľa v budúcnosti závisí od vyššie uvedených faktorov.

Zdroj získavania údajov: interný

Vypracoval: pplk. JUDr. Zuzana Gavorníková (z podkladov OBP)

Schválil: pplk. 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
% vykonaných skúšok a preškolení z požadovaného počtu	Plán	100	100	100	100
	skutočnosť	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 2018 bol úrad požiadaný o vykonanie 177 skúšok bezpečnostného zamestnanca. Skúšku bezpečnostného zamestnanca vykonalo 162 uchádzačov úspešne a 15 boli neúspešní. Z celkového počtu uchádzačov, na ktorých bola zaslaná žiadosť o vykonanie skúšky bezpečnostného zamestnanca, odbor vonkajších vzťahov kancelárie úradu pozval všetkých 177 uchádzačov.

V roku 2018 odbor vonkajších vzťahov zverejnil na webovom sídle úradu rôzne témy preškolení, na ktoré sa mohli záujemcovia prihlásiť. Vykonaných bolo celkovo 54 preškolení, ktorých sa zúčastnilo 421 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 : mjr. JUDr. Andrea Senková

Schválil : pplk. Blažej Lippay, M.A., PhD.

OD90102 ***Technická spôsobilosť na ochranu utajovaných informácií***

Gestor: ***technická sekcia***

Zodpovedný: ***riaditeľ technickej sekcie***

Komentár :

Ciele boli stanovené v súlade s požiadavkami platnej legislatívy SR (najmä zákona č. 215/2004 Z. z. 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.



Vypracovali: pplk. Ing. Dušan Spáč, 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 2014	Rok 2015	Rok 2016	Rok 2017	Rok 2018	Rok 2019	Rok 2020
% vybavených žiadostí	plán	97	97	97	97	97	97	97
v zákonom stanovenej lehote	skutočnosť	100	100	100	100	100	-	-

Plnenie cieľa:

V roku 2018 boli akreditované 2 komunikačné a informačné systémy pre manipuláciu utajovaných informácií NATO v súlade s Bezpečnostnou politikou NATO C-M(2002)49 a 3 systémy pre EÚ 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 zabezpečujú plnenie stanoveného cieľa a do budúcnosti nepredpokladajú žiadne riziká a odchýlky od rozpočtových zámerov.

Zdroj získavania údajov: interný

Vypracoval: pplk. Ing. Dušan Spáč

Schválil: pplk. Ing. Bibiána Magáthová, PhD.

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 2014	Rok 2015	Rok 2016	Rok 2017	Rok 2018	Rok 2019	Rok 2020
% vybavených žiadostí	plán	97	97	97	97	97	97	97
v zákonom stanovenej lehote	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 „MZIP a TZP“), technické prostriedky (ďalej len „TP“) a prostriedky šifrovej ochrany informácií (ďalej len „PŠOI“).

V roku 2018 bolo celkovo prijatých 104 žiadostí o certifikáciu (MZIP a TZP 36, TP 51, PŠOI 17) a 19 žiadostí o vydanie dodatku (TP 14, PŠOI 5). Z celkového počtu prijatých žiadostí bolo vybavených 89 žiadostí (MZIP a TZP 31, TP 42, PŠOI 16) a 19 dodatkov (TP 14, PŠOI 5). 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.

Proces certifikácie zariadení a prostriedkov pozostáva z niekoľkých fáz (podanie žiadosti spolu s požadovanou sprievodnou dokumentáciou, overovanie spôsobilosti zariadenia a prostriedku, vydanie certifikátu alebo zaslanie rozhodnutia o neudelení certifikátu). Výsledky činnosti pri procese certifikácie nezávisia len od úradu, ale tiež od iných subjektov, napr. od žiadateľa, výrobcu, autorizovanej osoby a v prípade dovážaných PŠOI aj od zahraničnej certifikačnej autority a dodávateľa.

Použitie certifikovaných zariadení a prostriedkov vyplýva priamo z legislatívy a je jedným zo základných predpokladov na zabezpečenie ochrany utajovaných skutočností. Vzhľadom na neustále meniacu sa bezpečnostnú situáciu a tiež na technologický rozvoj je možné očakávať nové hrozby a nové požiadavky na zariadenia a prostriedky, čomu sa bude musieť prispôbiť aj legislatíva v oblasti certifikácie.

V oblasti certifikácie neboli v hodnotenom období zistené žiadne riziká a odchýlky od rozpočtových zámerov.

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

OD90103 *Spôsobilosť na ochranu zahraničných utajovaných informácií*
Gestor: kancelária úradu
Zodpovedný: riaditeľ kancelárie úradu

Komentár :

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 centrálného registra.

Vypracoval: mjr. Mgr. Dana Ružovičová
Schválil: pplk. Blažej Lippay, M.A., PhD.

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

Názov ukazovateľa		Rok 2014	Rok 2015	Rok 2016	Rok 2017	Rok 2018	Rok 2019	Rok 2020
% poskytnutých služieb z počtu žiadostí o poskytnutie služby	plán	88	91	93	94	97	97	97
	skutočnosť	97	91	97	98	98	-	-



Plnenie cieľa :

V roku 2018 bolo plánované vykonať 97% poskytnutých služieb. Dosiahnuté výsledky v období od 01. 01. 2018 do 31. 12. 2018 zabezpečili plnenie zámeru programu. V sledovanom období bolo vykonané plnenie na 98 %.

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 6 226 zahraničných utajovaných skutočností označených stupňom utajenia Vyhradené, z toho 6 129 zaevidovali registre utajovaných skutočností.

Cieľ je merateľný a kvantifikovateľný vhodným merateľným ukazovateľom výsledku, pričom obsahuje konkrétnu cieľovú hodnotu - 98 % 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 centrálnemu registru.

Zdroj získavania údajov : interný

Vypracoval : mjr. Mgr. Dana Ružovičová
Schválil : pplk. Blažej Lippay, M.A., PhD.

OD904 – 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 pre poskytovanie dôveryhodných služieb 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. V roku 2018 bol vykonaný audit novovybudovaných kvalifikovaných dôveryhodných služieb orgánom posudzovania zhody. Novovybudovaná



infraštruktúra aj poskytované služby úspešne prešli auditom. Vonkajšie kontroly kvalifikovaných poskytovateľov dôveryhodných služieb boli podľa schváleného plánu vonkajších kontrol na rok 2018 vykonané v plnom rozsahu. V súčasnosti sú zabezpečené optimálne podmienky na poskytovanie dôveryhodných služieb v súlade so zákonom. K termínu zhodnocovania plnenia cieľov sa časový plán plní.

Vypracoval: mjr. Ing. Peter Garaj
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
% vykonaných dohľadov nad poskytovateľmi dôveryhodných služieb	Plán	100	100	100	100
	skutočnosť	100	100	-	-

Plnenie cieľa :

V pláne vonkajších kontrol na rok 2018 boli schválené 2 vonkajšie kontroly kvalifikovaných poskytovateľov dôveryhodných služieb. V septembri 2018 bola jedna plánovaná kontrola kvalifikovaného poskytovateľa služieb nahradená kontrolou ochrany utajovaných skutočností v podmienkach iného kontrolovaného subjektu. Možno teda konštatovať, že vonkajšie kontroly kvalifikovaných poskytovateľov dôveryhodných služieb boli podľa schváleného plánu vonkajších kontrol na rok 2018 vykonané v plnom rozsahu.

Zdroj získavania údajov : interný

Vypracoval : mjr. JUDr. Martin Šátek, PhD.
Schválil : pplk. Ing. JUDr. Alexandra Dianišková

OD905 – KYBERNETICKÁ BEZPEČNOSŤ

Zámer: Zabezpečiť budovanie spôsobilostí na úseku kybernetickej bezpečnosti

Gestor: Národná jednotka SK-CERT

Zodpovedný: riaditeľ Národnej jednotky SK-CERT

Komentár :

Národná jednotka SK-CERT ako samostatný útvar Národného bezpečnostného úradu v roku 2018 pokračovala v rozvíjaní svojich služieb a spôsobilostí v národnom kybernetickom priestore.

Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov vymedzil práva a povinnosti Národného bezpečnostného úradu v oblasti kybernetickej bezpečnosti, pričom určil úradu postavenie Národnej jednotky CSIRT. Úrad povinnosti národnej jednotky CSIRT, ako aj poskytovanie služieb vykonáva prostredníctvom samostatného útvaru Národnej jednotky SK-CERT. Prijatie zákona o kybernetickej bezpečnosti bol pozitívny krok, ktorý určil rámec požiadaviek na kybernetickú bezpečnosť a výkon práv a povinností v tejto oblasti.



Vypracoval: npor. Ing. Mgr. Andrea Pobocik, PhD.

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

Plnenie cieľa :

Na úseku kybernetickej bezpečnosti nadobudol dňa 01. 04. 2018 účinnosť zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov. Dňa 15. 06. 2018 nadobudli účinnosť tri vykonávacie predpisy, a to vyhláška Národného bezpečnostného úradu č. 164/2018 Z. z., ktorou sa určujú identifikačné kritériá prevádzkovej služby, vyhláška Národného bezpečnostného úradu č. 165/2018 Z. z. ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov a vyhláška Národného bezpečnostného úradu č. 166/2018 Z. z. o podrobnostiach o technickom, technologickom a personálnom vybavení jednotky pre riešenie kybernetických bezpečnostných incidentov. Dňa 01. 01. 2019 nadobudne účinnosť vyhláška Národného bezpečnostného úradu, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení. Možno teda konštatovať, že v roku 2018 boli vytvorené legislatívne podmienky pre kybernetickú bezpečnosť v Slovenskej republike.

Zdroj získavania údajov : www.slov-lex.sk

Vypracoval : mjr. JUDr. Martin Šátek, PhD.

Schválil : pplk. Ing. JUDr. Alexandra 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
Vytvorenie optimálnych technických podmienok	Plán	áno/nie	áno/nie	áno/nie	áno/nie
	skutočnosť	áno	áno	-	-

Plnenie cieľa :

Národná jednotka SK-CERT v roku 2018 pokračovala s budovaním softvérového a hardvérového zabezpečenia, slúžiaceho na efektívny výkon bezpečnostného a prevádzkového monitoringu ako jednej zo služieb tohto pracoviska.

Vybudovanie modernej infraštruktúry v rámci Národnej jednotky SK-CERT je dôležitým aspektom pre vytvorenie optimálnych podmienok vysokej úrovne kybernetickej bezpečnosti nie len na tomto pracovisku, ale implementáciou najnovších technologických trendov aj v rámci národného kybernetického priestoru.



Vytvorenie optimálnych technických podmienok je úzko späté aj s personálnym zabezpečením národnej jednotky SK-CERT. Personálny stav jednotky smeruje k ustáleniu jednotlivých rolí pracovníkov tak, aby bolo možné pokryť všetky služby, ktoré má Národná jednotka SK-CERT zo zákona poskytovať.

Zdroj získavania údajov : interný

Vypracoval : npor. Ing. Mgr. Andrea Pobocik, PhD.

Schválil : plk. Mgr. Rastislav Janota

OD903 – 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 OD9 – 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 2014	Rok 2015	Rok 2016	Rok 2017	Rok 2018	Rok 2019	Rok 2020
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 prispôbiť 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: pplk. Mgr. Zuzana Ružovičová
Schválil: plk. Ing. Anna Friesseová

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

Názov ukazovateľa		Rok 2014	Rok 2015	Rok 2016	Rok 2017	Rok 2018	Rok 2019	Rok 2020
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 - OUSIP, infraštruktúra, VoIP). Projekt OUSIP a projekt VoIP boli začaté budú realizované v roku 2019. Projekt serverovne a projekt na obnovu infraštruktúry bude potrebné realizovať v najbližšom období, čím sa odstráni 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 : interný

Vypracoval : mjr. Ing. Peter Garaj

Schválil : pplk. Ing. Bibiána Magáthová, PhD.



Programová štruktúra – medzirezortný program

OEK – 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

**OEKOU – 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 OEKOU 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 : mjr. Ing. Peter Garaj
Schválil : pplk. Ing. Bibiána Magáthová, PhD.

OEKOU01 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
Zefektívnené využitie výdavkov zo štátneho rozpočtu na prevádzku a údržbu jednotlivých informačných technológií	plán	áno/nie	áno/nie	áno/nie	áno/nie
	skutočnosť	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 2018 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 : interný

Vypracoval : mjr. Ing. Peter Garaj

Schválil : pplk. Ing. Bibiána Magáthová, PhD.

OEKOU02 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
Zefektívnené využitie výdavkov zo štátneho rozpočtu na prevádzku a údržbu jednotlivých informačných technológií	plán	áno/nie	áno/nie	áno/nie	áno/nie
	skutočnosť	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 OEKOU02 – 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 plán obstarávania.



Zdroj získavania údajov : interný

Vypracoval : mjr. Ing. Peter Garaj
Schválil : pplk. Ing. Bibiána Magáthová

OEKOU03 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
Zefektívnené využitie výdavkov zo štátneho rozpočtu na zabezpečenie infraštruktúry na prevádzku jednotlivých informačných systémov	plán	áno/nie	áno/nie	áno/nie	áno/nie
	skutočnosť	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 2018 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 OEKOU03 – 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 : interný

Vypracoval : mjr. Ing. Peter Garaj
Schválil : pplk. Ing. Bibiána Magáthová, PhD.