Koncepcia ochrany utajovaných skutočností
v Slovenskej republike

NBÚ, Bratislava 2007

Obsah

Prílohy

Úvod

Úlohou Národného bezpečnostného úradu a zároveň dôvodom jeho vzniku v roku 2001 bolo *garantovať ochranu utajovaných skutočností* (ďalej len OUS) *postúpených z NATO a EÚ*. Aby NBÚ mohol dobre plniť túto úlohu aj v budúcnosti, musí sa dnes usilovať o vytvorenie optimálneho systému OUS v rámci SR.

OUS v SR bola formulovaná v zákone č. 241/2001 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov a čiastočne reformovaná zákonom č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov (ďalej len „zákon o OUS“) s príslušnými vykonávacími vyhláškami.

Povinnosť spracovať Koncepciu ochrany utajovaných skutočností (ďalej len KOUS) vyplynula pre Národný bezpečnostný úrad z § 5 zákona o OUS. V súlade s touto koncepciou jednotlivé rezorty majú povinnosť vypracovať rezortné koncepcie OUS. Uznesením vlády SR č. 119 zo 14. februára 2007 bol schválený Plán práce Bezpečnostnej rady Slovenskej republiky na rok 2007, kde sa riaditeľovi NBÚ ukladá predložiť Návrh koncepcie OUS na rokovanie BR SR v mesiaci máj 2007 (bod 3).

V zákone o OUS je KOUS definovaná ako *súbor cieľov, obmedzení, požiadaviek, pravidiel a postupov, ktoré určujú spôsob a rozvoj ochrany utajovaných skutočností.*

Koncepcia všeobecne je *spôsob poňatia, chápania výkladu určitého javu; základné hľadisko, vedúca idea, myšlienková osnova, vysvetlenie javu; hlavný zámer alebo konštrukčný princíp pri rozličných druhoch činnosti**.

Koncepciu OUS možno teda chápať ako *usporiadanú sústavu názorov* (náhľad) na OUS. O spôsobe dosahovania cieľov v oblasti OUS však hovorí *stratégia* (náuka). Z uvedeného vyplýva, že definícia KOUS uvedená v zákone obsahuje aj prvky stratégie OUS.

Jedným z cieľov koncepcie je preto aj <u>zovšeobecnenie</u> základných pojmov a procesov s rešpektovaním špecifík jednotlivých oblastí bezpečnosti utajovaných skutočností (ďalej len BUS), pretože dosiaľ nebola publikovaná <u>usporiadaná sústava názorov na OUS</u> v uvedených súvislostiach. Nezastupiteľnou úlohou tejto koncepcie je preto urobiť to aspoň v prvom priblížení – ako základ budúcej teórie OUS a jej rozvoja smerujúcej k optimálnemu systému OUS.

Úlohou tejto KOUS je formulovať hlavné *princípy* OUS a *systémové* požiadavky na cieľový systém OUS. Predstaviť nový pohľad na skúmanie OUS a formulovať základné predstavy o *systémovej štúdii OUS*. Jej cieľom bude presnejšie zadefinovať *systém OUS* tak, aby sa mohol stať východiskom pre tvorbu nového zákona o OUS.

Súčasný stav

Súčasný stav OUS je charakteristický tvorbou medzinárodných dokumentov, ktoré vychádzajú z princípov OUS členských krajín EÚ a NATO. Pravidlá EÚ pre oblasť OUS sú dané legislatívou EÚ, ktorá je súčasťou právnych poriadkov členských krajín. V súčasnosti sa pracuje na smerniciach EÚ pre jednotlivé oblasti BUS. Na úrovni NATO sú nastavené len minimálne štandardy BUS a neexistuje jednotná politika EÚ, resp. NATO pre oblasť utajovaných skutočností (ďalej len US).

* Slovník cudzích slov akademický, Slovenské pedagogické nakladateľstvo - Mladé letá, s.r.o., Druhé, doplnené a upravené slovenské vydanie, 2005).

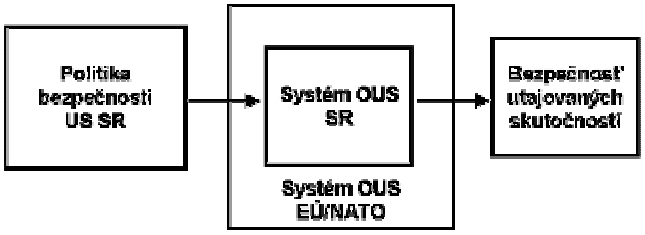
Ciele EÚ v oblasti ochrany utajovaných skutočností sú stanovené všeobecne, rovnako ako nástroje pre ich dosiahnutie.

V rámci EÚ rozhodujúcu úlohu z hľadiska prijímania záverov k OUS plní Rada Európskej únie. Ak neexistuje zhoda názorov členských krajín *je povolený samostatný prístup* s tým, aby sa členská krajina zdržala konania v rozpore so záujmami EÚ alebo znižovala účinnosť jej rozhodnutí.

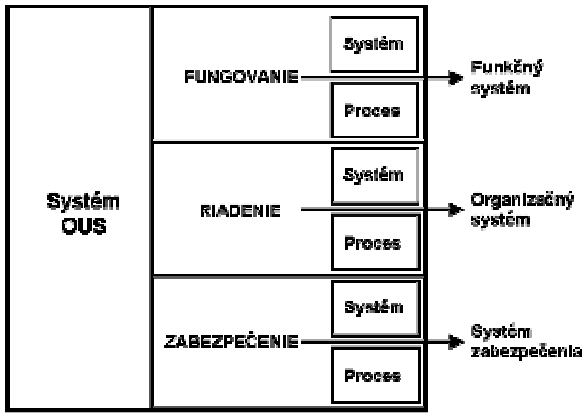
Vzhľadom na neexistenciu takejto zhody (spoločnej nadnárodnej koncepcie OUS, jednotne a jednoznačne definovaných záujmov, množiny spoločných bezpečnostných rizík a bezpečnostných štandardov EÚ a NATO) uplatňuje SR pri dosahovaní BUS vlastný (národný) prístup, ktorý bude zohľadňovať a rešpektovať pravidlá formulované v nariadeniach a rozhodnutiach EÚ a NATO.

Ciele OUS a spôsob ich dosahovania

Všeobecným cieľom ochrany US je dosiahnutie ich *bezpečnosti* (obr.1). V tomto poňatí je OUS prostriedkom, ktorým sa všeobecný cieľ dosahuje.



Obrázok 1 - Cieľ systému OUS



Obrázok 2 - Systém OUS

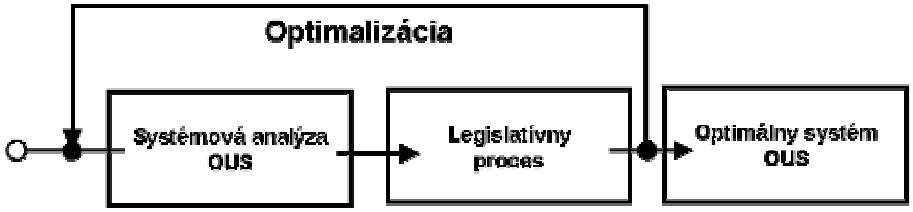
Dlhodobým cieľom OUS je vybudovanie *optimálneho systému* (príloha 1). Metóda, ktorá umožní dosiahnuť tento cieľ je *systémová analýza OUS,* ktorá sa stane základom pre formuláciu *princípov OUS* (príloha 3), z ktorých bude vychádzať *Bezpečnostná politika* utajovaných skutočností postavená na definovaných *záujmoch* SR. Zo záujmov SR vyplynú relatívne pružné a zároveň dostatočne stabilné *zoznamy utajovaných skutočností a bezpečnostných rizík (ďalej len BR).* Systém opatrení na dosiahnutie optimálnej BUS bude vyjadrený relatívne pružným a zároveň dostatočne stabilným systémom *bezpečnostných štandardov (ďalej len BŠ).* Potreba *relatívnej pružnosti* vyplýva z dynamiky bezpečnostného prostredia a požiadavka *stability* z reálnych časových možností zmien legislatívy.

Systémová analýza umožní definovať základné etapy a fázy procesu OUS a následne dopracovať zásady a odhaliť ďalšie princípy, ktoré sa stanú základom pre *ucelenú teóriu OUS.* Teória umožní definovať oblasti bezpečnosti utajovaných skutočností ako *cieľový stav* a zároveň formulovať základný *terminologický slovník OUS,* ktorý zabezpečí prehľadnosť, jednoduchosť a zrozumiteľnosť vyhlášok a zákona o OUS.

Teória OUS sa stane základom pre *koncepciu vzdelávania a rozvoja ľudských zdrojov* potrebných pre udržanie optimálneho stavu OUS. Okrem iného umožní predvídať potreby ľudských

zdrojov do budúcnosti, predvídať a pružne reagovať na zmeny bezpečnostného prostredia, ktoré sa musia premietnuť čo najskôr do procesu OUS a legislatívy.

Používanie nástrojov systémovej analýzy, opakovanej *optimalizácie* (obr.3) a metodiky alternatívneho riešenia problémov OUS s dopadovými štúdiami zabezpečí *adaptivitu* systému OUS na nepretržité zmeny bezpečnostného prostredia, v ktorom sa US budú nachádzať a zároveň jeho finančnú efektívnosť.



Obrázok 3 - Cyklické analýzy

Exaktnosť plynúca z rozvoja teórie OUS prispeje ku skvalitneniu procesu rozhodovania o výsledkoch bezpečnostných previerok, procesov získavania a spracovávania informácií. Rozvoj teórie OUS prispeje k vytvoreniu systému *znalostnej OUS*, ktorá v konečnom dôsledku významným spôsobom zvýši kvalitu a efektívnosť celého procesu OUS.

Aby bolo možné spomenuté nástroje aplikovať v praxi, je nevyhnutné neustále pripravovať ľudské zdroje v kontinuálnom odovzdávaní informácií a skúseností. Kvalitné ľudské zdroje nebude možné udržať ak im nebudú vytvorené podmienky kariérneho rastu a všestranné materiálne, technické, sociálne, zdravotné a dôchodkové zabezpečenie.

Dlhodobý cieľ OUS je možné naplniť len v spolupráci zložiek štátnej správy, samosprávy, ale aj súkromného sektora s využitím tvorivého potenciálu SR.

Princípy a zásady OUS

V súčasnosti je možné formulovať len základné princípy OUS. Podrobnejšie zásady a ďalšie princípy bude potrebné odhaľovať a usporiadať systematicky podľa etáp a fáz popísaného procesu OUS. Predbežný návrh je uvedený v prílohe 3.

Pre princípy OUS je charakteristická ich vnútorná rozpornosť vyplývajúca z veľkej dynamiky zmien bezpečnostného prostredia a zároveň snaha o čím dlhodobejšie zastabilizovanie legislatívy, ktorá ho popisuje.

Metóda riešenia OUS

Podstatou nového prístupu k OUS je nahradenie mechanického prístupu systémovým prístupom.

Mechanickým prístupom k riešeniu problému OUS sa rozumie rozloženie procesu na základné prvky (oblasti), ich izolované riešenie a agregácia výsledkov. Spätná väzba je minimálna.

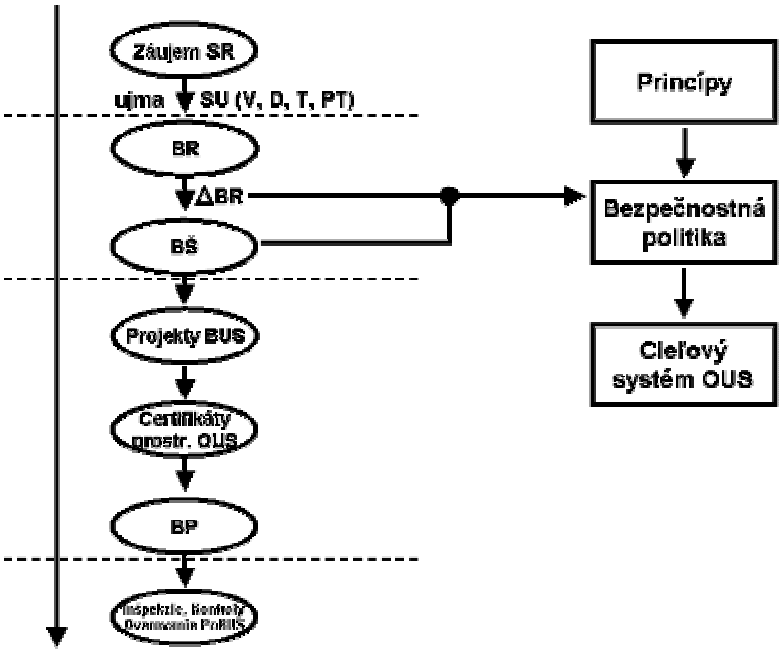
Systémovým prístupom k riešeniu problému OUS sa rozumie integrovaný spôsob, vychádzajúci z organického spojenia prvkov (oblastí) samotných i so systémovým okolím. Konštituuje rozhodovacie fázy, vrátane príslušných spätných väzieb.

Ak má byť OUS riešená *systémovo,* treba odpovedať na otázku čo je cieľom OUS, aké vlastnosti bude mať cieľový systém, aké vstupy a výstupy bude mať, aká bude jeho štruktúra, aké podsystémy a prvky bude obsahovať, aké budú ich vzájomné vzťahy a ako bude vyzerať systémové okolie OUS SR. Treba vyjadriť spôsob, ktorým sa bude možné dopracovať k cieľovej funkcii systému OUS a k účelovým funkciám jeho podsystémov. Bude potrebné prehodnotiť OUS na úrovni štátnej správy, samosprávy a v podnikateľskom prostredí zo systémového hľadiska.

Dnes ešte nie sú známe jednoznačné odpovede na všetky otázky, lebo prostredie, v ktorom sa majú US chrániť je veľmi rôznorodé a medzinárodný systém OUS sa len formuje.

Základná schéma OUS

Logická schéma (obr.4) ukazuje základné prvky systému OUS a ich vzájomnú nadväznosť. Predstavuje sled nadväzných procesov plynúcich zo samotnej podstaty OUS. Schéma je elementárna lebo ďalšie zjednodušovanie už nie je prípustné. Vypustenie ktoréhokoľvek prvku by malo fatálne následky na bezpečnosť utajovaných skutočností.



Obrázok 4 - Základná schéma OUS

Elementárna (základná, principiálna) schéma je východiskom pre tvorbu *politiky bezpečnosti US* (bezpečnostnej politiky US), formuláciu základných princípov OUS a cieľového systému OUS. Zároveň je základom pre terminologické zovšeobecnenie.

Všeobecne je potrebné zadefinovať *predmet utajenia* – utajované skutočnosti a závažnosť utajenia vyjadriť pridelením stupňa ich utajenia (*atribút*, vlastnosť US) v závislosti od veľkosti *ujmy* na *záujmoch*.

Množinu zadefinovaných US je možné sústrediť formou *zoznamu*, príp. *oblastí* ich predpokladaného vzniku. US je potrebné chrániť počas *doby* ich *života*, ktorá všeobecne začína vytvorením a končí ich zničením alebo zrušením stupňa ich utajenia (ďalej len „SU“).

US sa nachádzajú v konkrétnom bezpečnostnom prostredí charakterizovanom rizikami, ktoré by mohli ohroziť ich bezpečnosť – *bezpečnostné riziká* (ďalej len „BR“). Úlohou projektovania bezpečnosti utajovaných skutočností je minimalizovanie BR na požadovanú úroveň v závislosti od stupňa utajenia. Pretože v praxi nie je možné (alebo by bolo neúčelné z hľadiska vysokých nákladov) minimalizovať na nulu všetky BR je potrebné stanoviť *interval* (množinu), v ktorom sa BR môžu pohybovať (prípustné BR, miera BR). Opatrenia na zníženie BR na prijateľnú úroveň budú obsiahnuté v *bezpečnostnom štandarde* (ďalej len „BŠ“) pre daný SU v konkrétnom bezpečnostnom prostredí.

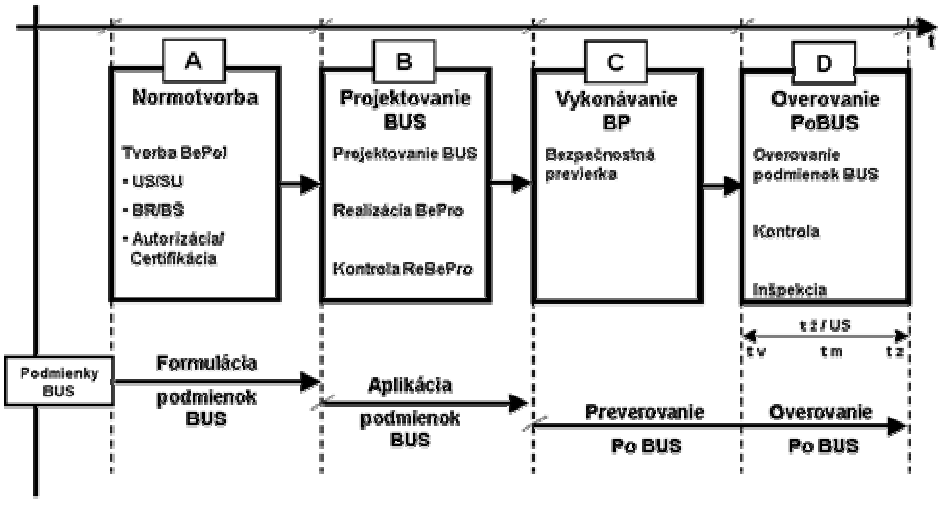
Ak sú známe BŠ potom je možné *projektovať* bezpečnosť US. Pri projektovaní je nutné, použiť na OUS daného SU len *technické prostriedky* certifikované v zhode s BŠ pre daný SU.

Po schválení *bezpečnostného projektu* príslušnou autoritou sa bezpečnostný projekt môže *zrealizovať*. *Bezpečnostnou previerkou* sa preveruje dodržanie nastavených BŠ vo všetkých oblastiach bezpečnosti (personálnej, objektovej a fyzickej, informačnej, administratívnej a u *podnikateľov* aj priemyselnej).

Po vydaní *certifikátu* osvedčujúceho bezpečnosť pre US daného SU na daný čas v konkrétnom prostredí je nevyhnutné *overovať* dodržiavanie podmienok bezpečnosti US až do ukončenia platnosti certifikátu.

Systém OUS SR sa vytvára v súlade s politikou bezpečnosti US SR. Politika bezpečnosti US SR sa odvádza od záujmov SR. Záujmy SR reprezentujú jednotlivé rezorty a v súlade s kompetenčným zákonom by mali formulovať aj BR.

Systém OUS môžeme vidieť z rôznych uhlov pohľadu v závislosti od toho, či chceme skúmať jeho fungovanie, riadenie, alebo zabezpečenie (obr.2). Možno ho však znázorniť aj ako sústavu nadväzných procesov *normotvorby*, *projektovania* BUS, *preverovania* podmienok BUS pred vydaním certifikátu a *overovania* podmienok BUS po jeho vydaní (obr.5).



Obrázok 5 - Proces OUS, jeho etapy a fázy

Procesy rozložené na etapy a fázy umožňujú presnejšie zadefinovanie zásad a odhaľovanie princípov OUS alebo lepšie pochopenie klasifikácie BR z rôznych hľadísk BUS.

Pri skúmaní jednotlivých zložiek (oblastí) bezpečnosti US ako cieľového stavu OUS, môžeme hovoriť o oblastiach personálnej (**PeB**), fyzickej a objektovej (**FOB**), informačnej (**IB**), administratívnej (**AB**) a u *podnikateľov* aj priemyselnej bezpečnosti (**PrB**).

Až konkrétna predstava o systéme OUS umožňuje vykonať systémovú analýzu, vidieť kardinálne problémy a študovať alternatívy ich riešení, umožňuje odhaľovať slabé miesta systému a nakoniec aj jeho optimalizáciu podľa zvolených kritérií.

US sa môžu vyskytovať na rôznych miestach SR, v štátnych a neštátnych inštitúciách alebo zariadeniach. Utajované skutočnosti teda spájajú rôzne oblasti vnútornej, či vonkajšej bezpečnosti, energetickej, jadrovej, enviromentálnej alebo iných druhov bezpečností. US prelínajú všetkými zložkami Bezpečnostného systému štátu a tvoria tak kostru národnej bezpečnosti.

Rezorty tvoriace bezpečnostný systém SR používajú rovnaké základné pojmy: bezpečnosť, bezpečnostné riziko, bezpečnostný štandard. Ich obsah je však často rozdielny.

Z uvedeného vyplýva, že nestačí povedať „bezpečnosť“, ale je nevyhnutné dopovedať aj bezpečnosť „čoho“. Predíde sa tým mnohým nezrovnalostiam, ku ktorým dnes ešte dochádza.

V tejto koncepcii sa rieši *bezpečnosť utajovaných skutočností*, preto sa musí hovoriť o bezpečnostných *štandardoch pre rôzne stupne utajenia* vytvorených na základe analýzy bezpečnostného prostredia SR charakterizovaného bezpečnostnými rizikami (BR).

Základná schéma sa dá použiť nielen na úrovni národnej ale aj medzinárodnej. V súčasnosti ju možno využiť pre posúdenie úrovne iných národných systémov OUS.

Problém OUS sa musí riešiť v *nehomogénnom* a *dynamicky* sa meniacom systéme. Z toho dôvodu treba prehodnotiť aj štruktúru, tvorbu a rozhodovanie o stupňoch utajenia US v zoznamoch US.

Utajované skutočnosti (veci alebo informácie) bude potrebné preskúmať vo všetkých variantoch pri postupovaní (vytváraní) medzi štátnymi (samosprávnymi) a podnikateľskými subjektami v národnom a medzinárodnom prostredí. *Utajované informácie* oddeliť od neutajovaných a riešiť ich systém bezpečnosti po *fázach* (vznik, spracovanie, prenos, ukladanie, archivácia) pre všetky *formy* (zvuk, obraz, dáta) pre všetky médiá (papier, elektromagnetické, optoelektronické, optické a iné médiá).

Bezpečnostné riziká sa vo všeobecnosti dynamicky menia v čase v závislosti od zmien bezpečnostného prostredia a vývoja technológií. V systéme OUS sú bezpečnostné riziká závislé predovšetkým na záujmoch SR ako výsledok pravdepodobnosti výskytu rizika a jeho následku. Veľkosť následku má pritom priamy súvis so stupňom utajenia. Ohrozenie US nastáva pri aktivovaní BR, ktorého dôsledkom môže byť samotné narušenie bezpečnosti US. Pretože záujmy SR a technológie sa budú meniť s časom, je nevyhnutné, aby aj systém posudzovania BR bol pružný. BR US je zároveň potrebné oddeliť od iných BR, ktoré nesúvisia s OUS. Vo všeobecnosti je potrebné na minimalizovanie BR formulovať protiopatrenia (preventívne, detekčné a eliminačné). Zámerom je, aby bezpečnostné riziká v jednotlivých oblastiach (bezpečnosť štátu, ochrana, obrana, hospodárske záujmy SR, zahraničné vzťahy) v budúcnosti sledovali a definovali odpovedajúce rezorty podľa svojich kompetencií. Taxatívne vymenovanie BR nikdy nepostihne aktuálny stav, ktorý sa dynamicky mení.

Bezpečnostné previerky (ďalej len BP) sa zo systémového hľadiska musia skúmať ako *proces* v troch fázach - *prípravy* na BP, *vykonávania* BP a *overovania* podmienok po vydaní potvrdenia (osvedčenia alebo certifikátu). Fáza prípravy na BP končí podaním žiadosti žiadateľa. Fáza vykonávania BP končí vydaním potvrdenia (osvedčenia alebo certifikátu).

Obsahom prvej fázy je všeobecne získavanie informácií od žiadateľov o previerku a projektovanie systému OUS v podmienkach žiadateľa (zatiaľ len u podnikateľov).

Obsahom druhej fázy je všeobecne analýza informácií získaných od žiadateľov a vyžiadaných od ostatných informačných zdrojov, overovanie dodržania bezpečnostných štandardov v rôznych oblastiach bezpečnosti (kontrola realizácie bezpečnostného projektu), certifikácia prostriedkov, posudzovanie bezpečnostných rizík a rozhodovanie o výsledku BP.

Obsahom tretej fázy je monitorovanie informácií o držiteľoch potvrdenia (osvedčenia alebo certifikátu), overovanie dodržiavania podmienok bezpečnosti US a kontrola OUS.

Fázovanie procesu BP nie je samoúčelné, ale poslúži k rozpracovaniu potrebných metodík a ich harmonizácii do optimálneho systému postupov. Vymedzenie množiny potrebných činností poslúži k formulovaniu požiadaviek na profily zamestnancov, ich počet a vytvorenie optimálnych organizačných štruktúr bez zbytočného navršovania, ale s potrebnou zálohou podľa prognózovaného vývoja.

Už dnes sa ukazuje, že spoľahlivý a komplexný systém OUS nie je možné dosiahnuť bez *projektovania* bezpečnosti US v konkrétnych podmienkach, hoci dnes sa požaduje len od podnikateľov. Otvárajú sa otázky kto je kvalifikovaný riešiť bezpečnostné projekty na OUS a v ktorej fáze BP treba požadovať ich realizáciu, či je korektné požadovať od podnikateľov vynaloženie finančných prostriedkov na realizáciu bezpečnostného projektu pred ukončením BP, a ďalšie. Jedným z cieľov v uvedenej oblasti je aj štrukturálna a pojmová harmonizácia bezpečnostných projektov jednotlivých oblastí bezpečnosti.

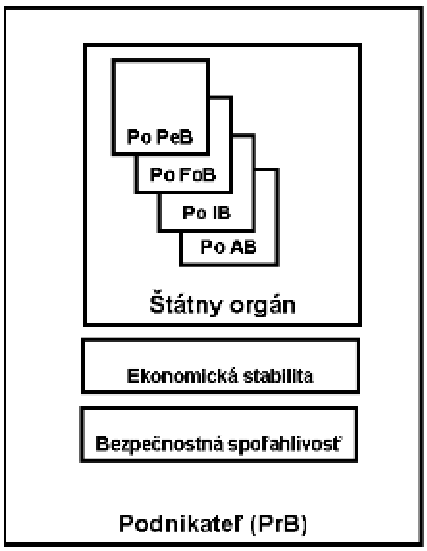
Pre exaktnosť ďalšieho skúmania a rozvoja systému OUS sa ukazuje nevyhnutné, aby úvodná časť koncepcie OUS tvorila základ pre budúci *terminologický slovník* OUS, ktorý sa bude rozvíjať spoločne s rozvojom teórie OUS a bude tým jednoduchší a kratší, čím hlbšie sa podarí preniknúť do podstaty vecí a javov.

V súčasnosti sa používajú niekedy zložité názvy výstupov z previerkového procesu (Potvrdenie o priemyselnej bezpečnosti, Osvedčenie na oboznamovanie sa s utajovanými skutočnosťami, a pod.). V súvislosti s tvorbou terminologického slovníka je len otázkou dohody, aký pojem sa bude používať do budúcnosti vo všetkých dokumentoch a legislatíve. Opäť platí, že hlbšie pochopenie procesu prinesie jednoduchšie a výstižnejšie pomenovanie jeho výstupov.

Oblasti bezpečnosti US

Bezpečnosť US sa všeobecne dosahuje *sústavou opatrení* v rôznych oblastiach bezpečnosti (personálnej, objektovej, informačnej, administratívnej). Po systémovej analýze však bude potrebné definovať oblasti bezpečnosti nielen ako „sústavu opatrení“, ale aj ako cieľový *stav* bezpečnosti US s jasnejšími hranicami. „Sústava opatrení“ musí byť lepšie previazaná s relatívne stálym, ale aj dynamicky sa meniacim bezpečnostným štandardom pre konkrétny stupeň utajenia. Dynamické zmeny môžu byť spôsobené zmenami v technológiách a záujmoch SR.

Zo systémového hľadiska možno vnímať oblasti bezpečnosti US ako *podsystémy* (obr.6). Ak sa má posudzovať BUS u podnikateľov (právnické osoby a fyzické osoby – živnostníci) potom hovoríme o priemyselnej bezpečnosti (ďalej len „PrB“).



Obrázok 6 - Podsystémy BUS

U podsystémov bezpečnosti (ďalej len „PoB“) bude potrebné formulovať ich účelové funkcie, vnútornú štruktúru (prvky) a vzájomné vzťahy. V snahe dosiahnuť súrodý systém bezpečnosti nestačí študovať jednotlivé oblasti len samostatne, ale aj vo vzťahu k iným oblastiam a to v národnom aj medzinárodnom prostredí. Bude potrebné prehodnotiť vstupy, vnútorné procedúry (postupy, metodiky, projekty, certifikáciu, systém riadenia) a výstupy. V podsystémoch treba rozlišovať *procesy* a ich jednotlivé fázy.

V súčasnosti odborné útvary úradu zodpovedajúce za jednotlivé oblasti bezpečnosti US vidia problémy OUS a spôsoby ich riešenia nasledovne:

Podsystém personálnej bezpečnosti

Personálna bezpečnosť (ďalej len **PeB**) sa dosahuje sústavou opatrení súvisiacou s výberom, určením a kontrolou osôb, ktoré sa oboznamujú v určenom rozsahu s utajovanými skutočnosťami. Účelom je identifikácia osôb, ktoré by mohli pre systém OUS predstavovať potenciálne riziko a ochrana utajovaných skutočností pred takýmito osobami, ktorými môže byť pôvodca, príjemca alebo prepravca. Na zabezpečenie OUS v oblasti PeB sa vykonávajú *bezpečnostné previerky osôb***,** ktoré majú byť určené na oboznamovanie sa s utajovanými skutočnosťami, pričom oprávnenie oboznamovať sa s utajovanými skutočnosťami je podmienkou pre výkon funkcie.

Zníženie počtu oprávnených osôb bez vykonania bezpečnostnej previerky

Členstvom Slovenskej republiky v NATO a EÚ sa vytvorili kvalitatívne nové predpoklady na realizáciu bezpečnostných záujmov a vývoj bezpečnostného prostredia. Z hľadiska PeB je potrebné vytvoriť podmienky, aby sa minimalizoval počet osôb oprávnených oboznamovať sa s utajovanými skutočnosťami bez vykonania bezpečnostnej previerky. Znížením počtu takýchto oprávnených osôb by sa zvýšila OUS a minimalizovalo by sa riziko postúpenia US osobám, ktorých bezpečnostná spoľahlivosť nebola posúdená v zmysle príslušných právnych predpisov. Vychádzajúc z bezpečnostných štandardov NATO a EÚ, k dodržiavaniu ktorých sa SR zaviazala, je podmienkou oboznamovania sa s utajovanými skutočnosťami v rámci týchto štruktúr vykonanie bezpečnostnej previerky bez ohľadu na to, v akom postavení navrhovaná osoba je.

Výber funkcií s požiadavkou bezpečnostnej previerky

Pre postupné znižovanie počtu preverovaných osôb, ktoré je vo výlučnej zodpovednosti vedúceho, je pri stanovovaní funkcií, pri ktorých je predpoklad oboznamovania sa s US potrebné uplatňovať zásadu „Need to know“. Výkon bezpečnostných previerok a činnosť úradu neslúži na overovanie spoľahlivosti zamestnancov. Zo strany vedúcich je preto potrebné pri uplatňovaní spomenutej zásady žiadať o vykonanie bezpečnostných previerok zamestnancov ako predpokladu pre výkon funkcie, ktorá je uvedená v zozname funkcií pri výkone ktorých sa oprávnené osoby môžu zoznamovať s utajovanými skutočnosťami. Rovnako je potrebné, aby vedúci žiadali pre navrhované osoby vykonanie bezpečnostnej previerky vyššieho stupňa len ak je reálny predpoklad, že navrhovaná osoba sa bude s US s tohto stupňa utajenia v budúcnosti oboznamovať.

Výkon bezpečnostných previerok

Právomoc vykonávať bezpečnostné previerky je zverená nielen Národnému bezpečnostnému úradu, ale vzhľadom na špecifiká činnosti aj Slovenskej informačnej službe, Vojenskému spravodajstvu a kriminálnemu spravodajstvu PZ SR. Vychádzajúc zo skutočnosti, že garantom ochrany utajovaných skutočností v Slovenskej republike vo vzťahu k NATO a EÚ je NBÚ, je žiaduce, aby vykonávanie bezpečnostných previerok, s výnimkou spravodajských zložiek a kriminálneho spravodajstva, bolo zverené do pôsobnosti úradu a súčasne, aby sa rozšírili jeho kompetencie v oblasti overovania predpokladov na oboznamovanie sa s utajovanými skutočnosťami, najmä pre stupeň utajenia Prísne tajné a Tajné, počas platnosti osvedčenia osôb.

Pružnosť reakcie na bezpečnostné hrozby

S ohľadom na bezpečnostnú stratégiu SR, ktorá sa zaoberá rozličnými hrozbami pre bezpečnostné prostredie, je potrebné reagovať na zmenu bezpečnostnej situácie a s tým súvisiacu zmenu bezpečnostných rizík tak, aby zohľadňovali reálny stav. Bezpečnostné riziká je potrebné rozšíriť ako na strategické globálne hrozby napr. terorizmus a šírenie zbraní hromadného ničenia, tak aj na priame hrozby, akou je organizovaný zločin vytvárajúci korupciu a nelegálnu ekonomiku. Na dosiahnutie tohto cieľa je nutný prechod od statického taxatívneho vymedzenia k dynamickému systému bezpečnostných rizík, ktoré by mohli byť flexibilne menené ako reakcie na zmeny hrozieb pre US.

Bezpečnostní zamestnanci

Osobitné miesto v podsystéme PeB zaujímajú bezpečnostní zamestnanci alebo osobitné pracoviská. Predstavujú výkonnú zložku v systéme ochrany utajovaných skutočností a preto je nevyhnutné upevňovať ich postavenie v organizačnej štruktúre, zvyšovať zodpovednosť, odbornú spôsobilosť a v konečnom dôsledku, vzhľadom na dôležitosť a náročnosť zverených úloh, zabezpečiť finančné zvýhodnenie, čo by malo vplyv aj na personálnu stabilizáciu.

Osobitné pracoviská plnia funkciu analytickú, plánovaciu, legislatívnu, metodickú, kontrolnú a vzdelávaciu. Mali by byť budované ako odborné organizačné útvary, ktorých výkon nie možné kumulovať s krízovým riadením, civilnou obranou alebo inou agendou priamo nesúvisiacou s OUS.

Podsystém fyzickej a objektovej bezpečnosti

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 na základe potreby vedieť. Opatreniami FOB sa identifikujú pokusy o vstupe narušiteľa a eliminujú sa bezpečnostné narušenia. FOB sa dosahuje aplikovaním mechanických zábranných prostriedkov (ďalej len „MZP“), technických zabezpečovacích prostriedkov (ďalej len „TZP“), fyzickej ochrany a režimových opatrení.

Realizácia opatrení fyzickej a objektovej bezpečnosti

Ochrana US z hľadiska FOB sa realizuje formou „hĺbkovej ochrany“ vo vrstvách. Vnútornú vrstvu tvoria opatrenia na ukladanie US, ďalšiu vrstvu tvoria opatrenia na ochranu chráneného priestoru, nasledujúcu vrstvu tvoria opatrenia na ochranu objektu a poslednú vrstvu tvoria opatrenia na ochranu perimetra.

Samotná realizácia opatrení FOB tvorí cyklus, ktorý pozostáva z jednotlivých procesov. Východiskom je špecifikácia aktív a následná identifikácia objektu a chráneného priestoru, kde majú byť umiestnené. Analýzou rizík sa identifikujú potenciálne riziká, klasifikujú sa, vyhodnotia sa a určí sa miera rizika ohrozenia US. Navrhnutím a prijatím vyvážených protiopatrení, ktoré zabezpečia minimálne požiadavky na ochranu US sa dosiahne optimalizácia finančných nákladov. Realizované opatrenia je nutné pravidelne monitorovať a vyhodnocovať. Na základe hodnotenia reálneho stavu je nutné operatívne realizovať nápravné opatrenia.

Pri určovaní primeraných a efektívnych opatrení FOB sa vychádza z hodnotenia rizika možného ohrozenia US, ktoré sa určuje po zhodnotení stupňa utajenia US, množstva a formy US, úrovne osvedčenia personálu a zhodnotenia ohrozenia US vonkajšími a vnútornými vplyvmi. Preto je prioritou uvážlivý manažment bezpečnostných rizík. Na NBÚ sa vytvorí analytické centrum špecializujúce sa na vykonávanie analýz rizík a následne vyhodnocovanie a navrhovanie optimálnych opatrení. Bude vypracovaná štúdia skúmajúca dostupné programové vybavenie a informačné databázy. Výsledkom bude vytvorenie funkčného systému hodnotenia rizík. Týmto sa dosiahne optimalizácia opatrení, stanovia sa najefektívnejšie metódy na odstránenie a elimináciu rizík, čím bude zaručená vysoká účinnosť a efektívnosť.

Opatrenia FOB predstavujú len jeden aspekt ochrany US a realizujú sa v kooperácii s opatreniami informačnej bezpečnosti, administratívnej bezpečnosti a personálnej bezpečnosti. Vyvážené aplikovanie jednotlivých opatrení zaručuje vysokú efektívnosť OUS.

Potreba harmonizácie legislatívy

Nakoľko legislatíva NATO a EÚ v oblasti FOB sa progresívne rozvíja, v nasledujúcom období bude žiadúca harmonizácia legislatívy SR s tým, že budú rešpektované špecifické požiadavky SR. Zreálnením vysokých stupňov utajenia utajovaných skutočností a ich počtu sa optimalizujú požiadavky na finančné a organizačné zabezpečenie OUS za oblasť FOB. Zmenou bezpečnostného štandardu sa spružní systém opatrení FOB. Posilní sa význam režimových opatrení a zvýši sa význam perimetrickej ochrany. Potreba fyzickej ochrany bude odvodená od reakčného času potrebného na prekonanie MZP a TZP a umožní sa používať najmodernejšie systémy. Zjednoduší sa bezpečnostná dokumentácia fyzickej bezpečnosti a objektovej bezpečnosti. Pre tento účel bude zriadená pracovná skupina vytvorená zo zástupcov NBÚ, ústredných orgánov štátnej správy a externých expertov. Pracovná skupina bude analyzovať všetky aspekty ovplyvňujúce opatrenia FOB pre jednotlivé formy US, a tiež špecifické podmienky vyplývajúce z činnosti ústredných orgánov štátnej správy a navrhovať optimálne opatrenia, ktoré sa následne premietnu do legislatívy.

Znalostné centrum

Dôležitým aspektom z hľadiska FOB je rýchly rozvoj nových technológií a veľké množstvo nových informácií. NBÚ vytvorí znalostné centrum pre hodnotenie rizík v podsystéme FOB, koncentrujúce všetky relevantné informácie o predpisoch v oblasti FOB, produktoch FOB, službách FOB a poskytujúce komplexné poradenské služby pri navrhovaní opatrení FOB. Znalostné centrum prispeje k vzájomnej koordinácii a integrácii výskumného a vývojového potenciálu SR v oblasti FOB a k zintenzívneniu medzinárodnej spolupráce. Dosiahnuté výsledky sa budú aplikovať na národnej a medzinárodnej úrovni v procese tvorby bezpečnostných štandardov, smerníc NATO, EÚ a v procese normotvorby. Pre dosiahnutie tohto cieľa sa bude formou štúdie analyzovať súčasný stav a budú integrovaní špecialisti. V krátkodobom horizonte sa problematika bude riešiť spoluprácou s akademickou obcou a vysokými školami.

V oblasti overovania bezpečnostných parametrov MZP a TZP sa zintenzívni spolupráca s autorizovanými osobami a oblasť autorizácie sa rozšíri aj na iné oblasti. V oblasti certifikácie sa úsilie sústredí na spoluprácu so zahraničnými certifikačnými autoritami a na intenzívnu prácu v oblasti normotvorby.

Pre financovanie činností, služieb, aktivít a programov riešenia výskumných a vývojových programov bude potrebné nájsť zdroje v štátnom rozpočte SR a využiť granty EÚ, resp. operačné programy EÚ.

Podsystém informačnej bezpečnosti

Informačná bezpečnosť (ďalej len **IB**) v systéme OUS sa v uplynulom období rozvíjala bez existencie jednotnej koncepcie, ktorá by komplexne zastrešovala celú problematiku s ohľadom na ciele, postupy a financovanie. Dôsledky sa prejavili v tom, že bola prijatá legislatíva, ktorá obsahuje len fragmenty IB a v tom, že hlavná pozornosť sa sústredila na plnenie povinností vyplývajúcich zo zmlúv s NATO a EÚ.

Legislatíva EÚ v oblasti IB je v porovnaní s inými oblasťami pomerne dobre rozpracovaná, ale zároveň najrozsiahlejšia. V nasledujúcom období je preto nevyhnutné ustanoviť pracovné skupiny vytvorené z pracovníkov NBÚ, ÚOŠS a externých špecialistov. Ich náplňou bude vykonanie analýzy právneho stavu predpisov IB NATO, EÚ a noriem IB, ich porovnanie s národnou legislatívou v oblasti IB a vytvorenie novej národnej legislatívy kompatibilnej so zahraničnou.

Informačná bezpečnosť utajovaných informácií (ďalej len „UI“) sa dosahuje aplikovaním bezpečnostných opatrení z oblasti počítačovej a komunikačnej, kryptografickej a emisnej bezpečnosti na ochranu utajovaných informácií spracovávaných, uchovávaných, zobrazovaných alebo prenášaných v komunikačných, informačných a iných elektronických systémoch proti náhodnej, nedbanlivostnej alebo úmyselnej strate dôvernosti, integrity alebo dostupnosti ako aj proti strate integrity a dostupnosti samotných systémov a opatreniami zamedzujúcimi popretie vykonanej operácie, resp. služby (non-repudiation).

Na dosiahnutie dôvernosti, integrity, autenticity a dostupnosti utajovaných informácií ukladaných, spracovávaných, zobrazovaných a prenášaných v komunikačných, informačných a iných elektronických systémoch musia byť vyvážene implementované opatrenia z oblasti informačnej bezpečnosti, fyzickej bezpečnosti a objektovej bezpečnosti, personálnej bezpečnosti, priemyselnej bezpečnosti a administratívnej bezpečnosti UI v elektronickej forme.

V rámci zabezpečenia interoperability SR s krajinami NATO a EÚ je budúcnosť medzinárodnej aj národnej výmeny UI v ich bezpapierovej forme. Prechod z papierovej formy na bezpapierovú má

za následok zmenu prostredia, v ktorom sa UI doteraz nachádzajú. To prinesie so sebou aj výrazné zmeny v evidencii a manipulácií s UI.

Budovanie IB tvorí uzavretý cyklus. Tento cyklus pozostáva z nasledovných samostatných procesov, ktoré na seba úzko nadväzujú. Vynechanie ktoréhokoľvek z nich znamená degradáciu úrovne celej IB.

Pri budovaní IB sa vychádza z **definovania informačných aktív,** ich vlastníctva a zodpovedností pri ich využívaní. Významnú úlohu zohráva i prostredie, v ktorom sú informačné aktíva umiestené.

Na tento proces nadväzuje **bezpečnostná analýza rizík**, ktorá definuje hodnotu informačných aktív, identifikuje potenciálne hrozby a zraniteľnosti a stanovuje úrovne rizík.

Jedným z najvýznamnejších nástrojov eliminujúcich hrozby, súvisiace s ľudským faktorom je stanovenie **bezpečnostnej politiky**, ktorej súčasťou je aj proces budovania **bezpečnostného povedomia a permanentného vzdelávania.** Je potrebné zriadiť ucelený systém vzdelávania s previazaním na výskum a realizačné pracoviská so zvláštnym zreteľom na silové rezorty. Koordináciu vzdelávania audítorov bezpečnosti informačných systémov najmä pre štátne orgány plniace úlohy na úseku bezpečnosti štátu bude vykonávať národná autorita na úseku OUS.

Stanovenie vhodnej **bezpečnostnej architektúry a jej implementácia** má výrazný vplyv na úroveň IB a následne na efektivitu vynaložených prostriedkov. Na riešenie problematiky informačnej bezpečnosti bude potrebné zaviesť a uplatňovať pravidlo účelového viazania rozpočtových prostriedkov.

Integrálnou súčasťou vybudovanej bezpečnostnej architektúry musí byť **správa bezpečnosti.**

Nevyhnutnými nástrojmi na dosiahnutie a udržanie požadovanej úrovne IB sú **monitoring** prevádzky, **audit** systému a **kontrola** jednotlivých prvkov informačných systémov (IS).

Z hľadiska požadovanej funkcionality systému je nutná adekvátna reakcia na **bezpečnostné incidenty** a **náprava** ich následkov v reálnom čase.

V súvislosti s certifikáciou technických prostriedkov a šifrových prostriedkov a s analyzovaním bezpečnostných incidentov bude potrebné inštitucionalizovať zabezpečenie týchto činností, v nadväznosti na systém medzinárodných inštitúcií.

Na základe analýzy stavu informačnej bezpečnosti na Slovensku a uvedených procesov boli identifikované nasledovné hlavné problémy, ktoré je potrebné riešiť v krátkodobom, resp. strednodobom horizonte:

Bezpečné produkty pre IS

V súčasnosti existuje zreteľná deliaca čiara medzi produktmi v oblasti US na spracovanie a prenos informácií v národnom prostredí a produktmi pre použitie na spracovanie a prenos informácií NATO a EÚ. Popri národnom výskume, vývoji a výrobe prostriedkov, ktorý nepokrýva celý rozsah požadovaných produktov pre prenos a spracovanie informácií, bude potrebné investovať značné prostriedky do dovozu certifikovaných bezpečnostných produktov. Pritom ide o prostriedky s vysokým pomerom ceny k výrobným nákladom, t.j. ide o typické produkty znalostnej ekonomiky. Slovenskí výrobcovia nie sú v súčasnosti schopní zabezpečiť kompletný rozsah produktov a služieb pre IB.

Je preto nevyhnutné prednostne rozvíjať vybrané oblasti ochrany US v oblasti IB patriace do znalostnej ekonomiky. Za týmto účelom bude nevyhnutné podporiť výskumný a vývojový potenciál SR v oblasti prostriedkov pre US s prednostnou orientáciou na produkty perspektívne certifikovateľné v certifikačných orgánoch NATO a EÚ a integrovať ho s výrobou.

Backbone (chrbticová sieť)

Systémy prenosu UI v SR vznikali podľa potreby bez vzájomnej koordinácie jednotlivých projektov. Na základe existujúcej legislatívy resp. zmlúv, podľa ktorých boli tieto systémy vybudované nie je možné v mnohých prípadoch stanoviť zodpovednosť za prevádzku resp. správu, dohľad a bezpečnosť.

Problémy, ktoré vznikli ako následok súčasnej praxe sú absencia štátnej politiky prenosových systémov pre utajované informácie a dostatočnej legislatívy, neurčitosť pri stanovení zodpovednosti za prevádzku, správu, dohľad a bezpečnosť, chýbajúca alebo nedostatočná zálohovateľnosť systémov, vysoké náklady na zriadenie a prevádzku ako aj nedostatočný stav personálu a jeho odborná príprava.

Je preto nevyhnutné vytvoriť jednotný systém prenosu a elektronickej registratúry UI a vybudovať personálne aj materiálne sieťovú zložku IB.

Infocentrum, znalostné centrum

V súčasnosti neexistuje referenčné miesto, ktoré by obsahovalo všetky relevantné informácie o predpisoch, produktoch a službách v oblasti IB a poskytovalo komplexné poradenské služby pri navrhovaní IS pre UI.

Rýchly postup v inováciách v oblasti informačných technológií vyžaduje odborne zdatný personál a nepretržité sledovanie vývoja v oblasti štandardizácie, v oblasti trendov vývoja nových produktov a ich bezpečnostného posudzovania (certifikácie). Okrem toho treba zabezpečiť prenos predpisov a noriem do prostredia SR a v rade prípadov aj zapojenie sa do riešiteľských a overovacích tímov.

NBÚ preto vytvorí pre IB v oblasti OUS databázu metodík, štandardov a súvisiacich predpisov. Bude to vyžadovať personálne posilnenie, doriešenie adekvátnej nominácie zástupcov SR v pracovných orgánoch NATO a EÚ, zabezpečenie finančných zdrojov pre účasť v pracovných orgánoch a vytvorenie systému prenosu štandardov do prostredia SR.

S uvedeným súvisí vybudovanie laboratórií na overovanie vlastností produktov a systémov. Ako podporná činnosť sa využije medzinárodná spolupráca s renomovanými pracoviskami. Vážnym problémom je absencia uceleného systému vzdelávania s previazaním na výskum a realizačné pracoviská.

Vybudovaním znalostného centra môže SR prevziať v budúcnosti úlohu kontaktného a certifikačného miesta (napr. pre oblasť TEMPEST) pre vybrané krajiny NATO.

Národná a rezortná autorita bezpečnosti informačných systémov a Národná autorita na ochranu pred nežiadúcim elektromagnetickým vyžarovaním

Informačná bezpečnosť (INFOSEC-Information Security) sa člení na komunikačnú bezpečnosť (COMSEC-Communication Security), počítačovú bezpečnosť (COMPUSEC-Computer Security) a na ochranu pred nežiadúcim elektromagnetickým žiarením (EMSEC-Emission Security).

V súčasnom systéme ochrany UI v SR oblasť komunikačnej bezpečnosti pokrývajú ústredný šifrový orgán (UŠO) a rezortné šifrové orgány (REŠO). UŠO vystupuje voči NATO a EÚ ako NCSA (National Communication Security Authority).

V systéme ochrany UI v SR je nevyhnutné pokryť všetky oblasti informačnej bezpečnosti a ustanoviť Národnú autoritu bezpečnosti informačných systémov (NABIS) a Rezortnú autoritu bezpečnosti informačných systémov (RABIS). NABIS by vystupovala voči NATO a EÚ ako NISSA (National Information System Security Authority), čím by bola splnená aj požiadavka Rady EÚ na nomináciu NISSA v súvislosti s pripravovaným dokumentom GENERAL INFOSEC POLICY (GEN-P) Rady EÚ.

Analogicky na zabezpečenie ochrany pred NEV ustanoviť Národnú autoritu na ochranu pred nežiadúcim elektromagnetickým vyžarovaním a v priestoroch NBÚ vybudovať špecializované pracovisko na meranie NEV.

Vytvoriť podmienky na praktickú realizáciu proti hrozbám vyplývajúcim z NEV. Pritom metodicky upraviť túto oblasť tak, aby náklady bolo možné optimalizovať s ohľadom na priestorové podmienky a vlastnosti technického prostriedku.

Evaluačná autorita na hodnotenie bezpečnostných produktov informačných a komunikačných technológií

Implementácii bezpečnostného prvku do systému spracovania a prenosu utajovaných informácií musí v požadovaných prípadoch predchádzať jeho certifikácia t.j. posúdenie jeho vlastností vo vzťahu k bezpečnostným štandardom a jeho schopnosti ochrániť informácie pred neoprávnenou manipuláciou. Vzhľadom na veľký rozsah používaných produktov je zrejmé, že v podmienkach SR nie je možné vybudovať univerzálnu inštitúciu, ktorá by zabezpečila evaluáciu bezpečnostných produktov.

Riešením je ustanovenie siete profesionálnych evaluačných pracovísk, zabezpečujúcich posudzovanie resp. audit produktov s cieľom ich následnej certifikácie uznávanou certifikačnou autoritou. Táto autorita by zároveň bola oprávnená uznať po preskúmaní certifikáty obdobných zahraničných autorít.

Tím pre hodnotenie bezpečnosti IS

Pre realizáciu niektorých špecializovaných aktivít v oblasti bezpečnosti UI (audity, analýzy rizík a pod.) sú nevyhnutné tímy špecialistov s vysokou odbornosťou. Pre vybudovanie takéhoto tímu je nutné vyriešiť personálne obsadenie, získať špecializované nástroje (napr. na analýzu rizík a pod.), ich domestifikáciu a realizovať špecializovanú prípravu personálu s periodickým preskúšavaním. Vo viacerých prípadoch bude nutné získať aj medzinárodne platný certifikát.

Budovať takéto tímy všade tam, kde sú potrebné je nielen ekonomicky neefektívne s ohľadom na ich plnú využiteľnosť, ale aj problematické s ohľadom na nutnosť nepretržitého výkonu činností v záujme udržania vedomostného potenciálu a praktických návykov. Okruh aktivít tímu a pôsobnosť vo vzťahu k vybraným orgánom štátnej správy bude určená v štúdii..

Analýza bezpečnostných incidentov IS

Narastajúca kriminalita v oblasti informačných technológií na jednej strane a prakticky beztrestnosť na strane druhej vytvárajú nedôveru k elektronickému spracovaniu dát resp. jeho zneužívanie. S tým úzko súvisí aj dôveryhodnosť príslušných orgánov v SR i vo vzťahu k zahraničným partnerom. Absencia systému analýzy incidentov a s tým súvisiaca zložitosť dokazovania tejto trestnej činnosti má priamy dopad na dôveryhodnosť inštitúcií a úroveň ochrany UI.

Preto je nutné vybudovať kapacity na analýzy incidentov so zapojením sa do medzinárodnej spolupráce. Spojením budovania systému analýzy incidentov a špeciálnych služieb (audity, analýzy rizík a pod.) vznikne silná odborná základňa pre radikálne zvýšenie informačnej bezpečnosti v oblasti UI pri minimalizácii nákladov. Budovanie týchto aktivít vyžaduje doplniť personálne obsadenie (možno integrovať so špeciálnymi službami), špeciálne technologické vybavenie, zodpovedajúce legislatívne zabezpečenie ako aj nadviazať medzinárodnú spoluprácu. Materiálne a organizačné zabezpečenie bude riešené po vypracovaní analytickej štúdie pre predmetnú oblasť.

Riešenie bezpečnostných incidentov

V SR neexistuje inštitúcia, ktorá by poskytla kvalifikovanú podporu používateľom informačných technológií OUS pri riešení následkov bezpečnostného incidentu pri jeho vzniku, v priebehu alebo po skončení. Neadekvátne správanie sa subjektu zvyšuje úroveň materiálnych i nemateriálnych škôd. V rade prípadov sú procesy poškodenia nevratné.

Vybudovanie systému reakcií na bezpečnostné incidenty v súlade s medzinárodnými predpismi a zvyklosťami a zapojenie sa do medzinárodnej spolupráce je preto nevyhnutné.

Zdroje

Pre financovanie činností, služieb, aktivít a programov pre zabezpečenie požadovanej úrovne je nutné nájsť zdroje v štátnom rozpočte SR a využiť granty EÚ, resp. operačné programy EÚ, ale aj analyzovať možnosti združovania prostriedkov rezortov.

Časový plán realizácie

Každá uvedená problematika IB pre OUS bude mať spracovanú analytickú štúdiu a podrobný plán realizácie, kde budú spresnené požiadavky na materiálne, technické, finančné a personálne zabezpečenie. Každý plán realizácie bude obsahovať finančnú analýzu s uvedením porovnania súčasného stavu a minimálnych potrieb.

- Do jedného roku po schválení koncepcie OUS – vypracovanie plánu realizácie.
- Do 5 rokov realizácia jednotlivých koncepčných problematík.

Podporné aktivity

Pre zvyšovanie odbornej úrovne vlastných pracovníkov formou školení, seminárov, prípadne stáží a postgraduálneho štúdia a na úhradu prác externých špecialistov v maximálnej miere využiť zdroje grantov EÚ.

Podsystém administratívnej bezpečnosti

Administratívna bezpečnosť (ďalej len **AB**) sa dosahuje súborom opatrení, realizáciou postupov a zásad oprávnenými osobami v časovo ohraničenom období (doba života utajovanej písomnosti), cieľom ktorých je minimalizovanie bezpečnostných rizík US a ohrozenia pred nepovolanými osobami a cudzou mocou. Doba života utajovanej písomnosti (ďalej len UP) je ohraničená vznikom UP (vytvorením) a fyzickým zničením alebo zrušením stupňa utajenia UP v rámci jej vyraďovania.

Určovanie stupňa utajenia a vytváranie zoznamov utajovaných skutočností

Pri vzniku UP vystupuje do popredia otázka určovania stupňa utajenia UP. Na základe praktických skúseností z procesu vytvárania zoznamov US v pôsobnosti ústredných orgánov štátnej správy a súčasného stavu, kedy zoznam US vydávaný vedúcim nemá charakter všeobecne záväzného právneho predpisu, je v budúcnosti potrebné pristúpiť k vytvoreniu konkrétnych okruhov.

Vymedzenie konkrétnych okruhov US smeruje k vytvoreniu efektívneho systému, ktorý by zabránil účelovému utajovaniu písomností, resp. vylúčil zbavenia sa zodpovednosti v prípade neoprávnenej manipulácie s poukázaním na skutočnosť, že bol nesprávne určený stupeň utajenia

a vytvoril podmienky pre špecifikovanie kritérií a postupov na zabezpečenie objektívneho výberu, triedenia a kvantifikovania stupňov a lehôt utajenia US v priamej väzbe na záujmy SR.

Existujúce zoznamy US budú harmonizované v krátkodobom horizonte a upravované v strednodobom horizonte zároveň s oblasťami, v ktorých sa predpokladá vznik US.

Tento cieľ je možné zabezpečiť spracovaním zoznamov US formou všeobecne záväzného právneho predpisu, ktorý zabezpečí zvýšenie právnej istoty pri vymedzení US, ich jednoznačné obsahové začlenenie do definovaných okruhov činnosti štátnych orgánov.

Neoprávnená manipulácia

Dôsledným sledovaním bezpečnostných rizík v oblasti administratívnej bezpečnosti sa zabezpečí eliminácia porušení právnych predpisov v oblasti OUS smerujúcich k vyzradeniu, zneužitiu, poškodeniu, neoprávnenému rozmnoženiu, zničeniu, strate alebo odcudzeniu US, ktoré je definované ako neoprávnená manipulácia.

Efektívne prešetrovanie a objasňovanie príčin neoprávnenej manipulácie je podmienené presným obsahovým vymedzením predtým uvedených pojmov, ich aktualizáciou s prihliadnutím na vývoj v oblasti ochrany utajovaných skutočností.

Väzby na ostatné oblasti bezpečnosti

Z hľadiska eliminácie bezpečnostných rizík je potrebné vytvárať aktívne väzby aj na ostatné oblasti bezpečnosti. V prípade uloženia a uschovávania UP ide o aktívnu väzbu na oblasť fyzickej a objektovej bezpečnosti. Nesprávna manipulácia s UP zo strany oprávnenej osoby je priamym prepojením administratívnej bezpečnosti s oblasťou personálnej bezpečnosti. Väzba medzi administratívnou bezpečnosťou a priemyselnou bezpečnosťou je vytváraná v prípadoch protizákonného využívania postúpených utajovaných písomností podnikateľom. Vzťah medzi administratívnou bezpečnosťou a informačnou bezpečnosťou vrátane bezpečnosti technických prostriedkov je vytváraný v procese spracovávania UP na necertifikovaných technických prostriedkoch a porušovaní zásad informačnej bezpečnosti. Udržiavanie funkčného systému OUS do budúcnosti vyžaduje neustále sledovanie interakcie jednotlivých oblastí bezpečnosti.

Interné predpisy

Ďalším z prvkov v procese OUS, ktorý je potrebné riešiť je spracovanie a vydávanie interných predpisov ústredných orgánov štátnej správy upravujúcich OUS na vlastné podmienky, ktoré často nekorešpondujú v plnom rozsahu so všeobecne záväznými právnymi predpismi vydanými v oblasti OUS. Týmto sa vytvárajú podmienky pre rozdielnu aplikáciu uvedených predpisov zo strany oprávnených osôb a následne dochádza k narušeniu OUS v rámci daného subjektu, ktoré môžu spôsobiť neoprávnenú manipuláciu. NBÚ bude dôsledne presadzovať koordinačnú a metodickú úlohu, pričom budú rešpektovať výnimky vyplývajúce zo špecifického postavenia spravodajských služieb.

Riešenie priestupkov v oblasti OUS

Súčasná právna úprava postupu riešenia priestupkov v oblasti OUS predstavuje zdĺhavý postup a vylučuje efekt rýchleho riešenia nezákonného stavu. Z hľadiska docielenia pružnosti systému OUS je potrebné rozpracovať špecifické procesné postupy pri riešení priestupkov v oblasti OUS, ktoré musia vychádzať zo zásady neodkladnosti OUS priamo vo vzťahu k US, k osobám manipulujúcim s US a k subjektom, ktoré manipulujú s US.

Tieto postupy musia jednoznačne zadefinovať vymedzenie skutkovej podstaty priestupkov a správnych deliktov v oblasti OUS z hľadiska ich závažnosti a súčasne zabezpečiť plánovanú dynamiku rozvoja OUS.

Centrálny register

Zabezpečenie ochrany US vymieňaných v súlade s uzatvorenými medzinárodnými dohodami realizuje pracovisko centrálneho registra (ďalej len „CR“), prostredníctvom ktorého sú US poskytované zahraničným partnerom a zároveň prijímané zo zahraničia. Plnenie úloh CR je vykonávané na základe platných všeobecne záväzných právnych predpisov SR a aplikácii bezpečnostných predpisov NATO a EÚ. Uvedená skutočnosť vyžaduje priebežné a aktívne sledovanie zahraničných ako aj medzinárodných bezpečnostných predpisov v oblasti ochrany US.

Správne fungovanie CR si vyžiada zefektívnenie štruktúry registra i samotného spôsobu výmeny zahraničných UI v podmienkach systému elektronickej výmeny informácií.

V rámci plnenia úloh CR je potrebné vlastnou metodickou činnosťou vytvoriť podmienky pre implementáciu vybraných prvkov bezpečnostných predpisov EÚ a NATO obsahujúcich aj tzv. zvláštne pokyny. Rozvoj metodiky v oblasti vykonávania poučení osôb predpokladá priebežnú aktívnu aplikáciu prvkov zameraných na predchádzanie možných hrozieb vyplývajúcich z bezpečnostných rizík tam, kde si to vyžaduje práca s US.

Súčasne bude v oblasti OUS kladený dôraz na odborný rast všetkých osôb prichádzajúcich do styku s predstaviteľmi krajín, ktorých spravodajské služby sa zameriavajú na EÚ, NATO a členské štáty pokiaľ ide o tajné informácie a aktivity EÚ, NATO.

V súlade s bezpečnostnými predpismi EÚ a NATO je potrebné v rámci koordinácie zabezpečiť rozšírenie a po vzájomnej dohode v súčinnosti so spravodajskými službami aj vykonávanie takejto metodickej činnosti resp. poučení.

CR v spolupráci s príslušnými bezpečnostnými zložkami SR vypracuje v horizonte rokov 2007 až 2009 odborné postupy zamerané na:

(a) nebezpečenstvo vznikajúce z nediskrétneho rozhovoru;
(b) opatrenia vo vzťahu k informačným médiám;
(c) ohrozenia, ktoré predstavujú aktivity spravodajských služieb, ktoré sa zameriavajú na EÚ, resp. NATO a členské štáty pokiaľ ide o tajné informácie a aktivity EÚ, NATO;
(d) povinnosť okamžite informovať príslušné bezpečnostné orgány o akomkoľvek prístupe alebo manévri, ktorý vedie k podozreniam z vyzvedania, vyzradenia či zneužitia US alebo o akýchkoľvek nezvyčajných okolnostiach týkajúcich sa bezpečnosti utajovaných skutočností.

Certifikáty NATO a EÚ

V súvislosti s vydávaním certifikátov EÚ a NATO je potrebné pristupovať k analýze a aplikácii systémového prístupu k existujúcim bezpečnostným predpisom mimo SR a tieto využívať pri príprave legislatívnych zmien. V oblasti bezpečnostných štandardov je potrebné docieliť špecifikáciu týchto štandardov pre oboznamovanie sa s US jednotlivých zoskupení.

Na základe hodnotenia súčasne platného právneho stavu je nevyhnutné vypracovanie legislatívnych a technických analýz pre vystavenie certifikátu ak o to požiada fyzická osoba.

S danou oblasťou úzko súvisí oblasť preukazovania platnosti certifikátu. Ide najmä o stav, keď osoby, ktorým zanikne pracovnoprávny, služobný alebo obdobný vzťah a certifikát si ponechajú v osobnej dispozícii. Odstránenie uvedenej disproporcie podmieňuje vypracovanie efektívneho riešenia v krátkodobom horizonte.

Národný ekvivalent EÚ LIMITÉ a NATO UNCLASIFIED

V slovenskej legislatíve existuje nepokrytý priestor medzi utajovanými skutočnosťami a všetkými ostatnými neutajovanými informáciami. Ide o informácie, ktoré nie je nutné ochraňovať utajením, existujú však jasne definované dôvody, pre ktoré sú možnosti manipulácie obmedzené (napr. zákaz zverejnenia, alebo poskytnutia tretej strane). Ide najmä o „citlivé“ interné údaje (napr. zápisy pracovných porád), alebo potenciálne zneužiteľné informácie (napr. pri teroristickom útoku).

Potreba systémového riešenia (inštitucionalizácie) v tejto oblasti úzko súvisí aj so vstupmi zo systémového okolia – neutajovanými informáciami s obmedzenou možnosťou manipulácie, ktoré SR prijíma z inštitúcií či orgánov EÚ a NATO. Napriek tomu, že nejde o utajované informácie, na ktoré by sa vzťahovali bezpečnostné štandardy NATO a EÚ platné pre US, tieto dokumenty nie sú všeobecne zverejniteľné (sú označované ako LIMITÉ EU, resp. NATO UNCLASSIFIED). Manipulovať s nimi možno len pri zachovaní integrity (nemožno meniť ich obsah) a dostupnosti (vždy musí byť jasné kto ich komu poskytuje).

Vzhľadom na to, že vo vzťahu k EÚ a NATO je NBÚ garantom dodržiavania zásad manipulácie s ich informáciami a SR pristúpila na dodržiavanie ich záväzných noriem, ukazuje sa ako nevyhnutné zaviesť do slovenského právneho poriadku pod gesciou úradu mechanizmy ich ochrany.

Vytvoreniu národného ekvivalentu musí predchádzať vnútorná diskusia na úrovni úradu i externá diskusia s rezortmi. Z diskusií vyplynie rozhodnutie, či sa táto oblasť stane platnou súčasťou systému OUS, alebo bude riešená samostatne mimo jeho rámca. V oboch prípadoch je potrebné rozhodnúť o forme právnej úpravy (novelizácia zákonov 215/2004 o OUS a 211/2000 o slobodnom prístupe k informáciám a novelizácia, prípadne úprava vyhlášky o administratívnej bezpečnosti), určiť mieru zodpovednosti úradu a vedúcich, implementovať súvisiace normy EÚ a NATO, stanoviť oblasti, ktorých sa to bude týkať, vytvoriť kompaktný systém manipulácie a evidencie a spracovať metodické pomôcky pre externé prostredie.

Utajované písomnosti v elektronickej podobe

Zvyšovanie podielu utajovaných písomností v elektronickej podobe vytvára požiadavku na spracovanie novej právnej úpravy, ktorá bude riešiť manipuláciu s UP v elektronickej podobe a ich následnú archiváciu v prípade trvalej dokumentárnej hodnoty.

Podsystém priemyselnej bezpečnosti

Priemyselná bezpečnosť (ďalej len **PrB**) sa dosahuje u podnikateľa sústavou opatrení na OUS, ktoré mu boli odovzdané, alebo ktoré u neho vznikli. Vydanie potvrdenia, ako aj jeho platnosť, je viazaná na spĺňanie podmienok priemyselnej bezpečnosti (spôsobilosť zabezpečiť ochranu utajovaných skutočností, ekonomickú stabilitu a bezpečnostnú spoľahlivosť). Výkon bezpečnostnej previerky podnikateľov je zverený výlučne do právomocí úradu a to pre všetky stupne utajenia.

Posudzovanie bezpečnostnej spoľahlivosti

Oblasťou, ktorú je nutné posudzovať v rámci systémového prístupu k celému bezpečnostnému prostrediu SR je problematika bezpečnostných rizík, ich tvorba, analýza a vyhodnocovanie v rámci výkonu bezpečnostných previerok či už fyzických osôb alebo podnikateľov. Táto problematika je v súčasnom zákone zahrnutá pod pojem bezpečnostná spoľahlivosť, tak u podnikateľov ako aj u fyzických osôb. Zákon v súčasnej podobe stanovuje riziká, pri naplnení ktorých je podnikateľ posudzovaný ako bezpečnostne nespoľahlivý.

V oblasti posudzovania bezpečnostných rizík je potrebné ustanoviť možnosť vyvodenia dôsledkov z konania vlastníka podnikateľa, ktorý nie je zastúpený v štatutárnom orgáne spoločnosti, pričom jeho praktické konanie v mene spoločnosti nesie znaky bezpečnostného rizika.

Súhrnným problémom pre oblasť bezpečnostných rizík je fakt, že v rámci zákona nie je jednoducho možné stanoviť také detailné riziká, aby spĺňali podmienku čo najväčšej konkretizácie so súčasnou potrebou reagovať na aktuálny vývoj v oblasti definovania bezpečnostných rizík. V rámci existencie predovšetkým nevojenských, dynamicky sa meniacich rizík je prvoradým záujmom štátu a štátnych orgánov stanoviť predovšetkým riziká reagujúce na aktuálny vývoj v oblasti definovania a vnímania bezpečnostných rizík v spoločnosti, ako aj partnerských medzinárodných organizáciách, pričom podmienka ich detailnosti a čo najväčšej konkretizácie je až druhoradá. Riešením je nadefinovanie bezpečnostných rizík štátnymi orgánmi podľa ich kompetencií v oblasti obrany, bezpečnosti, zahraničných vzťahov, hospodárskych záujmov a ďalších v spolupráci s expertmi z úradu ako aj zo spravodajských služieb. Takýmto postupom sa prinajmenšom zachová až zvýši transparentnosť rozhodovania úradu, predovšetkým v sporných prípadoch, ale aj spružní proces definovania bezpečnostných rizík, čo umožní pomerne rýchlo reagovať na aktuálny vývoj v danej oblasti.

Overovanie podmienok priemyselnej bezpečnosti

Pomerne významnou je aj oblasť overovania podmienok priemyselnej bezpečnosti úradom. Vydaním potvrdenia pre podnikateľa totiž úrad deklaruje ostatným štátnym orgánom, že podnikateľ spĺňa všetky podmienky priemyselnej bezpečnosti. To sa týka aj podnikateľov, uchádzajúcich sa o zákazky medzinárodných organizácií. Ustanovenia v súčasnosti platného zákona týkajúce sa priemyselnej bezpečnosti neposkytujú úradu v potrebnej miere možnosť overovania, či podnikateľ naďalej spĺňa zákonom dané podmienky. V súvislosti s rastúcim množstvom už preverených podnikateľov bude vzrastať potreba vykonávania týchto činností a to aj zo strany medzinárodných organizácií, resp. inštitúcií. S prihliadnutím na reálne predpoklady čoraz väčšieho zapojenia sa slovenských podnikateľov do zákaziek v medzinárodnom meradle je žiadúce aby kompetencie overovania podmienok priemyselnej bezpečnosti po vydaní potvrdenia, ako aj v oblasti ich preverovania v procese previerky boli rozšírené.

Posudzovanie ekonomickej stability

Oblasťou, ktorej význam v súčasnosti rastie hlavne v medzinárodnom meradle je oblasť posudzovania ekonomickej stability podnikateľa. Platná slovenská legislatíva sa obmedzuje len na skúmanie a konštatovanie stavu, ohľadne plnenia si povinností týkajúcich sa platobnej disciplíny podnikateľa. Neumožňuje však na základe objektívnych a v zahraničí uznávaných ekonomických analýz skonštatovať ohrozenú ekonomickú existenciu firmy a z toho vyvodiť závery o ekonomickej nestabilite podnikateľa. Postavenie podnikateľa, ktorý nepožíva dôveru ostatných podnikateľských subjektov, jeho ekonomické výsledky nie sú dobré pritom nastoľuje otázku, či má mať dôveru štátu v prípade postupovania utajovaných skutočností. Nakoľko už v súčasnosti je možné jednoznačne stanoviť aké ekonomické ukazovatele ohrozujú ekonomickú stabilitu podnikateľa, je nutné stanoviť ich vplyv na výsledok bezpečnostnej previerky podnikateľa.

Medzinárodné súvislosti

S ohľadom na skutočnosť, že SR je v súčasnosti členom všetkých významných medzinárodných inštitúcií a je súčasťou Európskej únie, vzrastá možnosť participácie slovenských firiem na zahraničných projektoch či už v pozícii hlavného dodávateľa, alebo ako subdodávateľa. Obdobne je tomu aj opačne, keď čoraz viac zahraničných právnických osôb je zapojených do projektov v rámci SR, pri ktorých dochádza k postupovaniu utajovaných skutočností. V týchto prípadoch dochádza k prienikom národných a medzinárodných systémov OUS. Záujmom úradu je sprehľadniť postupy platné pre zahraničné právnické osoby, ale aj vytvoriť širšie možnosti pre slovenských

podnikateľov participovať na medzinárodných tendroch v zahraničí umožnením vydávania certifikátov NATO, resp. EÚ, čo je oblasť, ktorú zákon v súčasnosti nepokrýva.

Úrad v spolupráci s ústrednými orgánmi štátnej správy vypracuje v krátkodobom horizonte postupy platné pre zahraničné právnické osoby pri ich participácii na projektoch v rámci SR a postupy platné pre slovenské právnické osoby pri ich participácii na medzinárodných projektoch v zahraničí, s dôrazom na postupy platné v rámci NATO a EÚ.

V neposlednom rade je potrebné upriamiť pozornosť na dva problematické okruhy vo vzťahu k priemyselnej bezpečnosti. Prvým je vykonávanie bezpečnostných previerok u novovytvorených podnikov. Ide o spoločnosti, ktoré nie sú etablované na trhu a ich história je taká krátka, že nie je možné posúdiť ich pôsobenie do budúcnosti, z čoho vyplýva aj zvýšené ekonomické riziko vyplývajúce zo vstupu do nového segmentu podnikania. Ich vznik často môže byť aj účelový so zámerom zbavenia sa „nálepky“ problémovej firmy. V takýchto prípadoch bude potrebné stanoviť zákonom danú podmienku niekoľkoročnej existencie spoločnosti.

Druhým problémom je v súčasnosti neregulovaný systém v oblasti spracovávania bezpečnostných projektov. Zámerom do budúcnosti je projektovanie ochrany utajovaných skutočností riešiť autorizáciou fyzických osôb, prípadne podnikateľov spĺňajúcich odborné predpoklady v danej oblasti.

Podsystémy riadenia a kontroly

Usmerňovanie riadiacich procesov

Efektívne zabezpečenie OUS bez spoločensky škodlivých následkov spôsobených nesprávnym rozhodnutím je možné iba vtedy, ak rozhodovacia zložka má možnosť na základe spätných väzieb ovplyvniť ďalší priebeh v súlade so žiadúcim stavom. Pokiaľ ide o spätnú väzbu v riadení a zabezpečovaní OUS, vo významnej miere ide o informácie, ktoré sú výsledkom kontrolnej činnosti. Teda aj v oblasti zabezpečenia OUS platí zákonitosť, že všetky procesy sú riadené a ovládané len vtedy, ak riadiaca zložka dostáva informácie o správaní výkonných zložiek a na základe týchto informácií upravuje ďalšie procesy.

Prienik rovín kontrolnej činnosti

Veľké množstvo týchto informácií má vo svojej kvalifikovanej podobe kontrolný charakter. Je dôležité vnímať platnosť uvedenej zákonitosti vo dvoch rovinách. Prvou rovinou je kontrolná činnosť NBÚ, zadefinovaná v systéme vonkajšej kontroly. V druhej rovine ide o vlastnú kontrolnú činnosť štátnych orgánov a iných právnických osôb v oblasti ochrany utajovaných skutočností, ktorá je vykonávaná v rámci systému vnútornej kontroly.

V oblasti kontroly OUS hrajú veľmi dôležitú úlohu vertikálne prieniky týchto dvoch rovín v oboch smeroch. V smere od NBÚ ku kontrolovaným subjektom, najmä pokiaľ ide o ústredné orgány štátnej správy, je potrebné zameranie kontroly nasmerovať na centrálne riadiace zložky kontrolovaného subjektu. Tu je potrebné kontrolovať najmä účinnosť vlastného vnútorného kontrolného systému a kontrolu v podriadených zložkách ponechať centrálnym riadiacim zložkám kontrolovaného subjektu. Uvedenou deľbou práce sa predíde nadbytočným kontrolám, kedy dva kontrolné orgány duplicitne kontrolujú OUS v tom istom subjekte. Tento smer vertikálneho prieniku aj tým, že kontrolnými zisteniami odhaľuje vlastné nedostatky, napomáha kontrolovanému subjektu pri skvalitňovaní úrovne ochrany utajovaných skutočností. Tým sa napĺňa preventívna, poznávacia, výchovná a informačná funkcia vonkajšej kontroly NBÚ, ale i vnútornej kontroly v kontrolovanom subjekte.

Opačný smer prieniku má význam pri metodických a školiacich aktivitách NBÚ. Rozpracovaním a zovšeobecnením kontrolných zistení a ďalších poznatkov z kontrolnej činnosti získavajú pracovníci NBÚ cenný zdroj poznatkov a informácií pre zostavenie obsahovej štruktúry a náplní školení bezpečnostných zamestnancov a pracovníkov bezpečnostných pracovísk.

Vonkajšia kontrola NBÚ je teda prednostne zameraná na štátnu správu, kde sa nakladá s najväčším počtom utajovaných skutočností. Kontrola bude vykonávaná najmä na ústredných orgánoch štátnej správy tak, aby bol, pokiaľ to bude možné, zachovaný aspoň trojročný cyklus. To však nevylučuje, že kontrolovanými subjektami nebudú aj obce, vyššie územné celky a podnikatelia.

Pri kontrole podnikateľa je potrebné jednoznačne odlíšiť, či ide o kontrolu alebo o overovanie dodržiavania podmienok priemyselnej bezpečnosti. Obdobne bude potrebné odlišovať vonkajšiu a vnútornú kontrolu od inšpekcií registrov US, ktoré sú vykonávané orgánmi EÚ a NATO vo svojich členských krajinách. Takýmto odlíšením sa neznižuje legitímnosť kontroly, ani previerkových aktivít podľa iných predpisov, ale naopak, dochádza k zlepšovaniu efektívnosti kontrolnej činnosti a ku zvyšovaniu účinnosti kontrolného systému.

Systémové okolie

Národný systém OUS je obklopený medzinárodným systémovým okolím, ktoré ho aktívne ovplyvňuje svojimi vstupmi (požiadavky, očakávania, záväzky) a je príjemcom jeho výstupov (garancia plnenia záväzkov, spolupráca na národnej a medzinárodnej úrovni, ochrana utajovaných skutočností postúpených SR).

Vzhľadom na záväzky, ktoré sa SR zaviazala plniť, sú prvkami systémového okolia, okrem NATO, EÚ a štátov, s ktorými má SR podpísanú dohodu o výmene utajovaných skutočností, aj medzinárodné organizácie (napr. OSN, OBSE, Rada Európy), a mnohé dobrovoľné združenia (napr. Wasseenaarské zoskupenie, Austrálska skupina a Skupina jadrových dodávateľov) s vlastným režimom ochrany informácií.

Na národnej úrovni má NBÚ postavenie orgánu štátnej správy s ústredným postavením pre oblasť OUS. Je tvorcom a garantom systému OUS v SR. Na medzinárodnej úrovni úradu patrí postavenie národnej bezpečnostnej autority, je partnerom národných bezpečnostných autorít a medzinárodných bezpečnostných štruktúr NATO a EÚ z čoho okrem iného vyplýva povinnosť podieľať na stanovovaní spoločných bezpečnostných noriem, zabezpečovať ich implementáciu a garantovať dodržiavanie zásad manipulácie s utajovanými skutočnosťami postúpených SR.

Systém prenosu informácií zo zahraničia k rezortom a od rezortov k NBÚ

Súčasné riešenie prenosu informácií nie je dostatočne efektívne. Potreba skvalitniť mechanizmy prenikania informácií o výsledkoch činnosti Bezpečnostných výborov EÚ a NATO (výsledky rokovaní, prijímanie dokumentov) do rezortov sa úzko prelína so záujmom úradu získavať aktuálne a včasné informácie od rezortov, ktoré participujú v oblasti zahraničnej bezpečnostnej politiky.

Správne nastavenie systému prenosu informácií môže nasledovať až po identifikovaní nefunkčných inštitúcií, väzieb a mechanizmov. Jedným z nástrojov je nahradenie prvku D-SITCEN už v minulosti uvažovaným uzlom Stály SITCEN, ktorý môže výhľadovo zohrávať úlohu koordinačného bodu pre zhromažďovanie, vyhodnocovanie a distribúciu informácií. K zlepšeniu komunikačných väzieb môže prispieť aj revitalizácia obsahu rokovaní Výboru pre zahraničnú politiku (ale aj ostatných výborov) Bezpečnostnej rady SR a nastavenie komunikácie s rezortnými partnermi tak, aby informácie prúdili aj na NBÚ. Táto otázka však musí byť riešená samostatne v rámci postavenia NBÚ v bezpečnostnom systéme SR.

Podiel na príprave bezpečnostných noriem EÚ a NATO

NBÚ z pozície národnej bezpečnostnej autority musí na medzinárodnej pôde aktívnym prístupom ovplyvňovať tvorbu predpisov a noriem EÚ a NATO v súlade so záujmami SR i s cieľmi úradu, citlivo vnímať legislatívny proces EÚ a NATO, predkladať stanoviská odborne podopreté a snažiť sa argumentovať v prospech riešení, ktoré sú výhodné pre úrad a SR.

Účasť zástupcov NBÚ na pracovných i rozhodovacích rokovaniach orgánov EÚ a NATO je potrebné zachovať v súčasnej miere, keďže ich participácia vychádza z postavenia úradu ako bezpečnostnej autority pre EÚ a NATO a teda z príslušných noriem týchto integračných zoskupení.

Znalosť odbornej anglickej terminológie v oblasti OUS je zatiaľ prekážkou pre efektívne prenikanie poznatkov a dokumentov z EÚ a NATO všetkým, ktorí s postúpenými utajovanými skutočnosťami manipulujú. Úlohou úradu bude v krátkej budúcnosti prekladať zásadné dokumenty do slovenčiny a poskytovať ich partnerom vo vnútri štátu aby OUS postúpených SR bola na čo najvyššej možnej úrovni. Rovnako dôležitá je príprava jazykovo zdatných zástupcov na rokovaniach orgánov EÚ a NATO ako i odborníkov vo všetkých organizáciách verejného a súkromného sektora, ktoré prichádzajú do styku s utajovanými skutočnosťami EÚ a NATO.

Implementácia noriem a predpisov EÚ a NATO

Implementácii noriem do každodennej praxe musí predchádzať zabezpečenie kvalitného prekladu relevantných predpisov. Súčasne je potrebné vhodne nastaviť systém priebežného prekladania novoprijatých noriem, aby v budúcnosti nedochádzalo k časovej tiesni. Oficiálne dokumenty EÚ publikované v Úradnom vestníku EÚ sú prekladané Centrálnou prekladateľskou jednotkou Úradu vlády SR a napriek úspešnej spolupráci v minulosti pri riešení problematickej terminológie v oblasti OUS, bude nutné túto spoluprácu naďalej rozvíjať.

Ďalším krokom musí byť zmapovanie vstupov (informačných tokov) zahraničných US do národného systému, špecifikovať ich príjemcov a zistiť ktorí s nimi pracujú najčastejšie a podľa povahy potrieb pripravovať metodické usmernenia, či školenia.

Bilaterálna spolupráca s partnerskými NSA

Bilaterálna spolupráca s partnerskými inštitúciami (zahraničnými národnými bezpečnostnými autoritami) sa na jednej strane rozvíja rámcovo (zmluvne) a pracovne, na druhej strane má aj svoj inštitucionálny (najvyšší predstavitelia) a expertný rozmer. Udržiavanie kontaktov na najvyššej úrovni je mimoriadne prospešné, pretože vytvára podmienky pre spoluprácu na expertnej úrovni.

Cieľom NBÚ je v prvej fáze pripraviť podmienky pre podpis medzivládnych dohôd o spolupráci a vzájomnej ochrane US, resp. nadviazať na existujúce (už podpísané) dohody. Tie sú základom pre konkrétne expertné partnerstvá - výmenu praktických skúseností, uplatňovanie spoločných zásad pri odbornej činnosti (napr. vydávanie certifikátov NATO, metódy certifikácie technických prostriedkov a pod., alebo dokonca ich vzájomné uznávanie a pod.), no i pre vytváranie spojenectiev pri presadzovaní spoločných záujmov na multilaterálnej úrovni.

V záujme posilnenia bilaterálnych vzťahov NBÚ so zahraničnými partnermi bude potrebné nadviazať základné vzťahy s partnermi (s využitím existujúcich kontaktov získaných pri podpisovaní zmlúv) a rozvíjať konkrétnu spoluprácu na odbornej úrovni (priame vzájomné návštevy, ale aj iné formy komunikácie). Výsledkom môžu byť podpísané memorandá resp. odborné dohody, ktoré uľahčia certifikácie, výkon previerok a pod.

Postupnosť plnenia cieľov koncepcie OUS v časových horizontoch

Spoločné zovšeobecnené koncepčné problémy rozložené v časových horizontoch (KH, SH, DH) sú uvedené v prílohe 2. V dlhodobom časovom horizonte (DH) je cieľom optimálny systém OUS, dosahovaný v strednodobom časovom horizonte (SH) optimalizáciou, ktorej v krátkodobom časovom horizonte (KH) predchádza systémová analýza.

Záver

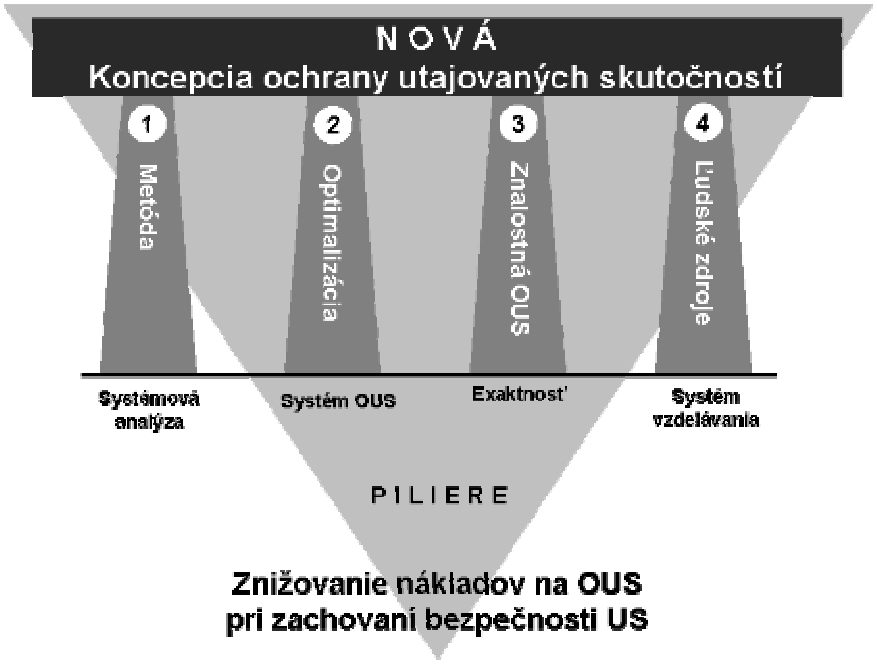
Dlhodobá KOUS je postavená na štyroch základných *pilieroch*):

1. Systémová analýza a syntéza ako nepretržitá *metóda* riešenia OUS.

2. *Optimalizácia* systému OUS ako prostriedok znižovania nákladov pri udržaní požadovaného stupňa bezpečnosti - bezpečnostného štandardu.

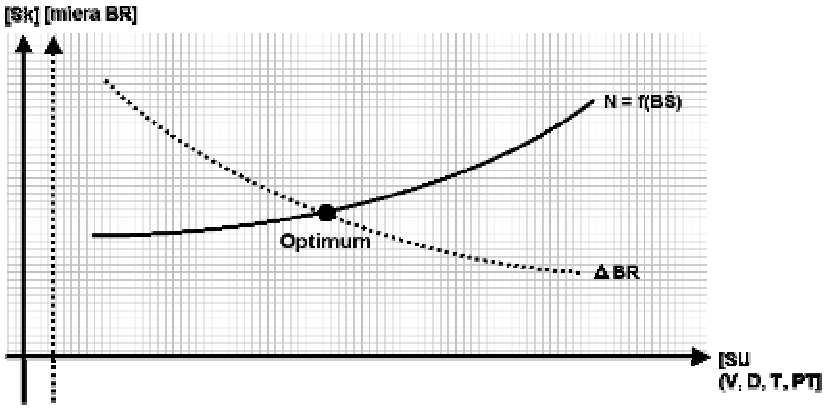
3. *Znalostná OUS* ako nevyhnutná podmienka exaktnosti systému OUS.

4. Kvalita *ľudských zdrojov* a ich systematické celoživotné *vzdelávanie* ako nástroj dlhodobo udržateľného rozvoja systému OUS.



Obrázok 7 - Piliere OUS

Výsledkom realizácie koncepcie OUS bude optimálne vynakladanie prostriedkov na OUS s uvážením prípustnej miery rizika pre daný stupeň utajenia US.



Obrázok 8 - Graf závislosti nákladov na OUS a miery rizika od stupňa utajenia

Prílohy

Príloha 1
Cieľový systém OUS

Príloha 2
Plnenie cieľov KOUS v časových horizontoch

Príloha 3
Postupnosť uplatňovania princípov a zásad OUS v časových horizontoch

Príloha 4
Zoznam použitých skratiek

Príloha 1

Cieľový systém OUS

Charakteristika

Optimálny, **flexibilný, homogénny, adaptívny**, **apolitický** systém OUS.

Spôsob dosiahnutia cieľového stavu

Nahradenie **mechanického** prístupu k riešeniu OUS **systémovým** a aplikáciou moderných metód práce. Zavedením *znalostnej OUS*, založenej na znalostiach (poznatkoch) a ich cieľavedomom využívaní vo všetkých fázach tvorby a rozvoja systému OUS. Vytvorením organizačných štruktúr odvodených od reálne vykonávaných činností prepojených navzájom a s okolím na národnej a medzinárodnej úrovni.

Optimálnosť dosiahnuť optimalizáciou systému OUS a vhodnou voľbou optimalizačných kritérií (náklady, čas, funkčnosť) s dôrazom na zachovanie funkčnosti systému v závislosti od stupňa utajenia pri minimálnych nákladoch a minimálnom čase.

Flexibilitu (pružnosť) dosiahnuť zavedením pružných zoznamov US a BR s relatívne pevným jadrom, zavedením pružného prvku do legislatívy – „politík bezpečnosti US“, ktoré rýchlejšie reagujú na zmeny hrozieb a BR ako vyhlášky a zákon.

Homogénnosť dosiahnuť **harmonizovaním** princípov, terminológie, metodík, postupov, posudzovania bezpečnostných rizík a rozhodovania o výsledkoch previerok, výstupov z bezpečnostných previerok, certifikáciou a štandardizáciou technických prostriedkov (systémov).

Adaptívnosť dosiahnuť nepretržitou komunikáciou v systéme OUS aj so systémovým okolím a zavádzaním korekcií v závislosti od zmien systému bezpečnosti US a BR.

Apolitickosť dosiahnuť zvýšením *exaktnosti* (minimalizovanie subjektívnych vplyvov) metodík, posudzovania BR, kolektívnym rozhodovaním o výsledkoch BP a krížovou kontrolou vlády SR a NR SR.

Príloha 2

Plnenie cieľov KOUS v časových horizontoch

KH	SH	DH
Systémová analýza ochrany utajovaných skutočností	Optimalizácia ochrany utajovaných skutočností (OUS)	
Štruktúra Systému OUS	Realizácia organizačného systému OUS a systému zabezpečenia	
Základy teórie OUS	Rozvoj teórie OUS	
Terminologický slovník OUS	Nový terminologický slovník	**Optimálny systém OUS**
Projekt vzdelávania a kariérneho rastu	Realizácia Projektu vzdelávania a kariérneho rastu	
Projekt rozvoja a zabezpečenia ľudských zdrojov (ĽZ)	Realizácia Projektu rozvoja a zabezpečenia ĽZ	
A	**A**	Optimálna **legislatíva**
Formulácia princípov OUS		
Formulácia BR - pružný zoznam US s pevným jadrom	Optimalizácia zoznamu US	
Formulácia BŠ pre stupne utajenia	Optimalizácia bezpečnostných štandardov (BŠ)	
Bezpečnostná politika utajovaných skutočností	Formulácia bezpečnostných politík pre oblasti bezpečnosti US (BUS)	
	Návrh nového zákona o OUS a nových vyhlášok	
B	**B**	Optimálne **projektovanie** BUS
Zásady projektovania OUS a štruktúra BePro	Optimalizácia projektu pre OUS	
Harmonizácia oblastí BUS v BePro	Štruktúra Bezpečnostného projektu pre štátny orgán (BeProŠO)	
Metodika posudzovania bezpečnost. projektu (BePro)	Optimalizácia metodiky posudzovania BePro	
Analýza systému certifikácie prostriedkov	Návrh nového systému certifikácie prostriedkov	
C	**C**	Optimálne **preverovanie** podmienok BUS
Pripojenie nových IZ zo systémového okolia	Automatizácia získavania informácií od informačných zdrojov (IZ)	
Analýza metodík analýz informácií	Zavedenie nových metód analýz informácií	
Analýza metodík rozhodovania o výsledkoch BP	Zavedenie nových metód rozhodovania o výsledkoch bez. prev. (BP)	
Analýza používaných formulárov	Zavedenie nových formulárov	
Metodika overovania informácií	Zavedenie systému overovania informácií	
Štúdia ekonomickej stability podnikateľa	Nová metóda posudzovania ekonomickej stability podnikateľa	
Štúdia bezpečnostnej spoľahlivosti podnikateľa	Nová metóda posudzovania bezpečnostnej spoľahlivosti podnikateľa	
D	**D**	Optimálny systém **overovania** podmienok BUS, inšpekcií a kontroly
Návrh systému overovania podmienok BUS po vydaní certifikátu	Realizácia systému overovania podmienok BUS po vydaní certifikátu	
Návrh systému kontroly	Realizácia systému kontroly	

Príloha 3

Postupnosť uplatňovania princípov a zásad OUS v časových horizontoch

KH
Oboznamovanie sa s US nie je právom ale výsadou
Oboznamovanie sa s US sa uskutočňuje len v nevyhnutnom rozsahu.
Súbeh neurčitosti a exaktnosti.
Súbeh flexibility a stability.
Právo poznať dôvody neudelenia certifikátu (osvedčenia, potvrdenia).
Vykonávanie odvolacieho procesu nezávislým orgánom.
SH
Cyklická systémová analýza a optimalizácia systému OUS.
Exaktnosť spracovávania informácií a zároveň neurčitosť vstupov.
Odvádzanie organizačnej štruktúry od požadovaných funkcií, na základe analýzy potrebných činností.
Návrh rozhodovania o výsledku BP je exaktný.
Kvantifikácia a merateľnosť.
Pevné jadro a relatívna pružnosť BR, BŠ a zoznamov US.
Minimalizácia nákladov na OUS pri zachovaní BŠ.
Projektovanie aplikovaného systému OUS.
Vykonávanie analýz informácií a rozhodovanie o výsledku BP na základe primárnych alebo overených informácií z nezávislých zdrojov.
DH
Povinnosť všetkých osôb ktoré, sa budú oboznamovať s US podrobiť sa BP bez výnimky.
Celoživotné vzdelávanie v oblasti OUS.
BP, okrem úzko určeného okruhu osôb, vykonáva jediná inštitúcia.
Flexibilita BR a zároveň stabilnosť legislatívy.
Apolitickosť.

Príloha 4

Zoznam použitých skratiek

AB	Administratívna bezpečnosť	**PeB**	Personálna bezpečnosť
AI	Analýza informácií	**PO**	Právnicka osoba
B	Bezpečnosť	**Po**	Podnikateľ
BePol	Bezpečnostná politika	**PoAB**	Podsystém administratívnej bezpečnosti
BePro	Bezpečnostný projekt	**PoB**	Podmienky bezpečnosti
BP	Bezpečnostná previerka	**PoBUS**	Podmienky bezpečnosti utajovaných skutočností
BR	Bezpečnostné riziká	**PoFOB**	Podsystém fyzickej a objektovej bezpečnosti
BR EÚ	Bezpečnostné riziká Európskej únie	**PoIB**	Podsystém informačnej bezpečnosti
BR NATO	Bezpečnostné riziká NATO	**PoPeB**	Podsystém personálnej bezpečnosti
BR SR	Bezpečnostné riziká Slovenskej republiky	**PrB**	Priemyselná bezpečnosť
BRPo	Bezpečnostné riziká podnikateľa	**„PT”**	Prisne tajné
BS	Bezpečnostný spis	**Re**	Realizácia
BŠ	Bezpečnostný štandard	**ReBePro**	Realizácia bezpečnostného projektu
BUS	Bezpečnosť utajovaných skutočnosti	**Rv**	Rozhodovanie o výsledku
CR	Centrálny register	**SOUS**	Systém OUS
„D”	Dôverné	**SU**	Stupeň utajenia
ES	Ekonomická stabilita	**ŠO**	Štátny orgán
FO	Fyzická osoba	**„T”**	Tajné
FOB	Fyzická a objektová bezpečnosť	**t UPC**	čas ukončenia platnosti certifikátu
HZ	Hospodárske záujmy	**tm**	Doba manipulácie s US
IBEP	Informačná bezpečnosť a elektronický podpis	**TP**	Technické prostriedky
IZ	Informačné zdroje	**tv**	Čas vzniku US
J	Jednoduchá ujma	**Tv**	Tvorivosť
K	Kvalifikácia ĽZ	**tz**	Čas zániku US
ĽZ	Ľudské zdroje	**tž/US**	Doba života US
MVU	Mimoriadne vážna ujma	**US**	Utajovaná skutočnosť
NzSR	Nevýhodne pre záujmy SR	**„V”**	Vyhradené
O	Obrana	**V**	Vážna ujma
OPoB	Overovanie podmienok bezpečnosti	**Z**	Získavanie infomácií
OSaS	Orgány samosprávy	**ZV**	Zahraničné vzťahy
OŠS	Orgány štátnej správy	**D/FO**	Dotazník fyzickej osoby
OUS	Ochrana utajovaných skutočností	**BD/Po**	Bezpečnostný dotazník podnikateľa
P	Počet ĽZ	**BeProPo**	Bezpečnostný projekt podnikateľa