

Aktuálny ročný komponent výročnej správy Národného bezpečnostného úradu – rok 2010

Úvod

Národný bezpečnostný úrad je ústredným orgánom štátnej správy pre oblasť ochrany utajovaných skutočností, elektronického podpisu a je ústredným šifrovým orgánom.

Činnosť Národného bezpečnostného úradu vymedzujú dva zákony – zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov a zákon č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov spolu s príslušnými vykonávacími predpismi.

Úradu patrí nezastupiteľné postavenie pri vytváraní systému ochrany utajovaných skutočností, pri príprave národnej legislatívy pre oblasť ochrany utajovaných skutočností a tvorbe strategických koncepčných dokumentov v tejto oblasti.

Národný bezpečnostný úrad je partnerom národných bezpečnostných autorít a medzinárodných bezpečnostných štruktúr NATO a EÚ. Z tejto pozície sa podieľa na určovaní spoločných bezpečnostných noriem a zabezpečovaní ich implementácie. Okrem iného má aj povinnosť garantovať dodržiavanie zásad manipulácie s utajovanými skutočnosťami postúpenými SR zo zahraničia.

A1 Činnosť NBÚ v roku 2010

A 1.1 Plán legislatívnych úloh, legislatívna činnosť úradu

Národný bezpečnostný úrad na začiatku roka spracoval rýchlu a krátku novelu vyhlášky Národného bezpečnostného úradu č. 135/2009 Z. z. o vyhotovení a overovaní elektronického podpisu a časovej pečiatky. Predmetom novelizácie uvedenej vyhlášky bolo predĺženie prechodného obdobia používania certifikovaných produktov pre zaručený elektronický podpis do uplynutia doby platnosti certifikátov týchto produktov, najdlhšie však do 31. decembra 2010. Vyhláška nadobudla účinnosť 1. februára 2010.

Prioritnou úlohou v legislatívnej oblasti bolo aj v roku 2010 pokračovanie legislatívnych prác na návrhu zákona o ochrane utajovaných informácií a o zmene a doplnení niektorých zákonov. V tejto súvislosti prebiehali v rámci mesačných pracovných stretnutí zainteresovaných útvarov Národného bezpečnostného úradu rámcové diskusie ku konkrétnym návrhom, zmenám a problémom, ktoré vyplynuli v prvom rade z analýzy jednotlivých pripomienok uplatnených k návrhu nového zákona v rámci medzirezortného pripomienkového konania. V druhom rade sa prejednávali problematiké a sporné otázky vyplývajúce z aplikácie jednotlivých ustanovení súčasnej platnej právnej úpravy, ktoré sa riešia interpretáciou, resp. prostredníctvom výkladových stanovísk, a tieto nové riešenia sa následne zapracovali a premietli do konkrétnych legislatívnych úprav v návrhu nového zákona. Opätovné predloženie návrhu nového zákona do legislatívneho procesu sa predpokladá v roku 2011.

Počas roka 2010 Národný bezpečnostný úrad ako ústredný orgán štátnej správy pre oblasť ochrany utajovaných skutočností vydal 42 rozhodnutí vo veci nevydania osvedčenia na oboznamovanie sa s utajovanými skutočnosťami a nevydania potvrdenia o priemyselnej bezpečnosti. V tejto súvislosti bolo proti prvostupňovému rozhodnutiu Národného bezpečného úradu podaných 26 odvolaní podľa zákona č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. Odvolací orgán, ktorým je Výbor Národnej rady Slovenskej republiky na preskúmanie rozhodnutí Národného bezpečnostného úradu zriadený ústavným zákonom č. 255/2006 Z. z., potvrdil 20 a zrušil 6 prvostupňových rozhodnutí. V tejto súvislosti bol Národný bezpečnostný úrad stranou v prípade 2 žalôb uplatnených na Najvyššom súde Slovenskej republiky, ktorý je príslušný na preskúmanie vyššie uvedených rozhodnutí.

Rozkladová komisia riaditeľa Národného bezpečnostného úradu zriadená podľa zákona č. 71/1967 Zb. o správnom konaní riešila v roku 2010 dva rozklady podané v správnom konaní vo veciach, o ktorých rozhodol v prvom stupni Národný bezpečnostný úrad. V oboch prípadoch bolo rozkladom vyhovené.

V roku 2010 bolo vo vestníku Národného bezpečnostného úradu vydaných 8 interných predpisov formou nariadení riaditeľa Národného bezpečnostného úradu. Zmeny nastali najmä v rámci organizačnej štruktúry Národného bezpečnostného úradu, kde došlo k drobným zmenám v povinnostiach a úlohách dotknutých útvarov a k zmene a rozsahu oprávnení a povinností na jednotlivých stupňoch riadenia. V ostatných prípadoch išlo len o novelizácie starších nariadení, resp. o vydanie nových nariadení, ktoré nahrádzali dovtedy platné nariadenia a tieto zmeny reflektovali novú platnú právnu úpravu a viedli k vyššej efektívnosti procesov.

Národný bezpečnostný úrad zapísaný ako znalecká organizácia v zozname znalcov, tlmočníkov a prekladateľov vedenom Ministerstvom spravodlivosti SR v odbore 520000 – ochrana utajovaných skutočností v priebehu roka 2010 nerealizoval žiadne znalecké skúmanie.

Činnosť úradu z hľadiska medzinárodných vzťahov

Z hľadiska medzinárodných vzťahov bolo prioritou plnenie úloh vyplývajúcich z členstva Slovenskej republiky v NATO a EÚ. Po rapidnom raste členov, v neustále sa meniacom bezpečnostnom prostredí a pri narastajúcom množstve ohrození vyplývajúcich z elektronizácie každodenných činností sa bezpečnostné orgány oboch integračných zoskupení zaoberajú otázkou potrebnej reformy. Ďalším faktorom vplyvujúcim na tieto otázky je ekonomická kríza, ktorá aj v NATO a EÚ vyvíja tlak na efektívnosť a má za následok snahu o znižovanie nákladov.

V rámci NATO je aj na základe záverov Lisabonského summitu dôraz kladený na ochranu kybernetického priestoru. Prebiehajúce inštitucionálne reformy reagujú na tieto skutočnosti. V rámci radiácií štruktúr NATO bola vytvorená nová sekcia, ktorej kompetenciou budú nové bezpečnostné hrozby. Keďže medzi tieto patrí aj ochrana kybernetického priestoru, NBÚ sa zúčastňuje práce tejto novej sekcie ako kontaktný bod SR voči NATO. V roku 2010 sa SR po prvý krát zúčastnila ako plnohodnotný účastník cvičenia ochrany kybernetického priestoru NATO. Koordinátorom zapojenia všetkých cvičiacich inštitúcií SR bol NBÚ. Výsledky a skúsenosti z cvičenia poukázali na nedostatky, ktoré spočívajú v prvom rade v nedoriešenej legislatíve a z toho vyplývajúcich nejasných kompetenčných vzťahoch. Na druhej strane cvičenie preverilo odborné a praktické zručnosti príslušníkov úradu, ktoré je na vysokej úrovni a je porovnateľné s odborníkmi z vyspelých členských krajín. Spolupráca s bezpečnostnými orgánmi NATO bola aj v roku 2010 na mimoriadne dobrej úrovni, čoho dôkazom je prijatie riaditeľa NBÚ F. Blanáríka končiacim i novým riaditeľom Bezpečnostného

úradu NATO (NOS). M. Evanoff po 3 ročnom období skončil s výkonom funkcie riaditeľa NOS a na jeho miesto nastúpil S. Smith, ktorý ako prvého predstaviteľa členskej krajiny vo svojej funkcii prijal práve F. Blanárka.

V rámci Európskej únie pokračuje diskusia a hľadanie riešení pre novú úpravu ochrany utajovaných skutočností EÚ už niekoľko rokov. Vzhľadom na komplikovaný inštitucionálny systém prijímania rozhodnutí a náročné hľadanie kompromisov pri veľkom počte členov sa nedarí prijať také pravidlá, ktoré by boli jednotné a systematické v rámci všetkých orgánov a súčastí EÚ. Už Správa o činnosti NBÚ za rok 2009 konštatuje, že vláda SR schválila tzv. multilaterálnu dohodu, ktorá je „základným rámcom pre vznik a výmenu utajovaných skutočností v členských krajinách EÚ a rámcovo upravuje základné princípy ochrany a manipulácie s utajovanými skutočnosťami EÚ“ pričom „zmluva zatiaľ podpísaná nie je, keďže neprešla schvaľovacím procesom vo všetkých členských krajinách“. Tento stav platí aj rok po napísaní týchto slov. NBÚ aktívne pristupuje k práci v bezpečnostných zložkách EÚ a prispieva k hľadaniu kompromisov.

V roku 2010 sa uskutočnilo druhé stretnutie riaditeľov bezpečnostných autorít krajín V4 v Poľskej republike v Krakove za účasti predstaviteľov NATO a EÚ. Táto nová tradícia, ktorej iniciátorom a prvým hosťom bol NBÚ v roku 2009 sa ukazuje ako prospešná, keďže mnohé spoločné problémy a spoločný postup na pôde NATO i EÚ je možné prediskutovať v neformálnej rovine. Takéto stretnutia uvítali aj predstavitelia NATO a EÚ, keďže im umožňuje bezprostrednejšie a adresnejšie komunikovať problematiku týkajúcu sa krajín V4.

Na poli bilaterálnej spolupráce pokračovalo rozširovanie počtu bilaterálnych zmlúv pre oblasť výmeny a ochrany utajovaných skutočností. NBÚ ako gestorský orgán oslovuje svojich partnerov v zahraničí a pripravuje návrhy textov zmlúv, ktoré následne schvaľuje vláda SR. V roku 2010 boli podpísané zmluvy s Francúzskom a Cyprom a v procese dohodovania návrhov textov zmlúv sú zmluvy s Poľskom, Luxemburskom, Indiou. Na základe požiadaviek rozvíjajúcej sa spolupráce ďalších inštitúcií SR (hlavne Ministerstva obrany SR) so svojimi partnermi v zahraničí, pri ktorej je vysoký predpoklad výmeny utajovaných skutočností oslovil úrad príslušné orgány v Arménsku a v Spojených arabských emirátoch so žiadosťou o rokovanie k predmetným zmluvám. V prípade Kórey, s predstaviteľmi ktorej bol NBÚ v kontakte niekoľko mesiacov však bola snaha neúspešná. Na základe centrálného rozhodnutia v Soule síce pretrváva záujem o spoluprácu aj v tejto oblasti, ale nie je prioritou v krátkodobom časovom horizonte.

Po prijatí príslušnej legislatívy a po ustanovení centrálnej štátnej autority bol nadviazaný kontakt so srbskou bezpečnostnou autoritou s návrhom metodologickej pomoci pri budovaní spôsobilostí v oblasti OUS. Srbský model OUS z časti vychádza zo slovenského, keďže zodpovední srbskí predstavitelia boli na študijnej návšteve v SR a vážne sa zaujímali o slovenský model. Pomoc v rámci prístupových procesov pokračovala aj v ďalších krajinách západného Balkánu. Experti na oblasť informačnej bezpečnosti viedli seminár k svojej problematike pre bezpečnostné authority Bosny a Hercegoviny a pokračovala komunikácia s Macedónskou republikou, ktorá vyústila v študijnej návšteve na NBÚ SR začiatkom roka 2011.

A 1.2 Súhrnná charakteristika hospodárenia a zhodnotenie výsledkov hospodárenia podľa rozpočtu kapitoly

1.1. Súhrnná charakteristika a hospodárenie v roku 2010

1.1.1. Charakteristika činnosti

Zákonom Národnej rady SR č. 241/2001 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov, bol zriadený Národný bezpečnostný úrad ako ústredný orgán štátnej správy. V súlade s opatrením Ministerstva financií SR č. 64 z 26. septembra 2001 dňom 1. októbra 2001 bol Národný bezpečnostný úrad zriadený ako samostatná rozpočtová kapitola č. 41 – Národný bezpečnostný úrad.

Národný bezpečnostný úrad plní úlohy vyplývajúce mu zo zákona č. 215/2004 Z. z. o ochrane utajovaných skutočností, zákona č. 215/2002 Z. z. o elektronickom podpise a príslušných vyhlášok, uznesení vlády a prevzatých záväzkov voči NATO a EÚ.

V hodnotenom roku Národný bezpečnostný úrad mal definované svoje hlavné úlohy v Ročnom pláne NBÚ na rok 2010, ktoré boli plnené nasledovne:

1. Zabezpečenie legislatívneho procesu návrhu nového zákona o ochrane utajovaných informácií a súvisiacich nových vyhlášok NBÚ

Úloha sa priebežne plní.

V oblasti legislatívnych úprav pokračovala príprava nového zákona o ochrane utajovaných informácií, ktorého legislatívny proces bol de facto prerušený v roku 2009. V záujme zapracovania pripomienok zaslaných v rámci medzirezortného pripomienkového konania a v záujme prípravy nového znenia, ktoré bude opätovne predložené do legislatívneho procesu úrad požiadal o vypustenie predloženia návrhu tohto zákona z legislatívnych úloh vlády na rok 2010. Nový návrh by mal predložený rezortom na pripomienkovanie v priebehu roka 2011.

2. Pokračovanie v realizácii KOUS spracovaním podkladov podľa priloženého harmonogramu

Aj v roku 2010 pokračovala realizácia Koncepcie ochrany utajovaných skutočností podľa plánovaného harmonogramu. Dôraz sa kládol na zvyšovanie odbornej pripravenosti príslušníkov a zamestnancov úradu. Na základe dohôd s vysokými školami boli vypísané 4 témy doktorandského štúdia k problematike OUS, ktoré študujú 4 príslušníci NBÚ. So súhlasom úradu študuje na vysokých školách ďalších 11 príslušníkov úradu.

Koncepcia ochrany utajovaných skutočností SR (ďalej len koncepcia) bola v roku 2010 realizovaná spracovávaním ďalších materiálov, ktoré po obsahovej stránke prehľbovali a rozširovali tri strategické realizačné projekty koncepcie. Ich konečným cieľom je optimálny systém ochrany a bezpečnosti utajovaných skutočností. Do ich riešenia boli zapojení, okrem odborných útvarov úradu, aj odborníci z iných rezortov a akademická obec.

Cieľom prvého strategického projektu je teoretické rozpracovanie problematiky ochrany utajovaných skutočností. V roku 2010 bol popísaný systém ochrany a bezpečnosti utajovaných

skutočností vo všetkých podstatných vnútroštátnych a medzinárodných väzbách, doplnený rozšírenou verziou nového terminologického slovníka. Bola popísaná a publikovaná tzv. úloha bezpečnosti, cieľom ktorej je odvodenie národných bezpečnostných štandardov od bezpečnostných hrozieb. Zároveň bola popísaná aj metodika jej riešenia v reálnom a kybernetickom priestore v dynamicky sa meniacom bezpečnostnom prostredí. Publikovaná bola aj optimalizačná úloha pre riešenie bezpečnosti utajovaných skutočností.

Cieľom druhého strategického projektu je vytvorenie systému prípravy ľudských zdrojov v novom bezpečnostnom prostredí. V roku 2010 boli vypracované ďalšie profily ľudských zdrojov, zámer ich kariérneho rastu, ale aj ich komplexného zabezpečenia. Cieľom uvedeného procesu je príprava a udržanie kvalitných ľudských zdrojov a personálna stabilita úradu. V rámci podpísaných dohôd o spolupráci s vysokými školami sa uskutočnil ďalší ročník Špecializačného štúdia príslušníkov NBÚ, za aktívnej účasti zamestnancov NBÚ a pedagógov Akadémie PZ, ktorému predchádzala metodická príprava lektorov. Boli zadané nové témy bakalárskych, diplomových a doktorandských prác. V januári a júni 2010 sa na NBÚ uskutočnili stáže študentov z Univerzity Mateja Bela v Banskej Bystrici a Univerzity Komenského v Bratislave. Boli publikované odborné články v recenzovaných časopisoch Fakulty špeciálneho inžinierstva Žilinskej univerzity a vybraní príslušníci NBÚ sa zúčastnili na medzinárodnej vedeckej konferencii Akadémie ozbrojených síl v Liptovskom Mikuláši (AOS LM) a ďalších odborných stretnutí. Príslušníci úradu sa ako lektori zúčastňujú na kurzoch organizovaných AOS LM, svojimi vyjadreniami a názormi úrad prispieva k práci Akreditačnej komisii pri akreditácii študijných odborov, ktorých predmetov je okrem iného aj OUS.

Cieľom tretieho strategického projektu je navrhnutie vnútroštátne a medzinárodne prepojeného systému riadenia OUS. V roku 2010 bola ďalšia verzia cieľového materiálu, vychádzajúca z nových funkcionalít úradu, plynúcich z aktuálnych zmien bezpečnostného prostredia. Návrh novej organizačnej štruktúry je prepojený s profilovaním nových ľudských zdrojov a nových činností, odvodených od nových cieľov.

3. Prejsť z projektovej do realizačnej fázy budovania Nosnej siete na prenos US

Už vo fáze plánovania bolo jasné, že rozsah plnenia tejto úlohy bude limitovaný pridelenými finančnými prostriedkami. Nakoľko v roku 2010 neboli úradu pridelené žiadne prostriedky na realizáciu projektu, úloha nebola splnená a jej plnenie sa očakáva (plánuje) v ďalšom období.

4. Zlepšiť schopnosti v oblasti ochrany kyberpriestoru

1. KIS Apeiron

Medzirezortný komunikačný a informačný systém Apeiron, ktorý je určený na výmenu informácií zúčastnených rezortov (NBÚ, MO SR(BÚ, ZASKIS), MZV SR, MV SR, VSS, VOS, SIS (po certifikácii)) v oblasti ochrany kybernetického priestoru. Vzhľadom na závažnosť informácií, je tento systém budovaný na vytváranie, spracovanie, prenos a ochranu utajovaných skutočností pre stupeň VYHRADENÉ.

Úlohou v roku 2010 bolo navrhnuť a čiastočne realizovať pilotnú prevádzku KIS Apeiron v rozsahu základných sieťových služieb, vybraných aplikačných služieb a monitoringu. Napriek počiatocným ťažkostiam bola navrhnutá a postupne aktualizovaná bezpečnostná sieťová architektúra. KIS Apeiron bol spustený do testovacej prevádzky v máji 2010. Medzirezortná časť z dôvodu nastavení GOVNET hraničných smerovačov a konfigurovania PŠOI bola spustená v septembri 2010. Systém poskytoval dve základné služby, a to web portál a mail. Obe sú hlavne využívané pre SK

CSIRC. Popritom boli realizované podporné služby DNS, Active Directory, firewall, NTP server. Navyiac voči pôvodnému zadaniu boli realizované ďalšie podporné služby – pravidelné aktualizácie AV a antivírusový monitoring.

Pre systém bola v novembri 2010 spracovaná prvá verzia bezpečnostnej dokumentácie a následne bol systém certifikovaný pre národné, EÚ a NATO US pre stupeň VYHRADENÉ. Po úspešnom absolvovaní cvičenia NCDEx2010, bol KIS Apeiron prevádzkovaný v zmysle zadaných cieľov. V decembri 2010 bol na KIS Apeiron čiastočne realizovaný hardening. V systéme boli vytvorené základy pre manažment podsietí (MAN-LAN) pre správu zariadení a serverov. Čiastočne bol integrovaný monitoring. Bola pripojená KI pre SK CSIRC s prevádzkovým monitoringom, kde bol inštalovaný systém CA Spectrum. Bola realizovaná jeho základná konfigurácia a zahájený proces pripájania monitorovaných zariadení, serverov a služieb.

Záverom do ďalšieho obdobia je trvalá certifikácia systému pre národné, EÚ a NATO US pre stupeň VYHRADENÉ a vybudovanie ochrany časti pre NBÚ vyhradeného nosného média GOVNET WAN firewallom s IPS a testovacieho (s prvkami záložného) prostredia pre KIS Apeiron.

2. Portál SK CSIRC

Portál SK CSIRC bol vytváraný súčasne s budovaním KIS Apeiron. Do testovacej prevádzky na OKO bol spustený v apríli 2010. Do plnej testovacej prevádzky pre celý KIS Apeiron, bol spustený v septembri 2010. Počas cvičenia NCDEx2010 bol zdrojom údajov pre zúčastnené rezorty. Portál SK CSIRC je plne integrovaný do KIS Apeiron a je jeho neoddeliteľnou časťou. Jeho funkčnosť je preto spojená s funkčnosťou samotného KIS Apeiron. Úlohou do ďalšieho obdobia je jeho pravidelná aktualizácia a rozvoj, ktoré sú súčasťou prevádzky monitorovacieho centra SK CSIRC.

3. Monitoring sietí, analýza a korelácia udalostí

Realizácia 1. etapy pre služby SK CSIRC.

V júni 2010 bola pripravená (po predošlej analýze) architektúra monitorovacieho centra. Boli vyčlenené priestory (kanc. č. 914). Nosnú technológiu tvoria aplikačné systémy CA Spectrum – prevádzkový monitoring a ArcSight Express – bezpečnostný monitoring. V auguste 2010 bola podpísaná zmluva o dielo na dodávku ArcSight Express a niektorých iných zariadení monitorovacieho centra. V priebehu septembra a októbra 2010 boli realizované prípravné práce a obstaranie niektorých častí:

- vytvorenie technologickej miestnosti č. 902 (plastová priečka, klimatizácia, privedenie samostatného elektrického okruhu, premiestnenie existujúcej technológie).
- obstaranie nábytku pre monitorovacie centrum
- obstaranie 2 ks PC staníc, ich inštalácia a integrovanie do monitoringu
- obstaranie veľkoplošných zobrazovacích monitorov, ich inštalácia a inštalácia monitorovacieho pola so 6 ks klasických monitorov.

V novembri 2010 bolo zahájené plnenie zmluvy o dielo, ktorej predmetom bola dodávka technológie ArcSight. Bezpečnostný monitorovací systém (ArcSight Express) bol odovzdaný 7.12.2010. Počas NCDEx2010 bola odhalená chyba filtrovacích mechanizmov, ktorá nebola dodávateľom do konca roka 2010 odstránená.

Napriek uvedeným nedostatkom (sú použiteľné iné analytické nástroje na vyhľadávanie v logoch) je možná úloha, tak ako bola definovaná, považovať za splnenú. Pre rok 2011 úloha pokračuje vo forme plného integrovania s KIS Apeiron.

1.1.2. Zhodnotenie plnenia záväzných ukazovateľov

Vládny návrh zákona o štátnom rozpočte na rok 2010 bol prerokovaný v orgánoch Národnej rady Slovenskej republiky a schválený dňa 4.11.2009 zákonom č. 497/2009 Z. z.

Nadväzne na bod C.1 uznesenia vlády SR č. 692 zo dňa 30. septembra 2009 k návrhu rozpočtu verejnej správy na roky 2010 až 2012 boli Národnému bezpečnostnému úradu oznámené záväzné ukazovatele štátneho rozpočtu na rok 2010 v rozsahu nižšie uvedených údajov.

Rozpis záväzných ukazovateľov rozpočtu kapitoly 41 - Národný bezpečnostný úrad a vplyv rozpočtových opatrení na výšku rozpočtu k 31.12.2010 je premietnutý v nasledujúcej tabuľke :

Text	Rozpis rozpočtu v €	Upravený rozpočet v €	Čerpanie v €	% plnenia	
				ku schvál. rozpočtu	k uprav. rozpočtu
I. Príjmy kapitoly					
A. Záväzný ukazovateľ	38 000	36 238	36 570,39	96,24	100,92
B. Prostriedky z rozpočtu EÚ	0				
II. Výdavky kapitoly spolu (A + B)	8 800 101	8 532 239	8 528 648,74	96,92	99,96
A. Výdavky spolu bez prostriedkov z rozpočtu EÚ (600+700)	8 800 101	8 532 239	8 528 648,74	96,92	99,96
Z toho :					
A.1. prostriedky na spolufinancovanie	0	0	0	0	0
A.2.mzdy, platy, služ. príj. a ost. os. vyrovnania (610), (kód zdroja 111)	4 817 968	4 628 968	4 628 834,14	96,07	99,99
z toho:mzdy, platy, sl. príjmy a ost. os. vyrovnania aparátu ústredného orgánu	4 817 968	4 628 968	4 628 834,14	96,07	99,99
Počet zamestnancov podľa príl. č. 1 k uzneseniu vlády SR č. 692/2009	268 osôb	268 osôb	*227 osôb	88,43	88,43
A.3. kapitálové výdavky (700) (bez prostriedkov na spolufinancovanie)	49 970	305 117	301 965,36	604,29	98,97
Z toho :					
Kód zdroja 111	49 970	305 117	301 965,36	604,29	98,97
B. Prostriedky z rozpočtu EÚ	0	0	0	0	0
C. Účelové prostriedky	8 800 101	8 532 239	8 528 648,74	96,92	99,96
D. Rozpočet kapitoly podľa Programov „ 085 – Bezpečnosť informácií	8 800 101	8 532 239	8 528 648,74	96,92	99,96
E. Systemizácia policajtov v štátnej službe :					
objem finančných prostriedkov na služ. príjmy v štátnej službe	4 557 350	4 385 350	4 385 301,74	96,22	99,99
počet miest spolu	232 osôb	232 osôb	*199 osôb	90,09	90,09

* uvádzaný je evidenčný počet zamestnancov k 31.12.2010

Záväzné ukazovatele štátneho rozpočtu kapitoly 41 – Národný bezpečnostný úrad boli dodržané.

Rozpočtované príjmy Národného bezpečnostného úradu boli prekročené o 332,39 € oproti upravenému rozpočtu. Prekročenie príjmov je spôsobené nepredvídaným príjmom na položke 220 - za certifikáciu produktu pre zaručený elektronický podpis vo výške 331,50 eur.

V rámci výdavkovej časti rozpočtu nedošlo k prekročeniu výdavkov vo vzťahu k upravenému rozpočtu. Vecné vymedzenie čerpania bežných výdavkov a kapitálových výdavkov je uvedené v časti 1.3.1. Výdavky kapitoly podľa ekonomickej klasifikácie.

Rozpočtované finančné prostriedky boli použité na krytie nevyhnutných potrieb a opatrení vyplývajúcich z osobitných predpisov. Pri používaní finančných prostriedkov bola zachovaná hospodárnosť, efektívnosť a účinnosť ich použitia.

V rámci uzatvárania zmluvných vzťahov sa Národný bezpečnostný úrad nezaviazal v hodnotenom rozpočtovom roku na také úhrady, ktoré nemal zabezpečené v rozpočte hodnoteného rozpočtového roka, a ktoré by zaťažili rozpočet pridelený Národnému bezpečnostnému úradu v nasledujúcich rozpočtových rokoch z dôvodu nedostatku zdrojov v hodnotenom rozpočtovom roku.

1.2. Príjmy

Rozpisom záväzných ukazovateľov rozpočtu na rok 2010 bol pre kapitolu 41 – Národný bezpečnostný úrad stanovený limit pre plnenie príjmovej časti rozpočtu vo výške 38 000 €. Upravený rozpočet : 36 238 €.

K 31.12.2010 príjmy za kapitolu Národný bezpečnostný úrad predstavujú čiastku 36 570,39 €.

1.2. Výdavky

Výdavky Národného bezpečnostného úradu za rok 2010 predstavovali čiastku 8 528 648,74 €, t. z. 99,96 % k upravenému rozpočtu 8 532 239,00 €.

V priebehu roka 2010 v nadväznosti na nedostatok kapitálových finančných prostriedkov bola čiastka 255 147,00 € presunutá z bežných výdavkov do kapitálových výdavkov. Presunuté finančné prostriedky boli použité na obstaranie technologického vybavenia pre obranu na informačné a komunikačné systémy, výmenu riadiacich a zaznamenávacích zariadení v kamerovom systéme NBÚ, výmenu klimatizácie v serverovniach, kúpu osciloskopu a upgrade informačného systému previerka.

V rámci bežných výdavkov došlo k viazaniu rozpočtových prostriedkov v celkovej čiastke 267 862,00 € (RO MF SR č. 3 a č. 5 – časť 1.1.3. Rozpočtové opatrenia).

1.3.1. Výdavky podľa ekonomickej klasifikácie

600 – Bežné výdavky

upravený rozpočet : 8 227 122,00 €

čerpanie : 8 226 683,38 €

Čerpanie v hlavnej kategórii 600 – Bežné výdavky predstavuje k 31.12.2010 čiastku 8 226 683,38 € z upraveného rozpočtu 8 227 122,00 € (99,99 %). Zostatok nevyčerpaných finančných prostriedkov vo výške 438,62 € (630 – Tovary a služby 126,46 €, 640 – Bežné transfery 312,16 €) bol odvedený do štátneho rozpočtu.

Z účtu cudzích prostriedkov na príjmový účet organizácie bola odvedená suma 1 314,80 € (610 – Mzdy, platy služobné príjmy a ostatné osobné vyrovnania 133,86 €, 620 – Poistné a príspevok do poisťovní 991,24 €, 640 – Bežné transfery 189,70 €)

700 – Kapitálové výdavky

upravený rozpočet : 305 117,00 €

čerpanie : 301 965,36 €

Celkový limit kapitálových výdavkov bol po realizácii rozpočtových opatrení stanovený vo výške 305 117,00 €. Všetky kapitálové výdavky boli realizované v rámci položky 710 – Obstarávanie kapitálových aktív. Čerpanie k 31.12.2010 bolo v sume 301 965,36 €, čo je 98,97 % k upravenému rozpočtu. Zostatok nevyčerpaných finančných prostriedkov vo výške 3 151,64 € bol odvedený do štátneho rozpočtu.

1.3.3. Vyhodnotenie plnenia programovej štruktúry

Celkové čerpanie z upraveného rozpočtu v čiastke 8 532 239,00 € roku 2010 k 31.12.2010 predstavuje sumu 8 528 648,74 € (99,96 %), z toho hlavná kategória 600 – Bežné výdavky 8 226 683,38 € (99,99 % z upraveného rozpočtu 8 227 122,00 €) a hlavná kategória 700 – Kapitálové výdavky 301 965,36 € (98,97 % z upraveného rozpočtu 305 117,00 €).

V roku 2010 Národný bezpečnostný úrad mal v rámci programového rozpočtovania otvorený program 085 – Bezpečnosť informácií a bol účastníkom medzirezortného programu 06G – Ľudské zdroje, podprogram 06G0T – Aktívna politika trhu práce a zvýšenie zamestnanosti – NBÚ, prvok 06G0T01 Stimulovanie a skvalitňovanie celoživotného vzdelávania pre potreby zamestnávateľov a podnikateľského sektora – NBÚ (ukončený v roku 2008).

Výdavky kapitoly na programe 085 – Bezpečnosť informácií celkom :

Por. č.	Kód programu	Názov programu	Skutočnosť 2009	Schválený 2010 eur	Upravený 2010 eur	Skutočnosť 2010 eur	% čerpania	
							ku schvál. rozpočtu	k uprav. rozpočtu
A	085	<i>Bezpečnosť informácií</i>	8 690 037,78	8 800 101,00	8 532 239,00	8 528 648,74	96,92	99,96
a)	08501	Riadenie a podpora programov	4 049 034,37	4 731 999,00	3 689 704,70	3 720 467,19	78,62	100,83
b)	08502	Ochrana utajovaných skutočností	1 702 535,73	1 590 191,00	1 773 706,73	1 808 834,20	113,75	101,98
1.	0850201	Bezpečnostné previerky	1 136 190,79	1 095 228,00	1 238 183,87	1 250 434,88	114,17	100,99
2.	0850202	Ochrana objektov a informácií	566 344,94	494 963,00	535 522,86	558 399,32	112,82	104,27
c)	08503	Bezp. kom. a informačných systémov	1 814 926,75	1 554 543,00	2 049 458,54	1 967 192,05	126,54	95,99
d)	08504	Elektronický podpis	1 123 540,93	923 368,00	1 019 369,03	1 032 155,30	111,78	101,25

Faktory ovplyvňujúce vývoj čerpania rozpočtu a plnenie rozpočtových zámerov

Celkové čerpanie upraveného rozpočtu v čiastke 8 532 239,00 € roku 2010 k 31.12.2010 predstavuje čiastku 8 528 648,74 € (99,96 % upraveného rozpočtu), z toho hlavná kategória 600 – Bežné výdavky 8 226 683,38 € (99,99 % upraveného rozpočtu 8 227 122,00 €) a hlavná kategória 700 – Kapitálové výdavky 301 965,36 € (98,97 % upraveného rozpočtu 305 117,00 €).

V roku 2010 mal NBÚ v rámci programového rozpočtovania otvorený program 085 – Bezpečnosť informácií a v rámci medzirezortného programu otvorený podprogram 06G0T Aktívna politika trhu práce a zvýšenie zamestnateľnosti – NBÚ, prvok 06G0T01 – Stimulovanie a skvalitňovanie vzdelávania pre potreby zamestnávateľov a podnikateľského sektora – NBÚ.

Čerpanie finančných prostriedkov podľa programov (v EUR):

Kód programu	Zdroj	Názov programu Kód zdroja	Schválený rozpočet	Upravený rozpočet	Skutočnosť	% čerp.	
						ku schv. rozp.	k upr. rozp.
085	111	Bezpečnosť informácií	8 800 101,00	8 532 239,00	8 528 648,74	96,92	99,96
		Bežné výdavky	8 750 131,00	8 227 122,00	8 226 683,38	94,01	99,99
		Kapitálové výdavky	49 970,00	305 117,00	301 965,36	604,29	98,97
08501		Riadenie a podpora programov	4 731 999,00	3 689 704,70	3 720 467,19	78,62	100,83
		Bežné výdavky	4 682 029,00	3 585 192,70	3 616 763,12	77,25	100,88
		Kapitálové výdavky	49 970,00	104 512,00	103 704,07	207,53	99,23
08502		Ochrana utajovaných skutočností	1 590 191,00	1 773 706,73	1 808 834,20	113,75	101,98
		Bežné výdavky	1 095 228,00	1 238 183,87	1 250 434,88	114,17	100,99
		Kapitálové výdavky	0,00	0,00	0,00	-	-
0850201		Bezpečnostné previerky	1 095 228,00	1 238 183,87	1 250 434,88	114,17	100,99
		Bežné výdavky	1 095 228,00	1 238 183,87	1 250 434,88	114,17	100,99
		Kapitálové výdavky	0,00	0,00	0,00	-	-
0850202		Ochrana objektov a informácií	494 963,00	535 522,86	558 399,32	112,82	104,27
		Bežné výdavky	494 963,00	535 522,86	558 399,32	112,82	104,27
		Kapitálové výdavky	0,00	0,00	0,00	-	-
08503		Bezpečnosť informačných a komunikačných systémov	1 554 543,00	2 049 458,54	1 967 192,05	126,54	95,99
		Bežné výdavky	1 554 543,00	1 848 853,54	1 768 930,76	113,79	95,68
		Kapitálové výdavky	0,00	200 605,00	198 261,29	-	98,83
08504		Elektronický podpis	923 368,00	1 019 369,03	1 032 155,30	111,78	101,25
		Bežné výdavky	923 368,00	1 019 369,03	1 032 155,30	111,78	101,25
		Kapitálové výdavky	0,00	0,00	0,00	-	-

06G0T		Aktívna politika trhu práce a zvýšenie zamestnanosti – NBÚ	0,00	0,00	0,00	-	-
-------	--	--	------	------	------	---	---

Zámer a ciele programu 085 – Bezpečnosť informácií

Zámer : Optimálne podmienky bezpečnosti ochrany utajovaných skutočností a elektronického podpisu dát

Ciel' 1 :

Urýchliť vybavovanie prijatých žiadostí o vykonanie previerok personálnej bezpečnosti

Monitorovanie cieľa:

Na základe porovnania plánovaného počtu dní na vykonanie bezpečnostnej previerky pre príslušný stupeň utajenia a skutočného počtu dní možno konštatovať, že plnenie cieľa je za hodnotené obdobie úspešné.

V porovnaní s plánom bolo v hodnotenom období prijatých o 331 žiadostí menej. Z 3669 žiadostí o vykonanie previerky personálnej bezpečnosti prijatých v hodnotenom období bolo ukončených 3421 bezpečnostných previerok osôb.

Formulácia cieľa je v súlade s platnou legislatívou, pričom sleduje zámer programu zabezpečiť optimálne podmienky bezpečnosti ochrany utajovaných skutočností tým, že vykonávaním bezpečnostných previerok osôb, ako jedným z predpokladov na vznik oprávnenia oboznamovať sa s utajovanými skutočnosťami, v čo najkratších lehotách, umožňuje zabezpečenie ochrany utajovaných skutočností na požadovanej úrovni dostatočným počtom oprávnených osôb.

Komentár:

Analýzou a porovnaním údajov za predchádzajúce obdobia možno konštatovať, že dosiahnutý priemerný počet dní na vykonanie bezpečnostnej previerky klesol tak, že jeho ďalšie znižovanie v budúcnosti by pri súčasnej snahe o dodržanie kvalitatívnych požiadaviek na vykonávanie bezpečnostných previerok osôb nebolo efektívne, preto sledovanie uvedených ukazovateľov v budúcnosti stráca opodstatnenie.

K sledovaniu ukazovateľa počtu vybavených žiadostí možno konštatovať, že tento je priamo úmerný k počtu doručených žiadostí, pričom úrad nemôže ovplyvniť počet doručených žiadostí o vykonanie bezpečnostnej previerky. Počet žiadostí o vykonanie bezpečnostných previerok osôb je priamo závislý od potreby oboznamovania sa s utajovanými skutočnosťami stanovenej najmä vedúcimi v jednotlivých štátnych orgánoch, obciach a u podnikateľov, a od počtu osôb ktorým v hodnotenom a nasledovnom období uplynie doba platnosti osvedčenia (PT 5 rokov, T 7 rokov a D 10 rokov) za predpokladu, že tieto osoby budú aj naďalej vykonávať funkcie určené vedúcim na oboznamovanie sa s utajovanými skutočnosťami, a teda budú potrebovať platné osvedčenie.

Gestor: Sekcia previerok, odbor personálnej bezpečnosti

Ciel' 2 :

Vykonávať certifikáciu prostriedkov a systémov šifrovej ochrany informácií v zmysle stanovených ukazovateľov

Monitorovanie cieľa : Cieľ bol splnený

Komentár :

- a) relevantnosť - povinnosť certifikovať PŠOI vyplýva NBÚ zo zákona, doba certifikácie nie je stanovená.
- b) efektívnosť - mierou efektívnosti je potvrdenie resp. verifikovanie parametrov predložených PŠOI na certifikáciu a prípadné odhalenie ich slabín. Časové kritérium v takomto prípade je sekundárne.
- c) účinnosť - vplyv na cieľovú skupinu – žiadateľov o certifikát je z hľadiska NBÚ nepodstatný.
- d) dosah/vplyv - sledovanie tohto cieľa pre NBÚ nemá praktický význam, nesystémové urýchľovanie certifikácie môže vyvolať nežiaduci efekt zdania uprednostňovania jednej firmy pred druhou.
- e) udržateľnosť - udržateľnosť cieľa je diskutabilná, najmä ak nemôžeme ovplyvniť jeden zo sledovaných parametrov. Výpovedná hodnota dĺžky trvania certifikácie na 1 PŠOI je minimálna, pretože nič nevypovedá o miere zložitosti v korelácii jednotlivých prostriedkov. Preto navrhujeme tento cieľ zrušiť, resp. nesledovať.

Gestor : Sekcia informačnej bezpečnosti a elektronického podpisu

Ciel' 3 :

Vytvoriť podmienky pre bezpečné používanie elektronického podpisu

Monitorovanie cieľa :

Plnenie cieľa v rámci podprogramu 08504 – Elektronický podpis, má oporu v zákone č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov (ďalej len „zákon“) a plnenie vychádza so záväzkov SR voči EÚ a NATO.

Súčasťou činností spojených s certifikačnými činnosťami je vytváranie podmienok pre bezpečné používanie elektronického podpisu. Na vytváranie zaručeného elektronického podpisu je potrebné mať certifikované technologické zariadenia a programové vybavenie. Taktiež elektronický podpis sa implementuje do informačných systémov, ktoré prevádzkuje NBÚ v rámci svojich interných informačných systémov (napr. registratúra, elektronická podateľňa, atď.) a informačných systémov medzirezortného charakteru (napr. IS silové rezorty). Pri prevádzke týchto informačných systémov je potrebné realizovať činnosti pri ich správe, udržiavaní v prevádzky schopnom stave a rozširovať ich podľa koncepcných zámerov.

Stanovený cieľ „Vytvoriť podmienky pre bezpečné používanie elektronického podpisu“ je plne aktuálny a prispôsobený skutočným potrebám, ktoré vychádzajú z požiadaviek kladených na NBÚ a sú v súlade so zákonom. Cieľ je dlhodobý a výsledkom jeho plnenia je funkčnosť a práca najmä nasledovných informačných technológií:

- koreňovej certifikačnej autority Slovenskej republiky (KCA),
- akreditovanej certifikačnej autority SNCA,
- poskytovania akreditovanej služby časovej pečiatky,
- poskytovania certifikačných služieb pre systém „Pasy SR“,
- elektronickej podateľne úradu.

- Potreba realizácie cieľa je v súlade so súčasnými potrebami a kapacitami úradu. Ich aktuálnosť bola premietnutá aj v rámci hlavných úloh úradu pre rok 2010.

Každá jedna úloha má jasne stanoveného gestora zodpovedného za jej plnenie a vždy začiatkom roka je stanovený, schválený časový harmonogram a termín realizácie. List úlohy obsahuje najmä:

- cieľ úlohy,
- plán postupu,
- výstupy úlohy,
- tím riešiteľov a spoluriešiteľov,
- príjemcov,
- potrebné disponibilné finančné zdroje
- súlad úlohy s politikou a koncepčným zameraním úradu so zreteľom na synergické hľadisko zámeru.

Plnením jednotlivých úloh bude zabezpečená ochrana elektronického podpisu na požadovanej úrovni v zmysle zákona s nasadením dostatočného počtu kompetentných pracovníkov a to tak, aby cieľ bol splnený v súlade so stanoveným harmonogramom, prípadne v čo možno najkratšom termíne pri súčasnom dodržaní kvalitatívnych požiadaviek.

Stav plnenia: K 31.12.2010 boli všetky stanovené úlohy splnené.

Plnenie cieľa je hodnotené ako efektívne a hospodárne.

Cieľ nebude efektívne dosiahnuteľný s menším počtom pracovníkov a znížením mzdových finančných prostriedkov. V prípade zníženia počtu pracovníkov by muselo prísť k ukončeniu činností, nakoľko by neboli splnené požiadavky na vydanie pozitívnej auditnej správy v zmysle zákona, alebo by muselo prísť k zadávaniu prác a realizácií vykonávania pravidelných servisných činností dodávateľským spôsobom. V tomto prípade by bola finančná úhrada neúmerne vyššia ako sú náklady v súčasnosti.

Zameranie cieľa je podmienené zákonom a cieľová skupina používateľov je zložená z užívateľov mimo NBÚ (verejnosť, podnikateľské prostredie, vybrané zložky štátnej správy, EÚ a NATO) a pracovníkov úradu. Plnenie tohto cieľa má zásadný vplyv na cieľovú skupinu. V prípade nedostupnosti služieb príde k ochromeniu a nedostupnosti certifikačných služieb v rámci Slovenskej republiky.

Komentár : Činnosti sa vykonávajú podľa harmonogramu stanoveného pre rok 2010.

Gestor : Sekcia informačnej bezpečnosti a elektronického podpisu

Cieľ 4 :

Vytvoriť podmienky pre ochranu kybernetického priestoru

Monitorovanie cieľa:

Vytvorenie podmienok pre ochranu kybernetického priestoru je proces, ktorý predstavuje akúsi úvodnú úlohu (štartovací cieľ) pre samotný nosný cieľ „Ochrana kybernetického priestoru v podmienkach SR“. Nosný a iné podporné súvisiace ciele postupne nahradia súčasný cieľ. Vytváranie podmienok je vo svojej podstate zložitý proces zložený z vytvárania vhodných technických, organizačných a legislatívnych podmienok.

Technický rámec zahŕňa vybudovanie:

- technického laboratória,
- centra reakcie na bezpečnostné incidenty - SK CSIRC,
- systému Apeiron - medzirezortného systému, ktorý zahŕňa vybrané rezorty.
- NSUI - nosnej siete na prenos utajovaných informácií

Organizačný rámec zahŕňa najmä:

- vytvorenie riadiaceho orgánu ochrany kybernetického priestoru SR,
- vytvorenie výkonného orgánu ochrany kybernetického priestoru,
- odborná príprava príslušníkov

Legislatívny rámec zahŕňa úpravu legislatívnych pravidiel (úprava zákonov, vyhlášok a interných pravidiel).

a) relevantnosť

S vývojom technológií žiaľ narastá aj svetový kybernetický terorizmus a počítačová kriminalita. Preto aj SR má ako jeden zo svojich cieľov ochranu kybernetického priestoru, ktorým bol ako gestor poverený úrad. Z tohto pohľadu identifikované potreby a ciele korešpondujú s cieľmi a zámermi danej úlohy. Vzhľadom na skúsenosti iných krajín s kybernetickou kriminalitou a kybernetickým terorizmom (Estónsko, Litva, Barma, Gruzínsko) identifikované potreby znásobujú relevantnosť danej úlohy.

b) efektívnosť a hospodárnosť

Aby bolo možné hodnotiť efektívnosť a hospodárnosť je potrebné sa pozerieť na proces vytvárania podmienok pre ochranu kybernetického priestoru ako na proces prípravy. Nosnou líniou tejto prípravy je úspešné absolvovanie medzinárodného cvičenia NCDEX 2010. Napriek počiatocnému zaostávaniu priebežného plnenia ukazovateľa v priebehu roka za hodnotené obdobie možno konštatovať že cieľ bol splnený v plnom rozsahu. Systém Apeiron bol spustený do prevádzky. V oblasti organizačnej sa postupovalo podľa plánovaných aktivít. Príslušníci absolvovali naplánované školenia, príprava na cvičenie NCDEX 2010 a samotné cvičenie prebehlo úspešne. V tejto oblasti, hlavne vo svetle úloh vyplývajúcich z bežnej prevádzky SK CSIRC sa ukázalo ako nedostatočné personálne obsadenie. Oblasť legislatívna je zameraná na vytváranie vhodného legislatívneho prostredia. V roku 2010 bol spracovaný návrh nového zákona o ochrane US a jeho samostatná časť o ochrane kybernetického priestoru.

c) účinnosť

Účinky dosiahnutých výsledkov na cieľovú skupinu možno premietnuť do schopnosti úspešného absolvovania cvičenia NCDEX 2010. V tejto skutočnosti je v technickej a organizačnej oblasti jasne definovaná cieľová skupina. Legislatívna oblasť má vplyv na celú SR.

d) dosah/vplyv

Sledovaný cieľ má jednoznačne pozitívny vplyv na sledovanú cieľovú skupinu. Užitočnosť a dôsledky realizácie badať na rozvíjajúcej sa spolupráci rôznych zložiek (skupín), ktoré majú v oblasti kybernetickej ochrany v SR rozhodujúci vplyv.

e) udržateľnosť

Účelom tohto cieľa je vytvorenie podmienok na dlhodobú, resp. trvalú ochranu kybernetického priestoru. Je možné predpokladať časový harmonogram ukončenia sledovaného cieľa, nie je ho však možné presne určiť. Jednoznačne je však možné povedať, že nie je potrebné až 100% plnenie, aby bolo možné spustiť nosný cieľ, ktorým je ochrana kybernetického priestoru.

Gestor : Sekcia informačnej bezpečnosti a elektronického podpisu

08501 – Riadenie a podpora programov

Zámer : Kvalitne fungujúce podporné útvary

Cieľ 1 :

Každoročne plniť úlohy pri zabezpečovaní činnosti úradu

Monitorovanie cieľa :

Kritérium relevantnosti :

Stanovený cieľ v rámci podprogramu 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 svojim 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, napríklad pri príprave kontroly ochrany utajovaných skutočností sa plán kontroly zohľadňuje vopred, na základe vykonaných analýz kontrolovaného subjektu a identifikovaných problémov. Taktiež v ročných plánoch kontrol sa ponecháva rezerva personálnych a časových kapacít tak, aby bolo možné vykonať operatívne kontroly na základe zistenej aktuálnej potreby, resp. vonkajšieho podnetu.

Potreby podmieňujúce existenciu podprogramu v nadväznosti na stanovený cieľ stále pretrvávajú. Aby odborné útvary dosahovali kvalitné plnenie svojich úloh v súlade so stanoveným časovým harmonogramom prác, je potrebné zabezpečiť a zosúladiť materiálne, technické, finančné, legislatívne, organizačné, personálne, bezpečnostné a kontrolné aktivity.

Efektívnosť a hospodárnosť :

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. Aj napriek prijatiu úsporných opatrení a minimalizovaniu výdavkov boli úlohy plnené v požadovanej kvalite a v požadovanom rozsahu pri súčasnom dodržaní finančnej disciplíny. K miernemu zvýšeniu čerpania finančných prostriedkov došlo v súvislosti

s vykonávaním operatívnych vonkajších kontrol ochrany utajovaných skutočností, ktoré bolo potrebné vykonať na krajských súdoch v celej Slovenskej republike. Uvedené aktivity boli vykonané efektívne a hospodárne, ich výsledkom je kvalitatívne zlepšenie úrovne ochrany utajovaných skutočností na úrovni krajských súdov a v celom rezorte ministerstva spravodlivosti.

Účinnosť :

V rámci zabezpečovania činnosti Národného bezpečnostného úradu podporné útvary plnili svoje úlohy na požadovanej úrovni. Za hodnotené obdobie boli vypracované odborné stanoviská k predkladaným návrhom právnych predpisov, a to nielen na úrovni vnútrorezortného pripomienkového konania, ale aj na úrovni medzirezortného pripomienkového konania, ako aj k návrhom predpisov NATO a EÚ. Uvedené stanoviská výrazne prispeli ku skvalitneniu práce odborných útvarov.

Veľmi pozitívny vplyv na činnosť odborných útvarov úradu, a v oblasti ochrany utajovaných skutočností smerom navonok mali aj výstupy z vnútorných a vonkajších kontrol. Upozorňovaním na vzniknuté nedostatky a následným prijatím adekvátnych opatrení sa môže v budúcnosti predchádzať opakovaniu nedostatkov v činnosti úradu. Už v súčasnom období je viditeľný kvalitatívny skok v úrovni zabezpečenia ochrany utajovaných skutočností v štátnych orgánoch a organizáciách, ako aj u podnikateľov, čo možno pripísať aj vplyvu metodických funkcií doposiaľ vykonaných vonkajších kontrol zo strany NBÚ.

Na plynulosti a kvalitnom plnení úloh odborných útvarov sa vo významnej miere podieľala včasná a správna koordinácia zahraničných aktivít úradu, plynulé organizačné zabezpečovanie prípravy medzirezortných rokovaní, podpisovania dohôd a dokumentov ako aj materiálne, technické a finančné zabezpečenie činností úradu.

Cieľavedomým plánovaním jednotlivých aktivít - vytváranie plánu hlavných úloh úradu a základných opatrení, ako je napríklad plánovanie zahraničných služobných ciest, verejné obstarávanie, systém riadenia kontroly a i. sa dosiahol významný pokrok pri dosahovaní plnenia zámeru a cieľa tohto podprogramu. Rovnaký prístup bol použitý aj pri výbere príslušníkov a zamestnancov úradu a ich odbornom vzdelávaní.

V rámci sledovaného obdobia boli jednotlivé úlohy zabezpečované podpornými útvarmi v súlade so stanoveným plánom úloh.

Dosah/vplyv :

Plnenie úloh podporných útvarov má vplyv nielen na samotnú cieľovú skupinu (odborné útvary), ale tento vplyv sa rozširuje aj mimo tejto cieľovej skupiny. Napríklad vykonávanie kontrol a na ich základe prijímanie adekvátnych opatrení, ktoré sú následne zapracovávané odbornými útvarmi do vyhlášok a metodických usmernení, majú významný vplyv na zlepšenie a skvalitnenie práce ostatných rezortov resp. podnikateľských subjektov v oblasti ochrany utajovaných skutočností. Činnosť kancelárie úradu v oblasti medzinárodnej spolupráce, negociácie a prípravy medzinárodných dohôd zasahuje aj mimo úrad, tzn. ovplyvňuje prácu ostatných rezortov resp. podnikateľských subjektov. Bol odštartovaný projekt zameraný na budovanie bezpečnostného povedomia a vzdelávania v oblasti ochrany utajovaných skutočností.

Udržateľnosť :

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.

Napríklad už vyššie spomínaný efekt „výchovnej“ funkcie vykonaných vonkajších kontrol ochrany utajovaných skutočností priebežne zvyšuje ochranu utajovaných skutočností vo všetkých oblastiach bezpečnosti. Jedná sa najmä o „vynútené“ dobudovanie chránených priestorov a certifikovaných technických prostriedkov, ale na druhej strane aj kvalitatívny odborný rast vedomostnej úrovne zodpovedných pracovníkov a s tým súvisiace znižovanie početnosti chýb v zabezpečení ochrany utajovaných skutočností. V súčasnosti nie je predpoklad, že by na udržanie dosiahnutých výsledkov boli potrebné dodatočné finančné zdroje. Do úvahy prichádza skôr možnosť rozšírenia niektorých podporných útvarov o kvalifikovanú pracovnú silu, čo ale je možné riešiť personálnymi kapacitami v rámci úradu.

Gestor : Sekcia ekonomiky

08502 – Ochrana utajovaných skutočností

0850201 – Bezpečnostné previerky

Cieľ 1 :

V roku 2010 začať realizáciu 95 % bezpečnostných previerok z počtu žiadostí prijatých v danom roku

Monitorovanie cieľa:

Odbor personálnej bezpečnosti sekcie previerok z 3669 prijatých žiadostí o vykonanie bezpečnostnej previerky navrhovanej osoby začal v hodnotenom období realizovať 3669 bezpečnostných previerok.

Odbor priemyselnej bezpečnosti sekcie previerok z prijatých 85 žiadostí o vydanie potvrdenia o priemyselnej bezpečnosti podnikateľa začal v hodnotenom období realizovať 85 bezpečnostných previerok.

Stanovený cieľ bol splnený.

Formulácia cieľa sleduje zámer programu, aby bola zabezpečená ochrana utajovaných skutočností na požadovanej úrovni dostatočným počtom oprávnených osôb, aby boli bezpečnostné previerky fyzických osôb a právnických osôb vykonávané v čo najkratších možných lehotách. Plnenie cieľa pozitívne vplýva na vytváranie vhodných podmienok v oblasti personálnej bezpečnosti a priemyselnej bezpečnosti ako jedných zo základných podmienok pre zabezpečenie ochrany utajovaných skutočností.

Vzhľadom na zmeny v procese vykonávania bezpečnostných previerok, napríklad implementácia nového informačného systému ako podporného prostriedku v oblasti bezpečnostných previerok a digitalizácia potrebných informácií) počty prijatých žiadostí o vykonanie bezpečnostných previerok príslušného stupňa utajenia a skrátenie lehôt na vykonávanie bezpečnostných previerok v hodnotenom období, sa nám javí potrebné v budúcnosti upraviť formuláciu cieľa.

Gestor: Sekcia previerok, odbor personálnej bezpečnosti

Ciel' 2:

V roku 2010 vykonať overovanie podmienok priemyselnej bezpečnosti u 21 podnikateľských subjektov

Monitorovanie cieľa:

Príjemcovia cieľa sú podnikatelia, ktorí majú platné potvrdenie o priemyselnej bezpečnosti podnikateľa. Zodpovednosť za realizáciu cieľa sú definované tak, aby bolo zrejmé, ktorá časť útvaru vykonáva čiastkové činnosti, a ktorá spracúva výsledný materiál s dopadom na overovanie podmienok priemyselnej bezpečnosti. Počas hodnoteného obdobia boli dosahované čiastkové hodnoty tak, aby bol na konci sledovaného obdobia dosiahnutý stanovený cieľ. Vykonávaná činnosť má vplyv na ochranu utajovaných skutočností, nakoľko kontinuálne sleduje plnenie podmienok priemyselnej bezpečnosti zo strany podnikateľov s platným potvrdením o priemyselnej bezpečnosti. Cieľ je v súčasnej dobe udržateľný.

Gestor: Sekcia previerok, odbor priemyselnej bezpečnosti

Ciel' 3 :

V roku 2010 ukončiť 55% bezpečnostných previerok z počtu žiadostí prijatých v danom roku

Monitorovanie cieľa:

Od 1.1.2010 do 31.12.2010 prijal odbor personálnej bezpečnosti sekcie previerok 3669 žiadostí o vykonanie previerky personálnej bezpečnosti, z ktorých bolo v hodnotenom období 3421 ukončených, t.j. 93%.

Odbor priemyselnej bezpečnosti sekcie previerok v období od 1.1.2010 do 31.12.2010 prijal 85 žiadostí o vydanie potvrdenia o priemyselnej bezpečnosti, z ktorých bolo v hodnotenom období 64 ukončených, t.j. 75%.

Spolu bolo prijatých 3754 žiadostí a z týchto bolo ukončených 3485 bezpečnostných previerok.

Formulácia cieľa je v súlade s platnou legislatívou, pričom sleduje zámer programu, aby bola zabezpečená ochrana utajovaných skutočností v štátnych orgánoch a u podnikateľov na požadovanej úrovni dostatočným počtom oprávnených osôb, a tým minimalizované riziko postúpenia utajovaných skutočností osobám alebo podnikateľom, ktorých bezpečnostná spoľahlivosť nebola posúdená podľa príslušných právnych predpisov. Cieľovými skupinami sú navrhované osoby a podnikatelia. Stanovený cieľ sleduje v hodnotenom období ukončiť čo najväčší počet bezpečnostných previerok osôb a podnikateľov z počtu doručených žiadostí tak, aby boli bezpečnostné previerky vykonávané kvalitne a v čo najkratších lehotách.

Komentár:

Vyššie percento ukončených bezpečnostných previerok v hodnotenom období je ovplyvnené najmä nižším počtom prijatých žiadostí a prevažujúcim počtom žiadostí o vykonanie bezpečnostných previerok personálnej bezpečnosti s kratšími lehotami na ich vykonanie.

Počas hodnoteného obdobia boli dosahované čiastkové hodnoty, a na konci sledovaného obdobia dosiahnutý stanovený cieľ, pričom výška percenta v jednotlivých hodnotených obdobiach bola ovplyvňovaná najmä zákonom stanovenými lehotami na rozhodnutie o bezpečnostnej previerke navrhovanej osoby (pri bezpečnostnej previerke II. stupňa do 3 mesiacov od začatia konania, pri bezpečnostnej previerke III. stupňa do 4 mesiacov od začatia konania, pri bezpečnostnej previerke IV. stupňa do 6 mesiacov od začatia konania, a ak nebolo možné vzhľadom na povahu veci rozhodnúť

v uvedených lehotách mohol úrad lehotu predĺžiť o tri mesiace) a zákonom stanovenými lehotami na rozhodnutie o bezpečnostnej previerke podnikateľa (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 nebolo možné vzhľadom na povahu veci rozhodnúť v uvedených lehotách mohol úrad lehotu predĺžiť o tri mesiace).

Vzhľadom na zmeny podmienok najmä počty prijatých žiadostí o vykonanie bezpečnostných previerok príslušného stupňa utajenia oproti plánovaným počtom, skrátenie lehôt na vykonávanie bezpečnostných previerok v hodnotenom období sa nám javí potrebné v budúcnosti upraviť formuláciu cieľa.

Gestor: Sekcia previerok, odbor personálnej bezpečnosti

Cieľ 4 :

V roku 2010 vydať 85 % potvrdení o absolvovaní skúšky bezpečnostného zamestnanca z celkového počtu preskúšaných bezpečnostných zamestnancov, na základe požiadaviek vedúcich ústredných orgánov štátnej správy, štátnych orgánov, právnických osôb a obcí

Cieľ: splnený

Aktivity na dosiahnutie cieľa

Od 1.1.2010 do 31.12. 2010 bolo prijatých na úrad celkom 214 žiadostí o vykonanie skúšky bezpečnostného zamestnanca (ďalej len „žiadost“). Z uvedeného počtu bolo 180 žiadostí od vedúcich orgánov štátnej správy a 34 žiadostí od vedúcich právnickej osoby – podnikateľa. Z celkového počtu prijatých žiadostí sa 5 osôb skúšky bezpečnostného zamestnanca (ďalej len „skúška BZ“) nezúčastnilo; k 1 osobe žiadost' o vykonanie skúšky BZ stiahol späť vedúci; k 1 osobe vykonanie skúšky BZ zastavil úrad na základe zistenia, že osoba v čase prijatia žiadosti do termínu vykonania skúšky BZ nespĺňala predpoklad na výkon funkcie bezpečnostného zamestnanca podľa § 9 ods. 1 zákona 215/2004 Z. z. (nemala platné osvedčenie úradu na oboznamovanie sa s utajovanými skutočnosťami); 12 osôb je pozvaných na vykonanie skúšky BZ v mesiaci január 2011. Celkom bolo vybavených 202 žiadostí o skúšku BZ.

Skúšku BZ absolvovalo celkom 195 účastníkov, z toho 194 účastníkov s hodnotením „prospeľ“ a 1 s hodnotením „neprospel“. Všetci účastníci skúšky BZ mali ku dňu vykonania skúšky platné osvedčenie úradu na oboznamovanie sa s utajovanými skutočnosťami. Skúšky BZ boli vykonávané počas hodnoteného obdobia priebežne v 42 termínoch.

Z celkového počtu 195 preskúšaných osôb, na základe požiadaviek vedúcich ústredných orgánov štátnej správy, štátnych orgánov, právnických osôb a obcí, vydal úrad za sledované obdobie celkom 194 potvrdení o absolvovaní skúšky BZ, čo je 99,49 %.

Monitorovanie cieľa :

- odskúšaním bezpečnostných zamestnancov sa nedá ovplyvniť percento úspešnosti, cieľ je vhodnejšie monitorovať z ohľadu prípravy (školení) osôb žiadajúcich o skúšku BZ, kde sa dá % úspešnosti čiastočne ovplyvňovať.

Kritérium relevantnosti :

Zámerom programu sú optimálne podmienky bezpečnosti OUS. Od roku 2004 je % vydaných potvrdení o absolvovaní skúšky blížiac sa ku 100 %. Zámer sa dosiahne, ak sa % úspešnosti zachová, ale kvalitnou prípravou bezpečnostných zamestnancov.

Efektívnosť a hospodárnosť:

Kvantitatívne ukazovatele pre vyhodnotenie plnenia cieľa neexistujú. V roku 2010 boli pripravené podmienky na prechod kompletných evidencií súvisiacich so skúškami bezpečnostných zamestnancov do IS Previerka. Skúšky bezpečnostných zamestnancov zabezpečujú dvaja pracovníci odboru kontroly, pričom tieto činnosti vykonávajú popri plnení iných hlavných úloh.

Účinnosť :

Plnenie cieľa tak, ako je naformulovaný teraz, je na cieľovú skupinu neúčinný. O účinnosti bude možné hovoriť, ak bude cieľ zameraný na prípravu bezpečnostných zamestnancov na vykonanie skúšky.

Dosah/vplyv :

Podobne ako pri účinnosti.

Udržateľnosť :

Po zmene cieľa tak, aby bolo jeho ťažisko v príprave bezpečnostných zamestnancov bude tento udržateľný aj do budúcnosti a jeho sledovanie prinesie kladné výkyvy.

Gestor : Odbor kontroly

0850202 – Ochrana objektov a informácií

Cieľ 1 :

V roku 2010 vybaviť 90 % žiadostí z celkového počtu žiadostí o vydanie certifikátu mechanických zábranných prostriedkov alebo technických zabezpečovacích prostriedkov prijatých v danom roku

Monitorovanie cieľa:

Zhodnotenie dosiahnutých výsledkov:

<i>Certifikačná činnosť 01.01.2010 – 31.12.2010</i>	<i>Počet prijatých žiadostí</i>	<i>Počet vybavených žiadostí</i>	<i>Percento všetkých vybavených žiadostí</i>
Žiadosti o certifikáciu typu prostriedku	53	53	-
Žiadosti o certifikáciu jednotlivého prostriedku	6	6	-
SPOLU	59	59	100 %

Relevantnosť:

Zámer programu „Vytváranie optimálnych podmienok na zabezpečenie ochrany utajovaných skutočností a elektronického prenosu dát“ úzko súvisí s bezpečnosťou SR, čím je previazaný s ochranou utajovaných informácií, vytvára priestor na zamedzenie ich neoprávnenej manipulácie a na zabezpečovanie ochrany pred ich možným únikom. So zámerom programu súvisia hlavné úlohy NBÚ, na ktorých sa podieľa OFEB SIBEP v komplexnom systéme určovania pravidiel a podmienok na zabezpečovanie fyzickej a objektovej bezpečnosti objektov a chránených priestorov, určených na

ukladanie a manipuláciu s utajovanými skutočnosťami. Cieľ č. 1 podprogramu 0850202-Ochrana objektov a informácií bol stanovený v nadväznosti na zámer programu tak, aby všetky činnosti vykonávané pri dosahovaní cieľa smerovali k jeho napĺňaniu a priamo tak vytvárali podmienky na zabezpečenie ochrany US. Fyzická a objektová bezpečnosť (ďalej len „FOB“) predstavuje systém opatrení, ktorými sa zabezpečujú US pred prístupom nepovolaných osôb a zároveň sa umožňuje prístup k US oprávneným osobám. Účinnými opatreniami FOB sa identifikujú pokusy o vstup narušiteľa a eliminujú sa bezpečnostné narušenia. FOB sa dosahuje okrem dôslednej realizácie režimových opatrení a fyzickej ochrany i aplikovaním mechanických zábranných prostriedkov a technických zabezpečovacích prostriedkov, ktoré podstatne zvyšujú bezpečnosť ochrany US.

Cieľ je indikovaný nosným merateľným ukazovateľom výstupu, čo predstavuje percento vybavených žiadostí, teda množstvo výstupu, t.j. 100 % žiadostí z celkového počtu žiadostí prijatých v roku 2010. Žiadosť sa považuje za vybavenú dňom vydania certifikátu typu alebo certifikátu jednotlivého prostriedku. Údaje v stanovenom ciele a merateľnom ukazovateli sú získavané z interných ľahko dostupných zdrojov, napr. z evidencie doručených žiadostí o certifikáciu MZP a TZP, z posudzovania záverečných protokolov, zo štatistickej evidencie vydaných certifikátov. Ako externý zdroj získavania relevantných údajov uvádzame vykonávanie skúšok MZP a TZP prostredníctvom autorizovaných osôb NBÚ, ktoré na základe žiadostí o certifikáciu výrobku vykonávajú ich overovanie podľa platných noriem a v súlade so zákonom a vykonávacími vyhláškami.

Z analýzy výskytu možných nedostatkov, hlavne pri hodnotení vhodne či nevhodne stanoveného cieľa vyplýva, že náš cieľ je stručný, konkrétny, zrozumiteľný, je ľahko merateľný a kvantifikovateľný vhodným merateľným ukazovateľom výsledku a obsahuje konkrétnu očakávanú cieľovú hodnotu, ktorou je 90 % vybavených žiadostí o certifikáciu, z celkového počtu prijatých žiadostí od 01.01.2010 do 31.12.2010, voči ktorej porovnáваме dosiahnutú skutočnosť, t.j. 100 % vybavených žiadostí. Požiadavky kladené legislatívou a potreby podmieňujúce existenciu daného cieľa sú stále aktuálne a žiaduce.

Efektívnosť:

Pri určovaní primeraných a efektívnych opatrení gestor vychádzal z hodnotenia rizika možného ohrozenia US, ktoré sa určuje po zhodnutí stupňa utajenia US, množstva a formy US, úrovne osvedčenia personálu a zhodnotením ohrozenia US vonkajšími a vnútornými vplyvmi. Gestor navrhol zmeny v legislatíve z dôvodu zvýšenia efektivity a optimalizácie ochrany US v oblasti certifikácie MZP a TZP napríklad v určovaní doby platnosti certifikátu, v overovaní kvality výroby u certifikovaných MZP a TZP počas platnosti certifikátu typu, v určovaní podmienok použitia MZP a TZP, vo vymedzení podmienok na zrušenie certifikátu, v podmienkach žiadosti o vydanie súhlasu s autorizáciou podnikateľa.

V rámci pravidelného prehodnocovania plánu činností a finančného plánu v hodnotenom období boli optimalizované nepriame náklady (podpoložka ekonomickej klasifikácie 633009, 637001, 637004) na zber a spracovanie údajov a znížilo sa čerpanie bežných výdavkov oproti predchádzajúcim rokom. Aj napriek prijatiu úsporných opatrení a minimalizovaní výdavkov (najlepšia kvalita/najnižšia cena) boli úlohy plnené na požadovanej kvantitatívnej i kvalitatívnej úrovni.

Neopomenuteľným vývinovým aspektom v sledovanej oblasti je rýchly rozvoj nových technológií a inovácií MZP/TZP, čo predpokladá pravidelné získavanie nových informácií, či už formou účasti na medzinárodných a európskych konferenciách, seminároch či veľtrhoch alebo výstavách bezpečnostného priemyslu. Taktiež zadávanie odborných štúdií a posudkov má svoje opodstatnenie. V rámci analýzy efektívnosti vykonávania všetkých činností potrebných na dosiahnutie

cieľa je nutné ponechať počet zamestnancov, ktorí sa podieľajú na plnení nosných úloh odboru a súčasne riešia i časovo náročné rozvojové úlohy. Predpokladané rozvojové úlohy za oblasť fyzickej bezpečnosti a objektovej bezpečnosti je možné rozdeliť do dvoch oblastí:

- a) akustická bezpečnosť,
- b) integrované systémy TZP.

a) K únikom utajovaných informácií počas rokovania môže dôjsť aj prostredníctvom pasívneho alebo aktívneho odpočúvania. Akustická bezpečnosť by mala viesť k zabráneniu týchto únikov. V tejto oblasti by bolo potrebné zakúpiť technické vybavenie na výkon technických bezpečnostných prehliadok a spracovať štúdiu, v ktorej sa určia akustické požiadavky na rokovaciu miestnosť. Náklady na uvedené technické vybavenie sa pohybujú v rozmedzí 115 tis. až 272 tis. € a náklady na spracovanie štúdie je možné odhadnúť na 15 tis. eur.

b) Technické zabezpečovacie prostriedky podliehajú certifikácii v zmysle zákona č. 215/2004 Z. z. V poslednej dobe sa začínajú vo väčšej miere využívať integrované systémy TZP. Tieto systémy zlučujú jednotlivé technické zabezpečovacie prostriedky do jedného systému. Z uvedeného dôvodu sa javí ako potrebné certifikovať aj integrované systémy TZP. Pre splnenie tejto rozvojovej úlohy je nutné spracovať štúdiu, ktorej obsahom bude najmenej analýza, rozdelenie a požiadavky na integrované systémy TZP. Na základe štúdie bude možné rozhodnúť o spracovaní skúšobného postupu. Náklady na štúdiu možno odhadnúť na 20 tis. €.

Z tohto pohľadu by bolo preto žiaduce v budúcich rokoch navýšiť rozpočet gestora.

Účinnosť:

V rámci zabezpečovania úloh vedúcich k plneniu cieľa boli vykonávané nasledovné činnosti:

- kontrola doručených žiadostí z pohľadu plnenia požiadaviek zákona a vyhlášok,
- evidencia doručených žiadostí o vydanie certifikátu typu a certifikátu jednotlivého prostriedku,
- posudzovanie záverečných protokolov a vypracovanie odborného stanoviska,
- schvaľovací proces vydania príslušného certifikátu typu a certifikátu jednotlivého prostriedku,
- realizácia vydávania certifikátov typu a certifikátov jednotlivého prostriedku,
- štatistická evidencia vydaných certifikátov typu a certifikátov jednotlivého prostriedku,
- zverejňovanie údajov o vydaných certifikátoch typu na internetovej stránke úradu,
- monitorovanie platnosti vydaných certifikátov typu MZP a TZP,
- evidencia certifikátov typu, ktorým skončila ich platnosť,
- zverejňovanie metodických pokynov a usmernení za oblasť certifikácie a autorizácie na internetovej stránke úradu,
- vykonávanie dohľadu nad autorizovanými osobami NBÚ,
- legislatívna, autorizačná, metodická, kontrolná a analytická činnosť SOFB NBÚ,
- štúdium odbornej literatúry a účasť na školeniach, kurzoch a konferenciách s úzko špecializovanou problematikou FOB.

V roku 2004 a 2005 bolo stanovené plánované percento merateľného ukazovateľa cieľa vo výške 70, t.z. bol predpoklad, že z celkového počtu prijatých žiadostí o vydanie certifikátu bude minimálne 70 % kladne vybavených žiadostí, t.z. vydaných certifikátov MZP a TZP. Skutočný počet vydaných certifikátov však výrazne prevyšoval plán, a preto bolo v ďalšom období zvýšené percento merateľného ukazovateľa cieľa - od roku 2006 na 90 % a od roku 2007 až na 95 %. V roku 2009 bol plán zvýšený na 96 %. Po detailnejšej analýze vyhodnocovania cieľa sme dospeli k názoru, že v prípade, ak na úrad bude doručený vyšší počet žiadostí o certifikáciu MZP a TZP v krátkom časovom období (cca 1 – 5 dní) pred plánovaným hodnotením cieľa, výrazne sa tým môže znížiť percento

skutočného vybavenia predmetných žiadostí, a teda môže dôjsť k nespĺneniu cieľa, pričom požiadavky zákona sú dodržané. Z tohto dôvodu plánovaný ukazovateľ cieľa klesá, i keď sa výrazne skutočnosť nemení. Počas hodnoteného obdobia boli dosahované cieľové hodnoty a pokrok bol zabezpečovaný dôsledným plánovaním a pravidelným monitorovaním všetkých čiastkových činností smerujúcich k plneniu cieľa.

Dosah/vplyv:

Pri zhodnotení výsledkov realizácie cieľa na spoločnosť ako celok uvádzame, že plnenie cieľa je závislé od platnej legislatívy, štandardov a noriem platných v oblasti certifikácie, autorizácie. Plnenie úloh a súvisiace činnosti sú pretransformované do zadaného cieľa, ktorého výsledky v značnej miere skvalitňujú ochranu objektov a chránených priestorov určených na ukladanie a manipuláciu s utajovanými skutočnosťami. Znižujú sa hrozby, ktoré môžu vytvoriť bezpečnostné riziko, pričom sa eliminujú riziká neoprávnených manipulácií s US. Užitočnosť programu je priamo úmerná jeho relevantnosti, ktorá je daná vzájomnou súvislosťou priorít vlády a vychádza predovšetkým z dodržiavania požiadaviek zákona. Plnenie úloh sa realizuje v kooperácii s opatreniami informačnej bezpečnosti, administratívnej bezpečnosti a personálnej bezpečnosti.

Udržateľnosť

Udržateľnosť cieľa úzko súvisí so stabilitou a účinkom celého programu a je závislá na realizácii častí podprogramov, na plnení jednotlivých cieľov, na perspektívnosti pôsobenia pozitívnych zmien. Pozitívne zmeny vo výstupovom ciele sú charakterizované cez kvantitu, kvalitu a efektívnosť. Kvalitu cieľa odráža spokojnosť žiadateľov, ktorí sa stávajú držiteľmi certifikátov MZP a TZP, ktoré potvrdzujú spôsobilosť MZP/TZP chrániť US požadovaného stupňa utajenia. Kvantitu cieľa predstavuje množstvo vydaných certifikátov, teda počet vybavených žiadostí o certifikáciu typu a jednotlivého prostriedku MZP alebo TZP, pretransformovaných do výsledku merateľného ukazovateľa cieľa, čo je za hodnotené obdobie až 100 %.

Na základe uvedeného konštatujeme, že podprogram 08502 Ochrana utajovaných skutočností je stabilný a udržateľný, čo je garantované plnením požiadaviek zákona a nastavenými prioritami vlády. V súčasnosti nie je predpoklad, že by sa tieto kladné zmeny stali v krátkom časovom horizonte zastarané a neudržateľné.

Gestor : Sekcia informačnej bezpečnosti a elektronického podpisu, Odbor objektovej a fyzickej bezpečnosti

Cieľ 2 :

V roku 2010 zaevidovať v elektronickej evidencii 85 % utajovaných písomností vymieňaných v rámci medzinárodnej spolupráce

V roku 2010 bolo plánovaných zaevidovať v rámci medzinárodnej spolupráce 85% došlých utajovaných skutočností v elektronickej evidencii. Dosiahnuté výsledky v období od 1.1.2010 do 31.12.2010 zabezpečili plnenie zámeru programu, nakoľko v tomto období bolo zaevidovaných na centrálnom registri gestora v elektronickej evidencii 95% utajovaných skutočností došlých v rámci medzinárodnej spolupráce.

Monitorovanie cieľa :

V hodnotenom období boli zaevidované na centrálnom registri v elektronickej evidencii utajované skutočnosti NATO a EÚ prijaté v rámci medzinárodnej spolupráce, čo predstavuje 95 %-nú evidenciu. Stanovený cieľ vystihuje zámer programu a dosiahnuté výsledky zabezpečujú jeho

plnenie. Plán evidencie utajovaných skutočností v elektronickej evidencii je postavený v súlade s jej možnosťami. V elektronickej evidencii utajovaných písomností na CR je možné evidovať len utajované písomnosti NATO a EÚ. Došlé utajované písomnosti vymieňané v rámci medzinárodnej spolupráce ostatných zahraničných subjektov sú doposiaľ evidované v bežných protokoloch utajovaných písomností. Skutočnosť, že je plnenie cieľa od roku 2004 vyššie ako bolo plánované závisí od počtu všetkých doručených utajovaných písomností na centrálny register. Z uvedeného vyplýva, že ak by sme chceli dosiahnuť 100%-né plnenie cieľa, bolo by potrebné zabezpečiť elektronickej evidencii pre všetky došlé utajované písomnosti vymieňané v rámci medzinárodnej spolupráce, čo je ekonomicky neefektívne. Neefektívnosť vidíme v tom, že náklady na zavedenie elektronickej evidencie utajovaných písomností sú vysoké v pomere na malé množstvo utajovaných písomností zahraničných subjektov. Tento cieľ je do budúcnosti plne udržateľný vychádzajúc z § 33 ods. 1 vyhlášky NBÚ č. 453/2007 Z. z. o administratívnej bezpečnosti.

Komentár : V období od 1.1.2010 do 31.12.2010 dosiahnutý výsledok v plnení cieľa zabezpečil plnenie zámeru programu v porovnaní s plánovaným počtom o 10%-né prekročenie stanoveného cieľa.

Gestor : Kancelária NBÚ, odbor administratívnej bezpečnosti a centrálného registra

Cieľ 3 :

V roku 2010 vykonať v sídle podnikateľa na základe doručených žiadostí o vydanie potvrdenia o priemyselnej bezpečnosti pre postúpenie a vznik utajovaných skutočností, zisťovanie podmienok administratívnej bezpečnosti u 70 % podnikateľov

V roku 2010 bolo plánované vykonať v sídle podnikateľa na základe doručených žiadostí o vydanie potvrdenia o priemyselnej bezpečnosti pre postúpenie a vznik utajovaných skutočností a zisťovanie podmienok administratívnej bezpečnosti u 70% podnikateľov. Dosiahnuté výsledky v období od 1.1.2010 do 31.12.2010 zabezpečili plnenie zámeru programu na 78%.

Monitorovanie cieľa :

V hodnotenom období bolo na OABCR doručených 42 žiadostí na posúdenie bezpečnostných smerníc podnikateľa týkajúcich sa oblasti administratívnej bezpečnosti. Príslušníci OABCR vykonali u 33 podnikateľov zisťovanie podmienok administratívnej bezpečnosti v sídle podnikateľa. Cieľom je zabezpečiť ochranu utajovaných skutočností a zistiť podmienky administratívnej bezpečnosti u podnikateľov na základe žiadostí o vydanie potvrdenia o priemyselnej bezpečnosti. Fyzicky vykonaná previerka umožňuje zistiť prípadné nedostatky, metodicky usmerniť oprávnené osoby u jednotlivých subjektov. Percento plnenia závisí od časového harmonogramu odboru priemyselnej bezpečnosti sekcie previerok, nakoľko zisťovanie podmienok podnikateľa pre vydanie potvrdenia o priemyselnej bezpečnosti je vykonávané v súčinnosti s inými útvarmi úradu a je viazané na spoločné termíny výjazdov. Plnenie cieľa má pozitívny vplyv na žiadateľov o vydanie potvrdenia, čo sa výrazne prejaví zvýšením úrovne ochrany utajovaných skutočností a v oveľa menších nedostatkoch pri kontrolách vykonávaných odborom kontroly. Zároveň je predpoklad, že u podnikateľov nebude dochádzať k neoprávnenej manipulácii.

Komentár : V období od 1.1.2010 do 31.12.2010 bol cieľ podprogramu splnený na 78% a vyhodnotený z reálneho počtu doručených žiadostí na posúdenie bezpečnostných smerníc podnikateľa týkajúcich sa oblasti administratívnej bezpečnosti a z reálneho počtu zisťovania podmienok administratívnej bezpečnosti u podnikateľa.

Gestor : Kancelária NBÚ, odbor administratívnej bezpečnosti a centrálného registra

Ciel' 4 :

V roku 2010 vykonať metodické školenia pracovníkov registrov utajovaných skutočností na 90% zriadených registrov

V roku 2010 bolo plánované vykonať 90% metodických školení na registroch utajovaných skutočností. Dosiahnuté výsledky v období od 1.1.2010 do 31.12.2010 priebežne zabezpečujú plnenie zámeru programu. V sledovanom období bolo vykonané plnenie na 100%.

Monitorovanie cieľa :

V hodnotenom období bolo vykonané metodické školenie na 26 registroch, čo predstavuje 100% z celkového počtu zriadených registrov. Zámerom podprogramu je zabezpečiť, aby pracovníci registrov utajovaných skutočností boli pravidelne metodicky preškolení v súlade s § 36 ods. 5 vyhlášky NBÚ č. 453/2007 Z. z. o administratívnej bezpečnosti a medzinárodnými dokumentmi EÚ a NATO. Vykonávanie metodických školení má výrazný vplyv na lepšiu kvalitu práce týchto pracovníkov, lepšie pochopenie problematiky a významný pokrok pri manipulácii s utajovanými písomnosťami.

Komentár : V období od 1.1.2010 do 31.12.2010 dosiahnutý výsledok v plnení cieľa zabezpečil plnenie zámeru programu na 100%.

Gestor : Kancelária NBÚ, odbor administratívnej bezpečnosti a centrálného registra

Ciel' 5 :

V roku 2010 ukončiť 80 % bezpečnostných previerok fyzickej bezpečnosti a objektovej bezpečnosti podnikateľa z celkového počtu žiadostí o vyjadrenie k spôsobilosti zabezpečiť ochranu utajovaných skutočností z hľadiska fyzickej bezpečnosti a objektovej bezpečnosti prijatých v danom roku

Monitorovanie cieľa:

Zhodnotenie dosiahnutých výsledkov:

<i>Previerková činnosť k 31.12.2010</i>	<i>Počet prijatých žiadostí</i>	<i>Počet vybavených žiadostí</i>	<i>Percento všetkých vybavených žiadostí</i>
Žiadosti o posúdenie bezpečnostnej dokumentácie v oblasti FOB	52	42	81 %

Relevantnosť:

Plnenie cieľa č. 5 prebieha v súlade so zákonom č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov, v súlade s vyhláškou NBÚ č. 314/2006 Z. z., ktorou sa mení a dopĺňa vyhláška NBÚ č. 337/2004 Z. z., ktorou sa upravujú podrobnosti o certifikácii mechanických zábranných a technických zabezpečovacích prostriedkov a o ich používaní, v súlade s vyhláškou NBÚ č. 336/2004 Z. z. o fyzickej bezpečnosti a objektovej bezpečnosti v znení vyhlášky NBÚ č. 315/2006 Z. z.

Nosné úlohy sú pretransformované do jednotlivých činností oddelenia fyzickej a objektovej bezpečnosti v rámci úloh, ktoré vedú k plneniu daného cieľa. Nakoľko sa tento cieľ sleduje len druhý rok, analýza počiatočného a skutočného stavu a hodnotenie pokroku by neboli efektívne a relevantné.

Cieľ sleduje predovšetkým zabezpečovanie ochrany US z pohľadu fyzickej a objektovej bezpečnosti (ďalej len „FOB“). FOB sa dosahuje komplexným súborom opatrení (režimových,

aplikáciou MZP/TZP v objektoch a chránených priestoroch) pomocou ktorých sa vytvára funkčný, efektívny a z hľadiska finančnej náročnosti optimálny systém ochrany US, ktorý podporuje zámer programu. Účinnými opatreniami FOB sa identifikujú pokusy o vstup narušiteľa a eliminujú sa bezpečnostné narušenia. Konkrétne požiadavky ohodnotenia úrovne FOB sú uvedené v bezpečnostnom štandarde FOB, ktorý je prílohou k vyhláške č. 336/2004 Z. z. o fyzickej bezpečnosti a objektovej bezpečnosti v znení vyhlášky NBÚ č. 315/2006 Z. z.

Cieľ je indikovaný nosným merateľným ukazovateľom výstupu, čo predstavuje percento ukončených bezpečnostných previerok z hľadiska fyzickej bezpečnosti a objektovej bezpečnosti prijatých a vybavovaných v danom roku, teda množstvo výstupu, t.j. 81 % ukončených bezpečnostných previerok. Údaje v stanovených cieľoch a merateľných ukazovateľoch sú získavané z interných a externých zdrojov, napr. z osobitnej evidencie doručených žiadostí, zo štatistickej evidencie bezpečnostných previerok, z realizácie vykonávania bezpečnostných previerok a overovania plnenia požiadaviek zákona na ochranu US priamo u podnikateľa alebo štátneho orgánu v súlade s vykonávacími vyhláškami a metodickými pokynmi.

Efektívnosť:

V rámci efektívnosti plnenia cieľa sme optimalizovali nepriame náklady (podpoložka ekonomickej klasifikácie 633009, 637001, 637004) na zber a spracovanie údajov v rámci pravidelného prehodnocovania plánu činností odboru a finančného plánu v hodnotenom období a znížili čerpanie bežných výdavkov oproti predchádzajúcemu roku. Napriek prijatiu úsporných opatrení a minimalizovaní výdavkov (najlepšia kvalita/najnižšia cena) sú úlohy plnené na požadovanej kvantitatívnej a kvalitatívnej úrovni. Zníženie nákladov na plnenie cieľa nemá k hodnotenému obdobiu vplyv na dodržiavanie časového harmonogramu činností vedúcich k cieľu.

Účinnosť:

V rámci zabezpečovania úloh vedúcich k plneniu cieľa boli vykonávané nasledovné činnosti:

- evidencia doručených žiadostí o zaslanie záverečného stanoviska o spôsobilosti podnikateľov zabezpečovať ochranu utajovaných skutočností v oblasti fyzickej bezpečnosti a objektovej bezpečnosti,
- posudzovanie bezpečnostnej dokumentácie chránených priestorov z pohľadu fyzickej bezpečnosti a objektovej bezpečnosti,
- realizácia overovania zabezpečenia chránených priestorov v mieste podnikateľa alebo štátneho orgánu, vypracovanie správy z previerky,
- vyjadrenie oddelenia fyzickej a objektovej bezpečnosti k zabezpečeniu chránených priestorov, vypracovanie záverečného stanoviska,
- štatistická evidencia previerkovej činnosti,
- zverejňovanie metodických pokynov a usmernení na internetovej stránke úradu,
- legislatívna, autorizačná, metodická, kontrolná a analytická činnosť oddelenia fyzickej a objektovej bezpečnosti,
- štúdium odbornej literatúry a účasť na školeniach, kurzoch a konferenciách s úzko špecializovanou problematikou FOB.

Počas hodnoteného obdobia boli cieľové hodnoty dosahované.

Dosah/vplyv:

Plnenie úloh odboru má vplyv na samotnú cieľovú skupinu, ktorou sú podnikatelia i štátne orgány a realizuje sa v kooperácii s opatreniami informačnej bezpečnosti, administratívnej bezpečnosti a personálnej bezpečnosti.

Udržateľnosť:

Pri spracovávaní podkladov k programovej štruktúre na roky 2011-2013 sme navrhli cieľ zrušiť, nakoľko nejde o závažnú zmenu programu a zrušenie cieľa nebude mať žiadny vplyv na štruktúru programu a plnenie jeho zámeru.

Gestor : Sekcia informačnej bezpečnosti a elektronického podpisu

Cieľ 6 :

V roku 2010 na základe doručených žiadostí o metodické usmernenie vykonať u 80 % štátnych orgánov a právnických osôb metodické usmernenia

V roku 2010 bolo plánované vykonať 80% metodických usmernení u štátnych orgánov a právnických osôb na základe doručených žiadostí o metodické usmernenie. Dosiadnuté výsledky v období od 1.1.2010 do 31.12.2010 priebežne zabezpečujú plnenie zámeru programu na 100%. Stanovený cieľ vystihuje zámer programu 085.

Monitorovanie cieľa :

V hodnotenom období bolo na odbor administratívnej bezpečnosti a centrálného registra doručených 19 písomných žiadostí o metodické usmernenie. V hodnotenom období bol cieľ splnený, metodické usmernenia boli vykonávané písomne aj fyzicky v sídle subjektu podľa požiadaviek a v závislosti od problematiky. Zámerom je dosiahnutie maximálnej kvality práce pri manipulácii s utajovanými písomnosťami. Na základe metodík predpokladáme menšiu chybovosť pri vedení protokolov utajovaných písomností a pri evidenciách v administratívnych pomôckach. Cieľ bude plne udržateľný do budúcnosti, nakoľko gestor pripravuje novú vyhlášku o administratívnej bezpečnosti.

Komentár : V období od 1.1.2010 do 31.12.2010 dosiahnutý výsledok v plnení cieľa zabezpečil plnenie zámeru programu na 100%.

Gestor : Kancelária NBÚ, odbor administratívnej bezpečnosti a centrálného registra

08503 – Bezpečnosť komunikačných a informačných systémov

Cieľ 1:

Zvýšenie spoľahlivosti a funkčnosti integrovaného komunikačného systému pre ústavných a vládnych činiteľov; v roku 2010 znížiť celkový počet porúch a výpadkov na maximálny počet 220

Monitorovanie cieľa :

Chybovosť systému sa pohybuje v predpokladaných hodnotách vzhľadom na veľkosť a zložitosť komunikačného systému

Komentár :

a) relevantnosť – zámerom programu je naplniť uznesenie vlády SR č.173/2003. Trend naznačuje, že systém, ktorý bol projektovaný v roku 2003 a realizovaný v priebehu roka 2004 má svoju životnosť a vzhľadom na prudký pokrok v informatike je už morálne zastaralý a v priebehu 1-2 rokov bude i fyzicky opotrebovaný, najmä ak by sa vyžadovali dodatočne určité funkcionality príp. upgrade. V neposlednom rade treba si uvedomiť, že objektívny parameter sledovaný u zariadení resp. u veľkých systémov t.j. doba medzi jednotlivými poruchami sa skraca. Inak povedané, staršie zariadenia a systémy vykazujú objektívne väčšiu chybovosť/poruchovosť.

b) efektívnosť - vzhľadom na uvedené je možnosť merania efektivity daná dostupnosťou požadovanej služby/služieb. V tomto prípade parameter nedostupnosti služby sa nedá vyhodnotiť ako štatisticky významný. Porovnávať efektívnosť väčším alebo menším počtom pracovníkov nemá výpovednú hodnotu, pretože špecializovanú činnosť len na tento program nevykonáva žiadny konkrétny pracovník, pretože predmet pracovných činností pracovníkov je koncipovaný v širšom rámci.

c) účinnosť - vzhľadom na vynakladané finančné prostriedky, ktoré sú smerované výlučne do servisu a opráv považujeme činiteľ účinnosti za viac ako dostatočný.

d) dosah/vplyv – realizáciou uznesenia vlády je daná možnosť bezpečnej komunikácie pre určených ústavných a vládnych predstaviteľov, ktorej garantom je v zmysle zákona

e) udržateľnosť – v zmysle uvedeného je dlhodobá udržateľnosť cieľa podmienená zvýšeným úsilím garanta, poruchovosť sa môže objektívne zvyšovať ale nepredpokladáme fatálny kolaps systému. Riešením problému (nie cieľa) je vybudovanie NSUI.

Gestor : Sekcia informačnej bezpečnosti a elektronického podpisu

Cieľ 2 :

Výskum a vývoj nových prostriedkov šifrovej ochrany informácií; v roku 2010 vyvinúť 1 prostriedok šifrovej ochrany informácií

Monitorovanie cieľa :

Na výskume a vývoji nových PŠOI prebiehajú práce v zmysle Projektu výskumu a vývoja v oblasti kryptológie a prostriedkov ŠOI na roky 2009-2011.

Komentár :

a) relevantnosť – vývojom národných PŠOI sa sleduje zníženie resp. odstránenie závislosti na importe zahraničných PŠOI, a tým zníženie finančných nákladov. V neposlednom rade sa garantuje kryptografická bezpečnosť, čo je parameter relevantný pre národnú bezpečnosť, najmä pre vyššie stupne utajenia

b) efektívnosť - vzhľadom na možnosti SR v tejto oblasti (personálne, firemné, legislatívne) je proces nastavený optimálne, akékoľvek nesystémové a nepredvídateľné zásahy budú mať za následok rozpad riešiteľského tímu a dočasný koniec tejto činnosti v SR

c) účinnosť - zabezpečená implementáciou vyvinutých PŠOI do prevádzky v rezortoch, ani jeden PŠOI nebol vyvíjaný samoučelne

d) dosah/vplyv – dosahom tejto úlohy je cca 70% používanie národných (vyvinutých) PŠOI v podmienkach SR. Ak túto skutočnosť premietneme na finančnú stránku, tak prichádza k 30% až 50% úspore finančných prostriedkov pri predpokladanom nákupe porovnateľných zahraničných PŠOI. Nezanedbateľný nie je ani sociálny dopad na zamestnanosť, odvody, vedomostnú ekonomiku a skutočnosť, že finančné prostriedky ostávajú v SR.

e) udržateľnosť – systém je veľmi citlivý na vonkajšie vplyvy a má veľa rizikových faktorov od čoho sa odvíja aj jeho udržateľnosť.

Gestor : Sekcia informačnej bezpečnosti a elektronického podpisu

Cieľ 3:

Certifikácia prostriedkov šifrovej ochrany informácií; v roku 2010 certifikovať 5 prostriedkov ŠOI

Monitorovanie cieľa :

Cieľ sa splnil, certifikácia sa vykonala podľa plánu.

Komentár :

a) relevantnosť – zámerom programu je naplniť ustanovenia zákona

b) efektívnosť - vzhľadom na náročnosť činnosti a dosahované výsledky a snahu o čo najvyššiu kvalitu je dosahovaná efektívnosť na hranici možností.

c) účinnosť - ako je z tabuľky zrejmé plánované počty môžu byť prekročené z istých dôvodov (2009), jednak sa môže jednať o recertifikáciu, keď sa overujú parametre predtým schválené v predošlom certifikáte, alebo sa jedná o prevzatie zahraničných certifikátov. Pri štandardnom certifikačnom procese je počet limitovaný.

d) dosah/vplyv – certifikačný proces je proces overenia deklarovaných parametrov PŠOI a tým garancie bezpečnosti prenášaných informácií, ktoré sú významné pre štátne záujmy a v neposlednom rade aj národnú bezpečnosť

e) udržateľnosť – otázka na potrebnosť certifikácie je otázkou na nutnosť bezpečnosti štátu a zmysluplnosti zákona

Gestor : Sekcia informačnej bezpečnosti a elektronického podpisu

Cieľ 4:

Certifikácia technických prostriedkov potrebných na ochranu utajovaných skutočností; v roku 2010 vydať 78% certifikátov z celkového počtu podaných žiadostí v priebehu roka spĺňajúcich požiadavky zákona a vyhlášky

Monitorovanie cieľa:

Relevantnosť - dosiahnuté výsledky zabezpečujú plnenie úlohy vyplývajúcej zo zákona č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov - ochranu utajovaných skutočností, spracovávaných na technických prostriedkoch. Merateľný ukazovateľ - percentuálne vyjadrenie vydaných certifikátov z počtu prijatých žiadostí o vykonanie certifikácie technických prostriedkov odráža plnenie cieľa.

Efektívnosť a hospodárnosť - sú primerané vo vzťahu k výsledkom. Je dodržiavaný časový harmonogram dosahovania uvedeného cieľa s rovnakým počtom príslušníkov počas celej doby hodnotenia plnenia ukazovateľa.

Účinnosť - v roku 2010 bolo prijatých celkom 182 žiadostí o vykonanie certifikácie technických prostriedkov. Z celkového počtu spĺňalo formálne aj obsahové náležitosti (resp. tieto boli postupne doplnené na základe nášho vyžiadania) 176 žiadostí. Proces certifikácie technických prostriedkov bol ukončený vydaním certifikátu v 165 prípadoch, čo predstavuje plnenie ukazovateľa na 93,7 %.

Dosah / vplyv - realizáciou cieľa je zo strany NBÚ kladený čoraz väčší dôraz na potreby ochrany utajovaných skutočností, spracovávaných na technických prostriedkoch v štátnych orgánoch a v podnikateľskej sfére.

Udržateľnosť - certifikácia technických prostriedkov je proces trvalý. Tento proces je podmienený morálnym starnutím technických prostriedkov (hardvérovým a softvérovým), technickým a technologickým vývojom, obmedzením doby platnosti certifikátov technických prostriedkov.

Gestor : Sekcia informačnej bezpečnosti a elektronického podpisu

Cieľ 5 :

Kategorizácia technických prostriedkov (TP), prostriedkov ŠOI a priestorov, v ktorých budú tieto prostriedky umiestnené, z hľadiska ochrany pred nežiaducim elektromagnetickým vyžarovaním; v roku 2010 kategorizovať z hľadiska ochrany pred nežiaducim elektromagnetickým vyžarovaním 200 TP, prostriedkov ŠOI a priestorov

Monitorovanie cieľa :

Relevantnosť:

Zámerom cieľa 5 podprogramu 08503 Bezpečnosť komunikačných a informačných systémov je vytváranie podmienok pre plnenie jednej zo základných požiadaviek zákona č. 215/2004 Z. z. o ochrane utajovaných skutočností na bezpečnosť technických prostriedkov a prostriedkov ŠOI, na ktorých sa tvoria, spracovávajú, prenášajú alebo ukladajú utajované skutočnosti, a to kategorizácia technických prostriedkov, prostriedkov ŠOI a priestorov z hľadiska ochrany pred nežiaducim elektromagnetickým vyžarovaním. Cieľovou skupinou v rámci plnenia zámeru podprogramu (cieľa) sú žiadatelia, t.j. orgány verejnej moci alebo podnikatelia, ktorí ukladajú a manipulujú s utajovanými skutočnosťami stupňa utajenia dôverné, tajné a prísne tajné na technických prostriedkoch, a majú povinnosť zabezpečiť ich proti neoprávnenej manipulácii.

V rámci jednotlivých meraní sa posudzuje úroveň nežiaduceho elektromagnetického vyžarovania zariadenia (technického prostriedku alebo prostriedku ŠOI) a úroveň elektromagnetického útľmu priestoru. Činnosti, ktoré vedú k plneniu cieľa sú zároveň činnosťami, bez ktorých nie je možné dospieť k naplneniu zámeru celého programu NBÚ. Ide hlavne o skúšky zariadení v špecializovanom laboratóriu a merania priestorov mobilnou meracou aparátúrou. Výstupom plnenia cieľa sú stanoviská z meraní, ktoré sú k podkladom k certifikácii technických prostriedkov a prostriedkov ŠOI. Posúdenie z pohľadu ochrany pred nežiaducim elektromagnetickým vyžarovaním je možné iba meraniami pomocou špeciálnej meracej techniky. Počet 220 kategorizovaných technických prostriedkov a priestorov z hľadiska ochrany pred nežiaducim elektromagnetickým vyžarovaním predstavuje konkrétne definovateľné merania technických prostriedkov, prostriedkov ŠOI a priestorov za obdobie roka 2010.

Celý proces meraní NEV je náročný, ako z pohľadu prípravy merania, tak aj samotného priebehu a vyhodnotenia nameraných hodnôt. Základom pre získanie relevantných výsledkov je vykonávanie zónových meraní priestorov, meraní prostriedkov ŠOI a meraní technických prostriedkov podľa normy SDIP 27.

Efektívnosť a hospodárnosť:

Laboratórium TEMPEST nie je v súčasnosti stále dobudované. Je potreba navýšiť rozpočet o ďalšie finančné prostriedky na zakúpenie príslušnej meracej techniky, na jej údržbu a obmenu, pravidelnú kalibráciu a na špeciálne školenia príslušníkov OFEB SIBEP NBÚ. Ide hlavne o zakúpenie meracej aparatury k zónovým meraniam priestorov (75.000 €) a softvéru na čiastočnú automatizáciu meraní NEV zariadení (50.000 €).

Účinnosť:

Počas hodnoteného obdobia boli cieľové hodnoty dosahované. Cieľ je sledovaný od roku 2007 kedy bol stanovený plán merateľného ukazovateľa cieľa v hodnote 100, čo značí, že v roku 2007 bolo uskutočnených spolu 100 meraní technických prostriedkov, prostriedkov šifrovej ochrany informácií a priestorov. Plán meraní bol v roku 2007 prekročený o vyše 100 %. V nasledujúcom roku bol stanovený plán na vyšší počet 150 meraní ročne, ktorý bol opätovne prekročený o vyše 9 %. Po analýze plánu a skutočného stavu meraní za uplynulé roky, sme na roky 2009, 2010 zvýšili plán na 200 meraní ročne. V roku 2009 sme prekročili počet o 7 meraní. V roku 2010 sme k 31.12.2010 vykonali 220 meraní, t.j. cieľ bol prekročený o 10 %.

Vzhľadom na vývoj nových technológií a inštaláciu zložitých zariadení najmä v orgánoch verejnej moci je potrebné, aby sa merania NEV v budúcnosti špecializovali napríklad na oblasť mobilných telefónov (kde už boli realizované prvé merania a bol spracovaný plán merania a merací protokol) alebo na oblasť realizácie on-site meraní. K dosiahnutiu týchto cieľov je potrebné zakúpenie nevyhnutných technických zariadení a vyškolenie príslušníkov NBÚ.

Na základe uvedeného konštatujeme, že pri dosahovaní cieľa bol zaznamenaný výrazný pokrok.

Dosah/vplyv:

Širšie ciele programu boli dosiahnuté (viď tabuľka cieľa). Všetky činnosti potrebné k napĺňaniu daného cieľa sú súčasťou celého komplexu činností nevyhnutných na OUS a smerujúcich k plneniu zámeru programu. Merania sú súčasťou certifikačného procesu technických prostriedkov.

Udržateľnosť

Z dôvodu plnej udržateľnosti cieľa bude potrebné zabezpečiť finančné prostriedky na obnovu existujúcej techniky a nákup nových zariadení na výkon špecializovaných meraní.

Gestor : Sekcia informačnej bezpečnosti a elektronického podpisu

Cieľ 6:

Vybaviť všetkých odborných pracovníkov výpočtovou technikou; v roku 2010 vybaviť 98% všetkých odborných pracovníkov výpočtovou technikou

Monitorovanie cieľa :

Stanovený cieľ „Vybaviť všetkých odborných pracovníkov výpočtovou technikou“ je plne aktuálny a prispôbostený skutočným potrebám, ktoré vychádzajú z požiadaviek kladených na NBÚ. Cieľ je dlhodobý, dynamického charakteru a výsledkom jeho plnenia je plne pokrytie technickým vybavením v oblasti pracovných staníc a ich príslušenstva. Dynamickosť plnenia cieľa je chápaná najmä v nutnosti sa prispôbovať tzv. morálnemu zastaraniu výpočtovej techniky, nakoľko prichádza k morálnemu zastarávaniu väčšiny hardvérových komponentov. Značná časť tejto výpočtovej techniky bola obstaraná ešte v rokoch 2001 až 2003. V súčasnosti používanému operačnému systému WinXP končí podpora v rokoch 2012 až 2014 a v prípade nutnosti prechodu na nový operačný systém

Windows 7 bude značne problematické využitie súčasnej výpočtovej techniky v terajších konfiguráciách. Preto v horizonte uvedených rokov sa uvažuje s komplexnejšou obnovou výpočtovej techniky celého úradu.

Potreba realizácie cieľa je v súlade so súčasnými potrebami a kapacitami úradu. Absenciou primeranej výpočtovej techniky by sa znefunkčnila činnosť úradu ako celku a ako synergický efekt by sa následne prejavila strata elektronickej komunikácie vo vnútri a navonok, zásadná strata efektivity práce a nutnosť navýšenia personálneho stavu pracovníkov. Plnenie cieľa má jasne stanoveného gestora zodpovedného za jej plnenie, či už v rozsahu nákupu novej výpočtovej techniky alebo správy používanej výpočtovej techniky, jej údržby a opráv.

Stav plnenia.

K 31.12.2010 bol stanovený percentuálny podiel pracovníkov vybavených výpočtovou technikou splnený na 100%.

Plnenie cieľa je hodnotené ako efektívne a hospodárne, nakoľko sa realizuje bez nutnosti zainteresovania dodávateľských firiem na integračnej úrovni.

Cieľ nebude efektívne dosiahnuteľný s menším počtom pracovníkov a znížením mzdových finančných prostriedkov. V prípade zníženia počtu pracovníkov by muselo prísť k zadávaniu prác a realizácií vykonávania činností dodávateľským spôsobom a za finančnú úhradu neúmerne vyššiu ako sú náklady v súčasnosti.

Zameranie cieľa je podmienené zameraním úradu a cieľová skupina používateľov je zložená z pracovníkov úradu.

Gestor : Sekcia informačnej bezpečnosti a elektronického podpisu

Cieľ 7:

V roku 2010 zvýšiť spoľahlivosť a funkčnosť informačného systému NBÚ znížením celkového počtu porúch a výpadkov na maximálny počet 13

Monitorovanie cieľa :

Stanovený cieľ „V roku 2010 zvýšiť spoľahlivosť a funkčnosť informačného systému NBÚ znížením celkového počtu porúch a výpadkov na maximálny počet 13“ reprezentuje celkový sumár porúch, prípadne výpadkov činností jednotlivých informačných technológií v oblasti podprogramu 08503 – Bezpečnosť komunikačných a informačných systémov. Úlohou je zabezpečiť dostupnosť informačných systémov, ktoré sú prevádzkované v rámci úradu, realizovať činnosti pri ich správe, udržiavaní v prevádzky schopnom stave a rozširovať ich podľa schválených koncepčných zámerov.

Stanovený cieľ je plne aktuálny a prispôsobený skutočným potrebám, ktoré vychádzajú z požiadaviek kladených na NBÚ a sú v súlade so zákonom. Cieľ je dlhodobý a výsledkom jeho plnenia je funkčnosť a práca najmä nasledovných informačných technológií:

- správa internetovej stránky úradu,
- správa intranetovej stránky úradu,
- správa mailových serverov úradu - vnútorná a vonkajšia pošta úradu,
- technologická správa automatizovaný informačný systém pre správu registratúry (Fabasoft),
- technologická správa ASPI,
- administrácia portálu právnych predpisov,

- technologická správa elektronického protokolov pre evidenciu US,
- technologická správa IS evidencie vystavených a vrátených certifikátov pre NATO a EÚ,
- technologická správa automatizovaného IS pre centrálny register,
- technologická správa serverov IS Previerka,
- technologická správa ekonomického a personálneho informačného systému Garis,
- správa informačného systému Integrovaná báza dát -neutajovaná časť,
- správa sieťovej infraštruktúry úradu,
- administrácia digitálneho multifunkčného systému,
- administrácia liniek a trunkov a optického pripojenia NBÚ,
- administrácia tarifikačného systému,
- administrácia VPN: NBÚ - NATO, EU, NBÚ - T-Mobile.

Potreba realizácie cieľa je v súlade so súčasnými potrebami a kapacitami úradu. Ich aktuálnosť bola premietnutá aj v rámci hlavných úloh úradu pre rok 2010.

Každá jedna úloha má jasne stanoveného gestora zodpovedného za jej plnenie a vždy začiatkom roka je stanovený schválený časový harmonogram a termín realizácie. List úlohy obsahuje najmä:

- cieľ úlohy,
- plán postupu,
- výstupy úlohy,
- tím riešiteľov a spoluriešiteľov,
- príjemcov,
- potrebné disponibilné finančné zdroje,
- súlad úlohy s politikou a koncepčným zameraním úradu so zreteľom na synergické hľadisko zámeru.

Plnením jednotlivých úloh bude zabezpečená ochrana informačných technológií s nasadením dostatočného počtu kompetentných pracovníkov a to tak, aby cieľ bol splnený v súlade so stanoveným harmonogramom, prípadne v čo možno najkratšom termíne pri súčasnom dodržaní kvalitatívnych požiadaviek.

Stav plnenia.

Počet výpadkov k 31.12.2010 bol v počte 12.

Podľa hodnotenia terajšieho stavu neprišlo k zásadnému nárastu počtu porúch voči plánu. Výskyt počtu porúch spadá do oblasti náhodnej veličiny a nakoľko technologické zariadenia informačných systémov sú už morálne opotrebované, je možné v budúcnosti očakávať zvyšujúci sa počet hardvérových porúch a výpadkov informačných systémov.

Plnenie cieľa je hodnotené ako efektívne a hospodárne, nakoľko značnú časť činností zabezpečujú pracovníci gestora, bez nutnosti zainteresovania dodávateľských firiem na integračnej úrovni aj napriek skutočnosti, že sa jedná o vysoko odborné činnosti v oblasti správy informačných technológií.

Cieľ nebude efektívne dosiahnuteľný s menším počtom pracovníkov a znížením mzdových finančných prostriedkov. V prípade zníženia počtu pracovníkov by muselo prísť k zadávaniu prác a realizácií vykonávania aj pravidelných servisných činností dodávateľským spôsobom a za finančnú úhradu neúmerne vyššiu ako sú náklady v súčasnosti.

Zameranie cieľa je podmienené potrebami úradu a cieľová skupina používateľov je zložená z pracovníkov úradu. Plnenie tohto cieľa má vplyv na cieľovú skupinu a v prípade nedostupnosti služieb

príde k ochromeniu a nedostupnosti služieb, znefunkčnenie činností úradu v závislosti od počtu a určenia nefunkčného informačného systému a ako synergický efekt by sa následne prejavila strata elektronickej komunikácie vo vnútri úradu a navonok, zásadná strata efektivity práce a nutnosť navštevovania personálneho stavu pracovníkov.

Gestor : Sekcia informačnej bezpečnosti a elektronického podpisu

Cieľ 8:

Akreditácia komunikačných a informačných systémov NATO, resp. národných systémov, v ktorých sa spracovávajú utajované informácie NATO

Monitorovanie cieľa:

Relevantnosť- dosiahnuté výsledky zabezpečujú plnenie úlohy, vyplývajúcej zo zákona č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov - ochranu utajovaných skutočností postúpených Slovenskej republike cudzou mocou, spracovávaných na technických prostriedkoch. Merateľný ukazovateľ - počet vydaných rozhodnutí odráža plnenie cieľa iba pre komunikačné a informačné systémy NATO.

Efektívnosť a hospodárnosť - sú primerané vo vzťahu k výsledkom. Je dodržiavaný časový harmonogram dosahovania uvedeného cieľa s rovnakým počtom príslušníkov počas celej doby hodnotenia plnenia ukazovateľa.

Účinnosť - v roku 2010 boli prijaté dve žiadosti o akreditáciu komunikačných a informačných systémov NATO. Proces akreditácie komunikačných a informačných systémov NATO bol ukončený vydaním rozhodnutí v súvislosti s akreditáciou komunikačných a informačných systémov NATO vo 2 prípadoch, čo predstavuje plnenie ukazovateľa na 100 %.

Gestor : Sekcia informačnej bezpečnosti a elektronického podpisu

Cieľ 9:

Akreditácia komunikačných a informačných systémov EÚ, resp. národných systémov, v ktorých sa spracovávajú utajované informácie EÚ

Monitorovanie cieľa:

Relevantnosť- dosiahnuté výsledky zabezpečujú plnenie úlohy, vyplývajúcej zo zákona č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov - ochranu utajovaných skutočností postúpených Slovenskej republike cudzou mocou, spracovávaných na technických prostriedkoch. Merateľný ukazovateľ - počet vydaných rozhodnutí odráža plnenie cieľa iba pre komunikačné a informačné systémy EÚ.

Efektívnosť a hospodárnosť - sú primerané vo vzťahu k výsledkom. Je dodržiavaný časový harmonogram dosahovania uvedeného cieľa s rovnakým počtom príslušníkov počas celej doby hodnotenia plnenia ukazovateľa.

Účinnosť - v roku 2010 boli prijaté dve žiadosti o akreditáciu komunikačných a informačných systémov EÚ. Proces akreditácie komunikačných a informačných systémov EÚ bol ukončený vydaním rozhodnutí v súvislosti s akreditáciou komunikačných a informačných systémov EÚ vo 2 prípadoch, čo predstavuje plnenie ukazovateľa na 100 %.

Gestor : Sekcia informačnej bezpečnosti a elektronického podpisu

08504 – Elektronický podpis

Zámer:

Vytvorenie podmienok pre bezpečné používanie elektronického podpisu v súlade so zákonom o elektronickom podpise a o zmene a doplnení niektorých zákonov

Cieľ 1:

V roku 2010 vykonať sedem kontrol certifikačných autorít zameraných na dodržiavanie ustanovení zákona o elektronickom podpise

Monitorovanie cieľa:

K 31.12.2010 bolo reálne vykonaných **12** kontrol certifikačných autorít a akreditovaných certifikačných autorít a 1 ZSC so zameraním na dodržiavanie ustanovení zákona o elektronickom podpise, pričom 4 kontroly z vykonaných kontrol sa uskutočnili mimo plánu kontrol. Z vykonaných kontrol z roku 2009 vyplynulo aj vykonanie kontroly plnenia opatrení v CA PSCA v roku 2010, ktorá nebola zohľadnená v pláne kontrol pre rok 2010.

Plánovanie a tvorba cieľa č.1, čo do obsahu („kontrola certifikačných autorít“), vyplýva Národnému bezpečnostnému úradu zo zákona č. 215/2002 Z.z. o elektronickom podpise a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. Plánovanie samotného rozsahu vykonaných kontrol vyplynulo zo stavu prostredia elektronického podpisu (PKI infraštruktúry verejného kľúča v SR) v roku 2009. Kontroly boli plánované v certifikačnej autorite CA Disig so sídlom v Bratislave, v CA APOLLO so sídlom v Bratislave, v CA Slovanet so sídlom v Bratislave, ZSC zameraná na posúdenie stavu podľa záverečnej správy bezpečnostného auditu v I.CA so sídlom v Českej Republike, ďalej kontrola v CA SNCA so sídlom v Bratislave, v CA Tedis so sídlom v Bratislave, v CAMOSR so sídlom v Trenčíne a v CA PSCA so sídlom v Bratislave.

Začiatkom roka 2010 sa uskutočnili kontroly, ktorých cieľom bolo posúdiť zapracovanie zmien v legislatíve, platných od 1.1.2010, do prevádzky a činností certifikačných autorít. Tieto kontroly sa všetky uskutočnili navyše oproti pôvodne plánovanému počtu.

Kontrola **CA Disig**, uskutočnená mimo plánu kontrol, bola začatá v januári 2010 a ukončená vo februári 2010 záznamom o kontrole, nakoľko nebolo zistené porušenie všeobecne záväzných právnych predpisov.

Kontrola **CA PSCA** mimo plánu kontrol bola začatá v januári 2010 a ukončená vo februári 2010 záznamom o kontrole, nakoľko nebolo zistené porušenie všeobecne záväzných právnych predpisov.

Kontrola **RA I.CA v DTCA** mimo plánu kontrol bola začatá v januári 2010 a ukončená v auguste 2010 protokolom o výsledku kontroly a následne zápisnicou o prerokovaní protokolu o výsledku kontroly, nakoľko bolo zistené porušenie všeobecne záväzných právnych predpisov.

Kontrola **RA I.CA v ČSOB** mimo plánu kontrol bola začatá v januári 2010 a ukončená v auguste 2010 protokolom o výsledku kontroly a následne zápisnicou o prerokovaní protokolu o výsledku kontroly, nakoľko bolo zistené porušenie všeobecne záväzných právnych predpisov.

Následne boli pracovníkmi Národného bezpečnostného úradu vykonávané kontroly v súlade s pôvodným plánom kontrol.

Kontrola **CA Disig** bola vykonaná v marci 2010 a ukončená záznamom o kontrole, nakoľko nebolo zistené porušenie všeobecne záväzných právnych predpisov.

Kontrola **CA APOLLO** bola vykonaná v marci 2010 a ukončená záznamom o kontrole, nakoľko nebolo zistené porušenie všeobecne záväzných právnych predpisov.

Kontrola **CA Slovanet** bola začatá v apríli 2010 a ukončená v máji 2010 záznamom o kontrole, nakoľko nebolo zistené porušenie všeobecne záväzných právnych predpisov.

Kontrola plnenia opatrení v **CA PSCA** bola začatá v apríli 2010 a ukončená v máji 2010 záznamom o kontrole, nakoľko bolo v kontrolovanom subjekte zistené odstránenie skutočností uvedených v protokole o výsledku kontroly z predošlej kontroly z roku 2009.

V I.CA ČR boli pracovníci na ZSC, ktorej obsahom bolo posúdiť dodržiavanie ustanovení zákona o elektronickom podpise, v máji 2010, čo bolo zavŕšené záverečnou správou auditu bezpečnosti certifikačnej autority I.CA od nezávislého audítora z apríla 2010.

Kontrola **CA SNCA** bola začatá v júli 2010 a ukončená v auguste 2010 záznamom o kontrole, nakoľko nebolo zistené porušenie všeobecne záväzných právnych predpisov.

Kontrola **CA Tedis** bola ukončená v septembri 2010 úradným záznamom, nakoľko fyzická kontrola nemohla byť vykonaná z dôvodu zániku tohto právneho subjektu.

Kontrola **CAMOSR** bola začatá v októbri 2010 a ukončená v novembri 2010 protokolom o výsledku kontroly a následne zápisnicou o prerokovaní protokolu o výsledku kontroly, nakoľko bolo zistené porušenie všeobecne záväzných právnych predpisov.

Kontrola **CA PSCA** bola vykonaná v decembri 2010 a ukončená záznamom o kontrole, nakoľko nebolo zistené porušenie všeobecne záväzných právnych predpisov.

Zistené nedostatky:

Zistené nedostatky v RA I.CA v DTCA a ČSOB súviseli s procesom vydávania následného kvalifikovaného certifikátu klientovi.

Zistené nedostatky v CAMOSR súviseli s používaním necertifikovaného HSM zariadenia ako bezpečného zariadenia pre vyhotovenie ZEP.

V kontrolovaných subjektoch boli uložené konkrétne opatrenia na odstránenie zistených nedostatkov a ich príčin uvedených v protokole o výsledku kontroly.

a) relevantnosť - povinnosť vykonávať kontroly CA a ACA vyplýva zo zákona č. 215/2002 Z. z. o elektronickom podpise. Počet kontrol závisí jednak od počtu registrovaných CA a ACA, ale aj od ďalších prvkov, ako sú zmeny životného cyklu týchto subjektov, zmeny technológie a prevádzkových procesov, zmeny legislatívy a iné... Kontroly vykonávajú dvaja až traja pracovníci odboru elektronického podpisu. Účelom, pre ktorý sa kontroly certifikačných autorít vykonávajú, je predovšetkým udržanie bezpečného prostredia pre používanie elektronického podpisu, a to tak v činnosti poskytovateľov certifikačných služieb ako aj v produktoch, ktoré títo pri svojej činnosti poskytujú verejnosti, a teda v súlade so stanoveným zámerom podprogramu 08504 -Elektronický podpis. Úlohou kontrol je zisťovanie rizikových skutočností v prostredí elektronického podpisu a formou ukladania nápravných opatrení a následného sledovania ich plnenia udržanie a zvyšovanie bezpečnosti prostredia elektronického podpisu a zaručeného elektronického podpisu v praxi.

b) efektívnosť - plnenie cieľa možno hodnotiť ako efektívne a hospodárne, nakoľko všetky činnosti zabezpečujú pracovníci odboru elektronického podpisu. Náklady predstavujú len použitie služobného dopravného prostriedku a náhrady pri TSC. V roku 2010 bol plán kontrol prekročený o 70% , pričom náklady boli vynaložené efektívne.

c) účinnosť - cieľom vykonávaných kontrol CA a ACA je udržanie a zvyšovanie bezpečnosti prostredia pre používanie elektronického podpisu a zaručeného elektronického podpisu v praxi. Kontrola sa vykonáva priamo v subjektoch, ktoré poskytujú certifikačné služby občanom, sú základným prvkom v infraštruktúre verejného kľúča PKI v SR, takže pracovníci Národného bezpečnostného úradu majú priamy dosah na sledovanie a zvyšovanie bezpečnosti celého prostredia.

d) dosah/vplyv - výkon kontrol priamo pozitívne vyplýva na zlepšovanie poskytovania certifikačných služieb zo strany poskytovateľov a vytváranie bezpečnejšieho prostredia pre používateľov elektronického podpisu, čo má vo veľkej miere vplyv aj na bezpečnosť súkromných ekonomických aktivít občanov a podnikateľskej obce.

e) udržateľnosť - plnenie cieľa vykonávania kontrol CA a ACA je ovplyvňované a musí reagovať na počet registrovaných CA a ACA, ale aj na ďalšie prvky, ktoré sa podieľajú na infraštruktúre verejného kľúča PKI v SR, ako sú zmeny životného cyklu subjektov v PKI, zmeny technológie a prevádzkových procesov subjektov v PKI, zmeny legislatívy o elektronickom podpise v kontrolovanom období.

Gestor : Sekcia informačnej bezpečnosti a elektronického podpisu

Cieľ 2

Inštalovať v roku 2010 50 % doplnkových technologických zariadení certifikačnej autority a záložného pracoviska potrebných pre zabezpečenie jej funkčnosti smerom k cieľovému stavu

Monitorovanie cieľa :

V roku 2009 vstúpila do platnosti novela zákona č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov. Na základe tejto novelizácie sa v roku 2009 začali realizovať činnosti prechodu na nové šifrovacie algoritmy, čo v praxi znamená vybudovanie novej PKI pre koreňovú certifikačnú autoritu a akreditovanú certifikačnú autoritu NBÚ.

Z dôvodu pridelenia finančných prostriedkov až v druhom polroku 2009 sa činnosti vybudovania následníka akreditovanej certifikačnej autority NBÚ presunuli do roku 2010.

Stanovený cieľ „Inštalovať v roku 2010 50 % doplnkových technologických zariadení certifikačnej autority a záložného pracoviska potrebných pre zabezpečenie jej funkčnosti smerom k cieľovému stavu“ je aktuálny a prispôsobený skutočným potrebám, ktoré vychádzajú z požiadaviek kladených na NBÚ a sú v súlade so zákonom. Cieľ je stanovený len do roku 2012 a po spustení predmetu cieľa do rutínnej prevádzky, vrátane ukončenia činností v záložnej lokalite, bude ukončený. Potreba realizácie cieľa je v súlade so súčasnými potrebami a kapacitami úradu. Ich aktuálnosť bola premietnutá v rámci hlavných úloh úradu HÚZO pre rok 2010 a to najmä: číslo úlohy 7.4 „Spustiť rutinnú prevádzku archívu kvalifikovaných certifikátov ACAs“.

Výsledkom plnenia cieľa je vytvorenie a spustenie do rutínnej prevádzky následníkov certifikačných autorít úradu:

- KCA následník,
- SNCA následník.

Plnenie cieľa má jasne stanoveného gestora zodpovedného za jeho plnenie a vždy začiatkom roka je stanovený a schválený časový harmonogram a termín realizácie. List úlohy obsahuje najmä:

- cieľ úlohy,
- plán postupu,
- výstupy úlohy,
- tím riešiteľov a spoluriešiteľov,
- príjemcov,
- potrebné disponibilné finančné zdroje,
- súlad úlohy s politikou a koncepčným zameraním úradu so zreteľom na synergické hľadisko zámeru.

Splnením cieľa budú splnené požiadavky vyplývajúce z novelizácie zákona. Činnosti sú realizované s nasadením dostatočného počtu kompetentných pracovníkov a to tak, aby cieľ bol splnený v súlade so stanoveným harmonogramom, prípadne v čo možno najkratšom termíne pri súčasnom dodržaní kvalitatívnych požiadaviek.

Stav plnenia:

Do rutinného stavu bol uvedený následník koreňovej certifikačnej autority Slovenskej republiky a následník akreditovanej certifikačnej autority SNCA. Na základe uvedeného je možné konštatovať, že stanovený cieľ pre rok 2010 bol splnený. Plnenie cieľa je hodnotené ako efektívne a hospodárne, nakoľko všetky činnosti zabezpečujú pracovníci, bez nutnosti zainteresovania dodávateľských firiem na integračnej úrovni aj napriek skutočnosti, že sa jedná o vysoko odborné činnosti v oblasti informačných technológií so zameraním na PKI.

Cieľ nebude efektívne dosiahnuteľný s menším počtom pracovníkov a znížením mzdových finančných prostriedkov. V prípade zníženia počtu pracovníkov by muselo prísť k realizácii prác dodávateľským spôsobom a za finančnú úhradu neúmerne, ktorá by dosahovala hodnotu niekoľko desiatok tisíc EUR.

Zameranie cieľa je podmienené zákonom a cieľová skupina používateľov je zložená z užívateľov mimo NBÚ (verejnosť, podnikateľské prostredie a vybrané zložky štátnej správy) a pracovníkov úradu. Plnenie tohto cieľa má vplyv na cieľovú skupinu a v prípade nedostupnosti služieb príde k ochromeniu a nedostupnosti certifikačných služieb v rámci Slovenskej republiky.

Gestor : Sekcia informačnej bezpečnosti a elektronického podpisu

Cieľ 3:

V roku 2010 eliminovať výpadky z dôvodu straty funkčnosti a nedostupiteľnosti služieb certifikačnej autority pri používaní elektronického podpisu na maximálny počet 5

Monitorovanie cieľa :

Úlohy vyplývajú zo zámeru podprogramu 08504 – Elektronický podpis, majú oporu v zákone č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov a vyplývajú zo záväzkov SR voči zámerom EÚ a NATO. Stanovený cieľ má priamu náväznosť na cieľ 3 „Vytvoriť podmienky pre bezpečné používanie elektronického podpisu“ a sleduje funkčnosť samostatnej architektúry Záložnej lokality certifikačných autorít úradu v Novom Meste nad Váhom.

V zmysle zákona č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov NBÚ zodpovedá za prevádzku Koreňovej certifikačnej autority, vydávanie certifikátov podriadeným akreditovaným certifikačným autoritám a zoznamu zneplatnených certifikátov. Uvedené činnosti musia byť vykonávané v reálnom čase a do stanoveného časového intervalu, tak ako definuje zákon a následné vyhlášky. NBÚ je taktiež povinný poskytovať v zmysle tohto zákona aj certifikačné služby pre vybrané zložky štátnej správy, vrátane poskytovania časovej pečiatky.

Predmetom plnenia cieľa je udržiavať v prevádzkovo schopnom stave PKI koreňovej certifikačnej autority, akreditovanej certifikačnej autority úradu, záložnú lokalitu a jej pridruženú podpornú infraštruktúru. Zákon a následné vyhlášky definujú povinnosť poskytovať certifikačné služby verejnosti, podnikateľskému prostrediu, vybraným zložkám štátnej správy, EÚ a NATO aj v prípade akejkoľvek nedostupnosti (aj rádovo niekoľko sekúnd) primárnej lokality (infraštruktúra úradu v Bratislave). Prechod činností na záložnú lokalitu zvyčajne prechádza v prípade vzniknutej poruchy na primárnej lokalite, nedostupnosti jej pripojenia na Internet, prípadne celkového zničenia primárnej lokality.

Stanovený cieľ „V roku 2010 eliminovať výpadky z dôvodu straty funkčnosti a nedostupiteľnosti služieb certifikačnej autority pri používaní elektronického podpisu na maximálny počet 5“ je plne aktuálny a prispôsobený skutočným potrebám, ktoré vychádzajú z požiadaviek kladených na NBÚ a sú v súlade so zákonom. Cieľ je dlhodobý a výsledkom jeho plnenia je funkčnosť prechod funkčnosti z primárnej do záložnej infraštruktúry u najmä nasledovných informačných technológií:

- koreňová certifikačná autorita Slovenskej republiky (KCA),
- akreditovaná certifikačná autorita SNCA,
- poskytovanie akreditovanej služby časovej pečiatky,
- poskytovanie certifikačných služieb systému Pasy SR,
- poskytovanie certifikačných služieb pre technické preukazy motorových vozidiel v SR.

Každá jedna úloha má jasne stanoveného gestora zodpovedného za jej plnenie a vždy začiatkom roka je stanovený a schválený časový harmonogram a termínu realizácie. List úlohy obsahuje najmä:

- cieľ úlohy,
- plán postupu,
- výstupy úlohy,
- tím riešiteľov a spoluriešiteľov,
- príjemcov,
- potrebné finančné zdroje,
- súlad úlohy s politikou a koncepcným zameraním úradu so zreteľom na synergické hľadisko zámeru.

Plnením jednotlivých úloh bude zabezpečená ochrana elektronického podpisu na požadovanej úrovni v zmysle zákona s nasadením dostatočného počtu kompetentných pracovníkov a to tak, aby cieľ bol splnený v súlade so stanoveným harmonogramom, prípadne v čo možno najkratšom termíne pri súčasnom dodržaní kvalitatívnych požiadaviek.

Stav plnenia.

Do 31.12.2010 prišlo k 7 výpadkom na primárnej infraštruktúre úradu. Tento stav reprezentuje zvýšenie počtu porúch voči plánu. Zvýšený počet porúch vznikol najmä z dôvodu výpadkov klimatizačných jednotiek a problémov spojených s ich opravou, nakoľko sa jedná o zastarané zariadenia. Z dôvodu nemožnosti opráv a ich neefektivity boli klimatizačné jednotky v kľúčových technologických miestnostiach vymenené.

Plnenie cieľa je hodnotené ako efektívne a hospodárne, nakoľko všetky činnosti zabezpečujú pracovníci, bez nutnosti zainteresovania dodávateľských firiem na integračnej úrovni aj napriek skutočnosti, že sa jedná o vysoko odborné činnosti v oblasti informačných technológií so zameraním na PKI.

Cieľ nebude dosiahnuteľný s menším počtom pracovníkov a následným znížením mzdových finančných prostriedkov. V prípade zníženia počtu pracovníkov by muselo prísť k zadávaniu prác a realizácii vykonávania pravidelných servisných činností dodávateľským spôsobom a za finančnú úhradu neúmerne vyššiu ako sú náklady v súčasnosti.

Zameranie cieľa je podmienené zákonom a cieľová skupina používateľov je zložená z užívateľov mimo NBÚ (verejnosť, podnikateľské prostredie, vybrané zložky štátnej správy, EÚ a NATO) a pracovníkov úradu. Plnenie tohto cieľa má vplyv na cieľovú skupinu a v prípade nedostupnosti služieb príde k ochromeniu a nedostupnosti certifikačných služieb v rámci Slovenskej republiky.

Gestor : Sekcia informačnej bezpečnosti a elektronického podpisu

Záver hodnotenia programovej štruktúry :

Postavené ciele sú reálne, kontrolovateľné a merateľné. Merateľné ukazovatele sú formulované v priamej nadväznosti na stanovený cieľ, pričom ciele odrážajú zámer programu.

Pokiaľ ide o posúdenie, či za rovnaké vstupy je možné získať vyššie výstupy, alebo či je možné za nižšie vstupy dosiahnuť rovnaké výstupy, vo väčšine prípadov je pomer medzi vstupmi a výstupmi adekvátny. Ciele stanovené v rámci jednotlivých podprogramov a prvkov programu 085 – Bezpečnosť informácií sú konzistentné s rozpočtovými zdrojmi.

A 1.3 Hodnotenie vývoja úradu ako celku z hľadiska jeho organizačnej štruktúry a personálneho vybavenia

Plnenie úloh Národného bezpečnostného úradu zabezpečujú predovšetkým príslušníci NBÚ, ktorí sú v služobnom pomere podľa zákona č. 73/1998 Z. z. o štátnej službe príslušníkov Policajného zboru, Slovenskej informačnej služby, Zboru väzenskej a justičnej stráže SR a Železničnej polície v znení neskorších predpisov. Na činnosti NBÚ sa podieľajú aj zamestnanci, ktorí sú v pracovnom pomere podľa zákona č. 552/2003 Z. z. o výkone prác vo verejnom záujme. Postavenie riaditeľa úradu upravuje zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

Z hľadiska organizačnej štruktúry sa úrad člení na sedem sekcií, ktoré sa členia na odbory a niektoré z odborov sú rozdelené na oddelenia. Počet systemizovaných miest príslušníkov úradu v služobnom pomere a zamestnancov v pracovnom pomere je schválený uznesením vlády Slovenskej republiky. Pre rok 2010 bolo schválených 232 miest príslušníkov a 36 miest zamestnancov (vrátane riaditeľa úradu).

Národný bezpečnostný úrad vznikol 1. 7. 2001 a ku dňu 31. 12. 2010 dosiahol 88 % obsadenosť, čo predstavuje 209 príslušníkov a 27 zamestnancov. Pomer mužov a žien bol 51 % muži a 49 % ženy. Veková štruktúra príslušníkov a zamestnancov úradu bola nasledovná:

- do 30 rokov 16 %,
- do 40 rokov 44 %,
- do 50 rokov 20 %,
- do 60 rokov 18 %,
- nad 60 rokov 2 %.

Vzdelanostná štruktúra v roku 2010 predstavovala:

- počet príslušníkov a zamestnancov s vysokoškolským vzdelaním II. stupňa: 77 %,
- počet príslušníkov a zamestnancov so stredoškolským vzdelaním: 20 %,
- počet zamestnancov so základným vzdelaním, resp. bez ukončeného základného vzdelania (pomocné a upratovacie práce): 3 %.

Ochrana utajovaných skutočností je základným poslaním Národného bezpečnostného úradu a zároveň dôležitým pilierom bezpečnosti štátu. Toto poslanie musia napĺňať ľudské zdroje na vysokej odbornej a morálnej (osobnostnej) úrovni. Zákon č. 73/1998 Z. z. o štátnej službe príslušníkov Policajného zboru, Slovenskej informačnej služby, Zboru väzenskej a justičnej stráže SR a Železničnej polície v znení neskorších predpisov upravuje v porovnaní s pracovným a štátnozamestnaneckým pomerom prísnejšie a náročnejšie podmienky pre prijatie do služobného pomeru predovšetkým v oblasti zdravotnej, telesnej a duševnej spôsobilosti, bezúhonnosti i spoľahlivosti. Dôležitou podmienkou pre výkon štátnej služby a plnenie pracovných povinností v podmienkach úradu je aj bezpečnostná spoľahlivosť, ktorá sa posudzuje u každého uchádzača o prijatie do služobného aj pracovného pomeru.

Národný bezpečnostný úrad za účelom udržiavania odbornej pripravenosti a zručností príslušníkov a zamestnancov úradu umožňuje prehlbovanie kvalifikácie formou odborných kurzov doma i v zahraničí a v prípade potreby aj zvyšovanie ich kvalifikácie na vysokých školách a zabezpečuje špecializované policajné (odborné) vzdelávanie príslušníkov úradu na Akadémii Policajného zboru v Bratislave, ktoré je podmienkou pre zaradenie do stálej štátnej služby.

A 1.4 Prehľad najčastejšie žiadaných informácií podľa zákona NR SR č. 211/2000 Z. z. o slobode informácií

V roku 2010 Národný bezpečnostný úrad zaevidoval 101 žiadostí o poskytnutie informácií podľa zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám. Niektorí žiadatelia žiadali o metodické usmernenie (najmä z oblasti administratívnej bezpečnosti), prípadne o výklad jednotlivých ustanovení zákona o ochrane utajovaných skutočností a zákona o elektronickom podpise. Na úrad sa obracali aj občania sťažujúci sa na postup štátnych orgánov. Tieto podnety však nebolo možné posudzovať v zmysle zákona o slobode informácií, podľa vecnej príslušnosti boli odstúpené na riešenie zodpovedajúcim adresátom.

Pokiaľ ide o obsahovú stránku, najviac otázok sa týkalo problematiky elektronického podpisu (spôsob nadobudnutia EP, kontakt na certifikačné authority, rozličné technické aspekty podpisových politík, služby časovej pečiatky, vývoja hardvéru a softvéru pre EP). Žiadatelia ďalej zisťovali podmienky a okolnosti bezpečnostného preverovania fyzických a právnických osôb (požadované podklady, lehoty, stav vybavovania žiadosti a podobne), administratívnej bezpečnosti (evidencia, náležitosti, rozmnožovanie utajovaných písomností, podmienky oboznamovania), certifikácie technických prostriedkov. Ďalšie žiadosti sa týkali rozličných okruhov činnosti úradu – najmä úlohy, kompetencie a kontrola úradu, vzdelávanie zamestnancov, školenia bezpečnostných zamestnancov, protikorupčnej politiky NBÚ, atď.

Národný bezpečnostný úrad v roku 2010 odpovedal na všetky doručené žiadosti. K dvom žiadostiam úrad vydal Rozhodnutie o odmietnutí poskytnúť informácie. Medzi žiadateľmi prevažovali fyzické osoby, vyskytli sa aj žiadosti právnických osôb. Takmer všetky otázky boli doručené i vybavené elektronickou poštou, niektoré poštou, viaceré vyvolali osobné stretnutia so žiadateľmi, na ktorých boli detailne prediskutované zložitejšie odborné problémy. Národný bezpečnostný úrad žiadosti vybavoval priebežne a načas, v zmysle ustanovení zákona a v súlade s internými predpismi. Gestorom odpovedí bola Kancelária úradu, odborné otázky boli konzultované s príslušnými odbornými útvarmi.

A 2 Činnosť NBÚ v roku 2011

A 2.1 Rozpočet úradu na rok 2011

Rozpis záväzných ukazovateľov – program 085 – Bezpečnosť informácií

	v eurách
	Rozpis rozpočtu
I. Príjmy kapitoly	
A. Záväzný ukazovateľ	41 000
B. Prostriedky z rozpočtu EÚ	0
II. Výdavky kapitoly spolu (A + B)	7 989 756
A. Výdavky spolu bez prostriedkov z rozpočtu EÚ	7 989 756
Z toho :	
A.1. prostriedky štátneho rozpočtu (kód zdroja 111)	7 989 756
A.2. prostriedky na spolufinancovanie	0
A.3. mzdy, platy, služ. príj. a ost. os. vyrovnania (610), (kód zdroja 111)	4 379 784
Z toho : mzdy, platy, služ. príjmy a ost. os. vyrovnania aparátu ústredného orgánu	4 379 784
Počet zamestnancov	261 osôb
Z toho : aparát ústredného orgánu	261 osôb
A.4. kapitálové výdavky (700) (bez prostriedkov na spolufinancovanie)	49 791
Z toho :	
Kód zdroja 111	49 791
B. Prostriedky z rozpočtu EÚ	0
C. Účelové prostriedky	
085 Bezpečnosť informácií	7 989 756
D. Rozpočet podľa programov :	
085 Bezpečnosť informácií	7 989 756
E. Systemizácia policajtov v štátnej službe	230 osôb
	4 142 632