Ministerstvo životného prostredia Slovenskej republiky
Odbor krízového riadenia a kritickej infraštruktúry
Nám. Ľ. Štúra 1, 812 35 Bratislava

Bratislava 9 **. decembra 2013**

Číslo: 3355 - 53/2013
Počet listov: 25
Prílohy: 3/3

Schvaľujem : _____
Ing. Peter ŽIGA, PhD.
minister

KONCEPCIA

OCHRANY UTAJOVANÝCH SKUTOČNOSTÍ

V MINISTERSTVE ŽIVOTNÉHO PROSTREDIA SLOVENSKEJ REPUBLIKY

Bratislava 2013

KONCEPCIA

OCHRANY UTAJOVANÝCH SKUTOČNOSTÍ

V MINISTERSTVE ŽIVOTNÉHO PROSTREDIA

SLOVENSKEJ REPUBLIKY

O B S A H

Prílohy

Úvod

Ochrana utajovaných skutočností v Ministerstve životného prostredia Slovenskej republiky je upravená zákonom č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon“) a príslušnými vykonávacími vyhláškami.

Koncepcia ochrany utajovaných skutočností v Ministerstve životného prostredia Slovenskej republiky vychádza z koncepcie ochrany utajovaných skutočností v Slovenskej republike. Je základným programovým dokumentom, ktorý určuje koncepčné ciele, opatrenia a postupy na ich dosiahnutie. Koncepcia ochrany utajovaných skutočností dáva dôraz na zladenie základných pojmov a procesov s rešpektovaním špecifík jednotlivých oblastí bezpečnosti utajovaných skutočností.

Povinnosť spracovať koncepciu ochrany utajovaných skutočností vyplynula pre Ministerstvo životného prostredia Slovenskej republiky z § 5 zákona. Uznesením vlády Slovenskej republiky č. 475 z 30. mája 2007 bola schválená koncepcia ochrany utajovaných skutočností Slovenskej republiky a v súlade s touto koncepciou jednotlivé rezorty majú povinnosť vypracovať rezortné koncepcie ochrany utajovaných skutočností.

V zákone je koncepcia ochrany utajovaných skutočností 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 ochrany utajovaných skutočností možno teda chápať ako usporiadanú sústavu názorov, postojov na ochranu utajovaných skutočností O spôsobe dosahovania cieľov v oblasti ochrany utajovaných skutočností však hovorí stratégia. Z uvedeného vyplýva, že definícia koncepcie ochrany utajovaných skutočností uvedená v zákone obsahuje aj prvky stratégie ochrany utajovaných skutočností.

Jedným z cieľov koncepcie ochrany utajovaných skutočností je preto aj zovšeobecnenie základných pojmov a procesov s rešpektovaním špecifík jednotlivých oblastí, pretože dosiaľ nebola publikovaná usporiadaná sústava názorov na ochranu utajovaných skutočností v uvedených súvislostiach. Nezastupiteľnou úlohou tejto koncepcie je preto urobiť to aspoň v prvom priblížení – ako základ budúcej teórie ochrany utajovaných skutočností a jej rozvoja smerujúcej k optimálnemu systému ochrany utajovaných skutočností.

Úlohou tejto koncepcie ochrany utajovaných skutočností je formulovať hlavné princípy ochrany utajovaných skutočností v Ministerstve životného prostredia Slovenskej republiky a systémové požiadavky na cieľový systém ochrany utajovaných skutočností.

1. Súčasný stav

Súčasný stav ochrany utajovaných skutočností je charakteristický tvorbou medzinárodných dokumentov, ktoré vychádzajú z princípov ochrany utajovaných skutočností členských krajín EÚ a NATO. Pravidlá EÚ pre oblasť ochrany utajovaných skutočností sú

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

dané legislatívou EÚ, ktorá je súčasťou právnych predpisov členských krajín. V súčasnosti sa pracuje na smerniciach EÚ pre jednotlivé oblasti bezpečnosti utajovaných skutočností.

Ciele EÚ v danej oblasti sú stanovené všeobecne, rovnako ako nástroje na ich dosiahnutie. V rámci EÚ rozhodujúcu úlohu z hľadiska prijímania záverov na ochranu utajovaných skutočností plní Rada Európskej únie. Ak neexistuje zhoda názorov členských krajín je povolený samostatný prístup s tým, aby sa členská krajina zdržala konania, ktoré by mohlo byť v rozpore so záujmami EÚ alebo znižovala účinnosť jej rozhodnutí.

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

Súčasný stav ochrany utajovaných skutočností v Slovenskej republike je daný platnou legislatívou, ktorá sa neustále vyvíja. Zásadným spôsobom ochranu utajovaných skutočností ovplyvňovali a ovplyvňujú zmeny spojené so vstupom Slovenskej republiky do NATO a EÚ. V priebehu relatívne krátkeho obdobia sa podarilo vytvoriť systém ochrany utajovaných skutočností, ktorý umožňuje pomerne dôsledné sledovanie reálneho stavu v tejto oblasti a prijímanie zodpovedajúcich opatrení.

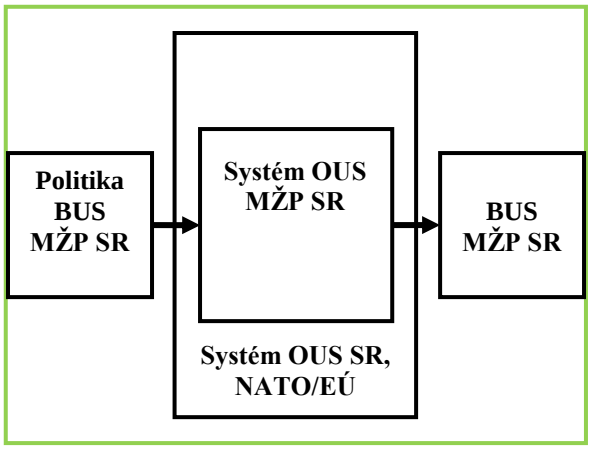
V rezorte Ministerstva životného prostredia Slovenskej republiky nie je vypracovaná politika bezpečnosti utajovaných skutočností ako strategický dokument, nakoľko to nestanovuje žiadna platná legislatívna norma (legislatívna norma túto povinnosť stanovuje len podnikateľským subjektom). Ministerstvo životného prostredia Slovenskej republiky má vypracované dokumenty stanovené legislatívou a dokumenty stanovené v zmysle metodických pokynov Národného bezpečnostného úradu. Sú to nasledujúce:

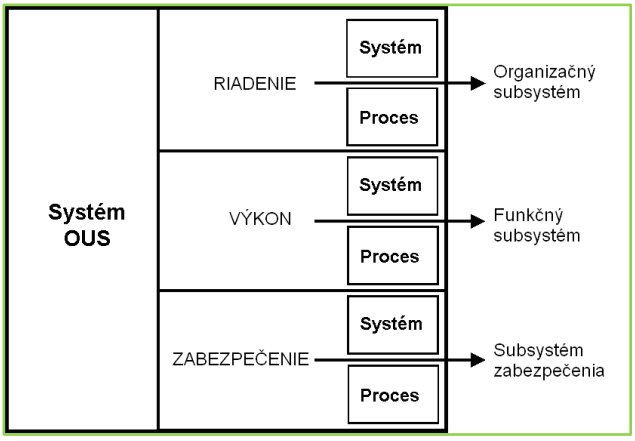
- zoznam utajovaných skutočností v pôsobnosti Ministerstva životného prostredia Slovenskej republiky,
- zoznam funkcií, pri ktorých výkone sa môžu oprávnené osoby oboznamovať s utajovanými skutočnosťami v pôsobnosti Ministerstva životného prostredia Slovenskej republiky,
- bezpečnostná dokumentácia fyzickej bezpečnosti a objektovej bezpečnosti,
- bezpečnostný projekt a smernica technického prostriedku.

Uvedené dokumenty stanovujú zabezpečenie ochrany utajovaných skutočností a kto, kde a akým spôsobom môže s utajovanými skutočnosťami manipulovať.

2. Ciele ochrany utajovaných skutočností a spôsob ich dosahovania

Všeobecným cieľom ochrany utajovaných skutočností je dosiahnutie ich bezpečnosti (obr. 1). V tomto chápaní je ochrana utajovaných skutočností prostriedkom, ktorým sa všeobecný cieľ dosahuje. Systém ochrany utajovaných skutočností môžeme definovať ako celostný a komplexný prístup k riešeniu a chápaniu systému opatrení ochrany utajovaných skutočností, od okamihu vzniku utajovanej skutočnosti, jej vývoja a manipulácie s ňou po celý čas jej trvania až po jej zánik (obr. 2).

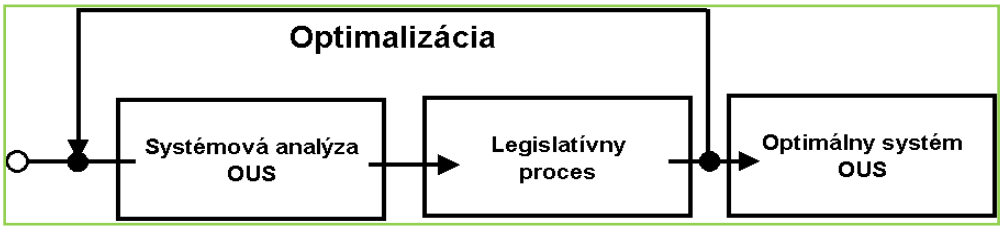




Obrázok 1 – Cieľ systému OUS

Obrázok 2 – Systém OUS

Dlhodobým cieľom ochrany utajovaných skutočností je vybudovanie optimálneho systému (príloha 1), ktorý zabezpečí bezpečnosť utajovaných skutočností rezortu Ministerstva životného prostredia Slovenskej republiky. Pôjde o nahradenie mechanického prístupu k riešeniu ochrany utajovaných skutočností systémovým prístupom a aplikáciou moderných metód práce. Systémový prístup umožňuje definovať základné etapy a fázy procesu ochrany utajovaných skutočností a následne dopracovať zásady a odhaliť ďalšie princípy, ktoré sa stanú základom pre ucelenú teóriu ochrany utajovaných skutočností. Teória potom umožňuje definovať oblasti bezpečnosti utajovaných skutočností ako cieľový stav a zároveň formulovať základný terminologický slovník ochrany utajovaných skutočností, ktorý zabezpečí prehľadnosť, jednoduchosť a zrozumiteľnosť vyhlášok a zákona o ochrane utajovaných skutočností. Zavedením znalostnej ochrany utajovaných skutočností, založenej na znalostiach (poznatkoch) a ich cieľavedomom využívaní vo všetkých fázach tvorby a rozvoja systému ochrany utajovaných skutočností; vytvorením funkčných organizačných štruktúr odvodených od reálne vykonávaných činností prepojených navzájom v rámci rezortu Ministerstva životného prostredia Slovenskej republiky a s okolím na národnej a medzinárodnej úrovni - to sa stane základom pre praktickú implementáciu zásad ochrany utajovaných skutočností v rezorte Ministerstva životného prostredia Slovenskej republiky (príloha 2).



Obrázok 3 – Cyklické analýzy

3. Zásady ochrany utajovaných skutočností

Pre fungovanie a ďalší rozvoj systému ochrany utajovaných skutočností v rezorte Ministerstva životného prostredia Slovenskej republiky budú uplatňované následné zásady:

Optimálnosť vychádzajúca z optimalizácie systému ochrany utajovaných skutočností a vhodnej voľby optimalizačných kritérií (náklady, čas, funkčnosť) s dôrazom na zachovanie funkčnosti systému v závislosti od stupňa utajenia pri minimálnych nákladoch a minimálnom čase.

Flexibilita opierajúca sa o prepracované postupy implementácie systému ochrany utajovaných skutočností a transparentný zoznam utajovaných skutočností a bezpečnostných rizík pre tento systém.

Homogénnosť vychádzajúca z rozpracovanej metodológie ochrany utajovaných skutočností vrátane terminológie a príslušných metodík, postupov, vyhodnocovania bezpečnostných rizík, rozhodovania o výsledkoch bezpečnostných previerok I. stupňa, výstupov z bezpečnostných previerok, certifikácie a štandardizácie technických prostriedkov (systémov).

Adaptabilita spočívajúca v nepretržitej výmene informácii v systéme ochrany utajovaných skutočností a realizácii korekcií v závislosti od zmien v zozname utajovaných skutočností a bezpečnostných rizík.

Apolitickosť spočívajúca v minimalizovaní subjektívnych vplyvov pri posudzovaní bezpečnostných rizík.

4. Metóda ochrany utajovaných skutočností

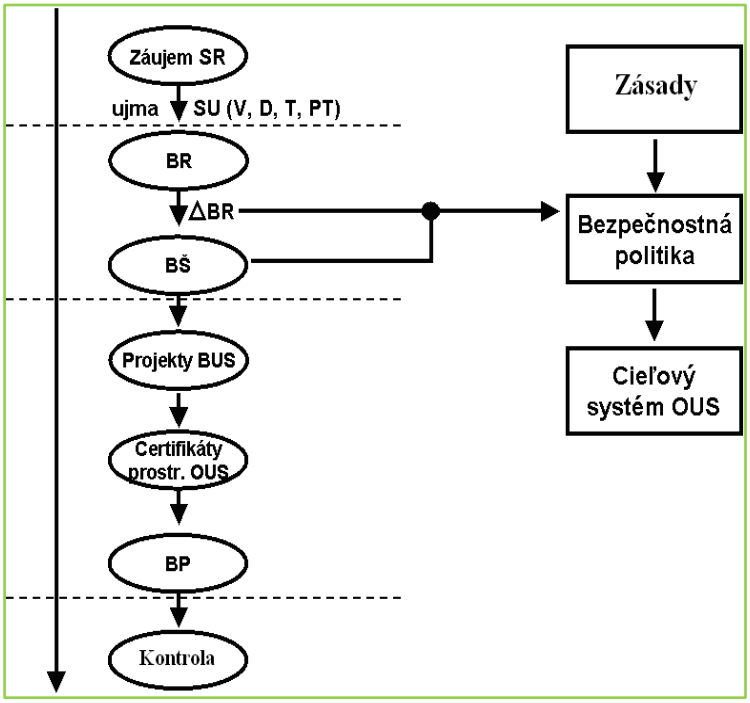
Podstatou prístupu k ochrane utajovaných skutočností v rezorte Ministerstva životného prostredia Slovenskej republiky v súlade s koncepciou ochrany utajovaných skutočností v Slovenskej republike je nahradenie mechanického prístupu systémovým prístupom. Týmto prístupom sa rozumie integrovaný spôsob, vychádzajúci z organického spojenia prvkov (oblastí) samotného systému ochrany utajovaných skutočností navzájom a aj ich spojenie s ich systémovým okolím. Konštituuje rozhodovacie fázy, vrátane príslušných spätných väzieb.

Ak má byť ochrana utajovaných skutočností riešená systémovo, treba odpovedať na otázku čo je cieľom ochrany utajovaných skutočností, 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 ochrany utajovaných skutočností Slovenskej republiky. Treba vyjadriť spôsob, ktorým sa bude možné dopracovať k cieľovej funkcii systému ochrany utajovaných skutočností a k účelovým funkciám jeho podsystémov v rámci Ministerstva životného prostredia Slovenskej republiky.

Dnes ešte nie sú známe jednoznačné odpovede na všetky otázky lebo prostredie, v ktorom sa majú utajované skutočnosti chrániť je veľmi rôznorodé a medzinárodný systém ochrany utajovaných skutočností sa len formuje.

5. Základná schéma ochrany utajovaných skutočností

Logická schéma (obr. 4) ukazuje základné prvky systému ochrany utajovaných skutočností a ich vzájomnú nadväznosť. Predstavuje sled nadväzných procesov plynúcich z jej samotnej podstaty. Absencia ľubovoľného prvku tohto systému by mala nepriaznivé následky pre bezpečnosť utajovaných skutočností.



Obrázok 4 – Základná schéma OUS

Základná schéma je východiskom pre tvorbu politiky bezpečnosti utajovaných skutočností v rezorte Ministerstva životného prostredia Slovenskej republiky, formuláciou základných zásad ochrany utajovaných skutočností a cieľového systému. Všeobecne je potrebné zadefinovať predmet utajenia – utajované skutočnosti a vážnosť utajenia vyjadriť pridelením stupňa ich utajenia (atribút, vlastnosť utajovanej skutočnosti) v závislosti od veľkosti ujmy na bezpečnostných záujmoch.

Tvorba utajovaných skutočností je jedným z najdôležitejších krokov, ktorý má zásadný vplyv na systém ochrany utajovaných skutočností. Na základe doterajších skúseností z vydaného zoznamu utajovaných skutočností rezortu Ministerstva životného prostredia Slovenskej republiky a spracovaného zoznamu funkcií, pri ktorých výkone sa môžu oprávnené osoby oboznamovať s utajovanými skutočnosťami (ďalej len „zoznam funkcií“) je možné konštatovať, že najúčinnejšou ochranou utajovaných skutočností je, ak oprávnené osoby:

- poznajú svoje povinnosti a práva pri ochrane utajovaných skutočností,
- vedia a realizujú všetko, čo potrebujú na vytvorenie podmienok ochrany utajovaných skutočností,
- sú oboznamované s utajovanými skutočnosťami v rozsahu, ktorý potrebujú vedieť pre výkon svojej funkcie,
- nedávajú o utajovanej skutočnosti a zvlášť o ochrane utajovaných skutočností informácie.

Opatrenia na zníženie rizík na vyhovujúcu úroveň budú obsiahnuté v štandarde pre daný stupeň utajenia:

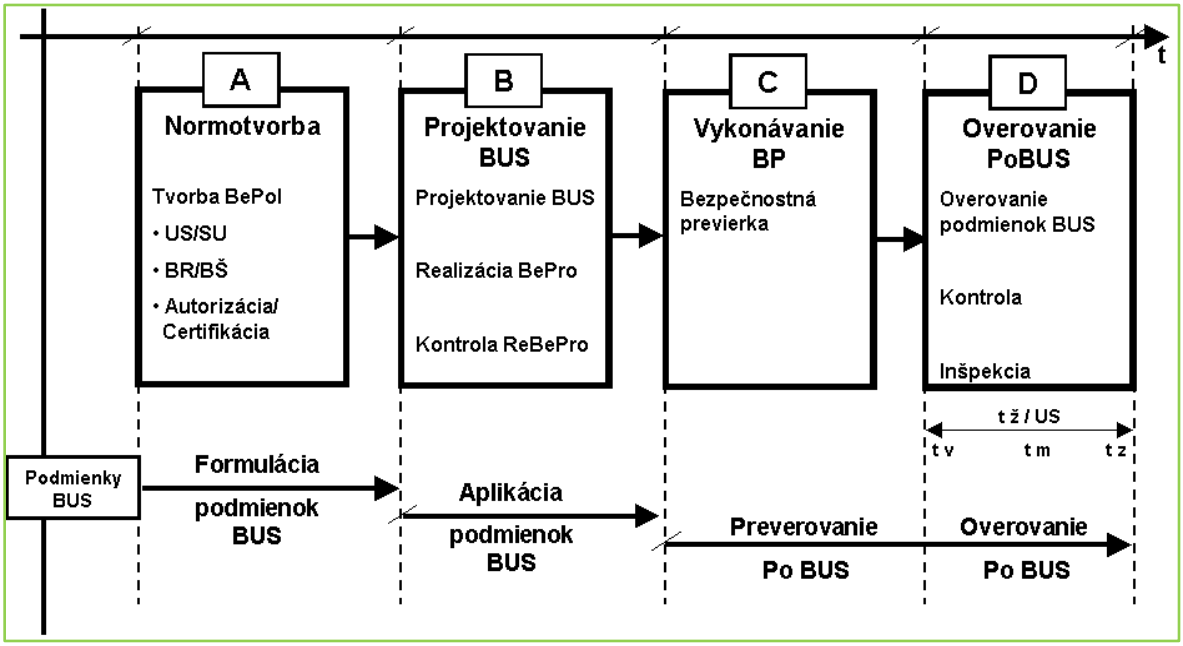
- pri projektovaní je povinnosťou použiť na ochranu utajovaných skutočností len certifikovaný bezpečnostný produkt technického prostriedku na požadovaný stupeň utajenia,
- po schválení bezpečnostného projektu príslušnou autoritou sa bezpečnostný projekt môže zrealizovať,
- bezpečnostnou previerkou sa preveruje dodržanie nastavených štandardov vo všetkých oblastiach bezpečnosti,

- po vydaní certifikátu, osvedčujúceho bezpečnosť pre utajovanú skutočnosť daného stupňa utajenia, na daný čas v konkrétnom prostredí je nevyhnutné dodržiavať podmienky bezpečnosti utajovaných skutočností až do skončenia platnosti certifikátu.

Vytvorenie optimálne funkčného systému vyžaduje:

- zabezpečenie potrebných ľudských zdrojov na plnenie úloh ochrany utajovaných skutočností,
- účelné vybudovanie a usporiadanie chránených priestorov a objektov, ktoré vytvárajú podmienky ochrany utajovaných skutočností,
- prípravu a uplatňovanie organizačných a režimových opatrení.

Systém ochrany utajovaných skutočností 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 bezpečnosti utajovaných skutočností, preverovania podmienok bezpečnosti utajovaných skutočností pred vydaním certifikátu a overovania podmienok bezpečnosti utajovaných skutočností po jeho vydaní (obr. 5).



Obrázok 5 – Proces OUS, jeho etapy a fázy

Pri skúmaní jednotlivých zložiek (oblastí) bezpečnosti utajovaných skutočností ako cieľového stavu ochrany utajovaných skutočností, môžeme hovoriť o oblastiach personálnej bezpečnosti, fyzickej bezpečnosti a objektovej bezpečnosti, informačnej bezpečnosti, administratívnej bezpečnosti a u *podnikateľov* aj o priemyselnej bezpečnosti.

Utajované skutočnosti (veci alebo informácie) je potrebné preskúmať vo všetkých variantoch pri postupovaní (vytváraní) medzi štátnymi a podnikateľskými subjektmi v národnom a medzinárodnom prostredí. Utajované informácie je potrebné oddeliť od neutajovaných a riešiť ich systém bezpečnosti po fázach (vznik, spracovanie, prenos, ukladanie, archivácia) pre všetky formy (zvuk, obraz, dáta) a 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. Pretože záujmy Slovenskej republiky a technológie sa budú meniť s časom, je nevyhnutné, aby aj systém posudzovania bezpečnostného rizika bol pružný. Riziko utajovaných skutočností je potrebné oddeliť od iných rizík, ktoré nesúvisia s ochranou utajovaných skutočností.

Vo všeobecnosti je potrebné na minimalizovanie bezpečnostného rizika formulovať protiopatrenia (preventívne, detekčné a eliminačné). Zámerom je, aby sa bezpečnostné riziko v jednotlivých oblastiach ako je bezpečnosť štátu, ochrana, obrana, hospodárske záujmy Slovenskej republiky, zahraničné vzťahy sledovali a aplikovali do prostredia Ministerstva životného prostredia Slovenskej republiky.

6. Oblasti bezpečnosti utajovaných skutočností

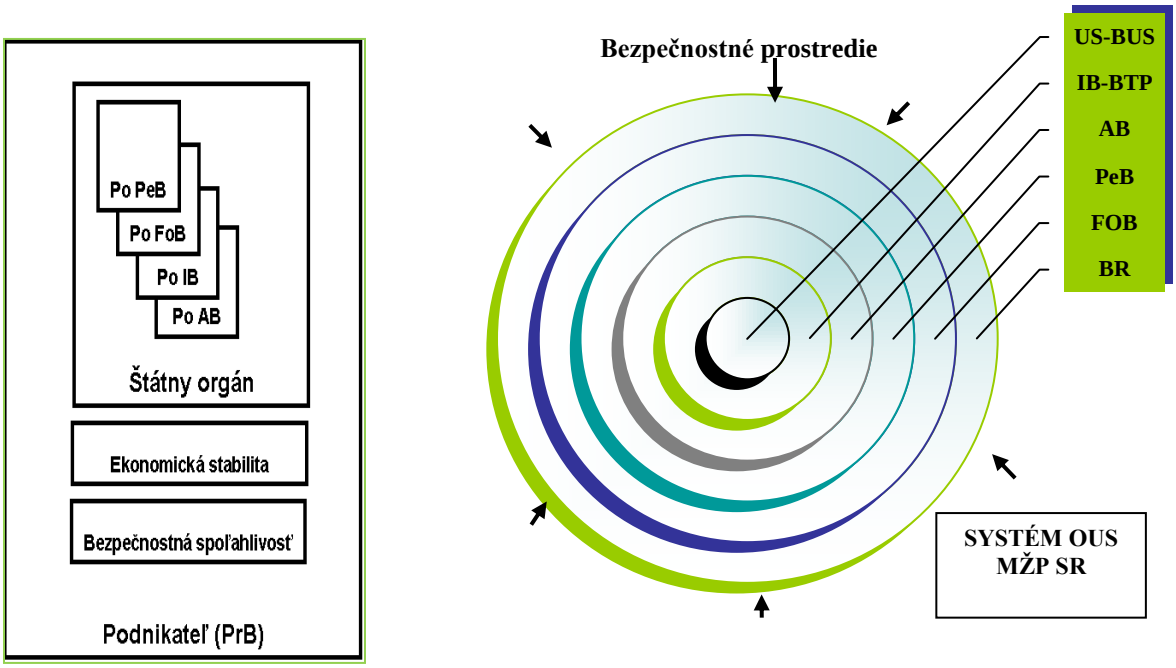
Pojem bezpečnosť utajovanej skutočnosti vyjadruje stav ochrany utajovaných skutočností, istú kvalitu, ktorá sa vyvíja, mení spolu s vlastným systémom a jeho okolím. Ide tiež o sústavu opatrení, pravidiel a postupov v personálnej bezpečnosti, fyzickej bezpečnosti a objektovej bezpečnosti, informačnej bezpečnosti, administratívnej bezpečnosti a priemyselnej bezpečnosti.

Na zabezpečenie bezpečnosti utajovaných skutočností sa musí určiť:

- aká má byť bezpečnosť utajovanej skutočnosti, táto je určovaná interným normatívnym aktom rezortu životného prostredia v súlade s nariadením vlády Slovenskej republiky,
- koho utajovaná skutočnosť, ako a kde sa má chrániť, to znamená určenie pôvodcu a podľa určeného stupňa utajenia zabezpečiť manipuláciu s utajovanou skutočnosťou v súlade so štandardmi,
- pred kým alebo čím je potrebné utajovanú skutočnosť chrániť alebo zabezpečiť jej bezpečnosť, to znamená, či pred konkrétnymi osobami, záujmami skupín osôb, záujmami cudzej moci alebo pred teroristickým útokom, mimoriadnou udalosťou alebo kombináciou týchto faktorov.

Rozhodujúcim činiteľom a základným pilierom v celom systéme a zvlášť pri výkone ochrany utajovaných skutočností je pôvodca, oprávnená osoba a poverená osoba. Táto zásada vychádza z reálneho stavu a stavu, ktorý chceme dosiahnuť. Ochranu a bezpečnosť vo všetkých jej oblastiach vytvárajú a zabezpečujú konkrétne osoby, nepovolané osoby nevynímajúc.

Zo systémového hľadiska možno vnímať oblasti bezpečnosti utajovaných skutočností ako súhrn podsystémov a vzájomných väzieb a procesov medzi nimi (obr. 6).



Obrázok 6 – Podsystémy BUS (na úrovni národnej a Ministerstva životného prostredia SR)

U podsystémov bezpečnosti je potrebné formulovať ich účelové funkcie, vnútornú štruktúru (prvky) a vzájomné vzťahy. V snahe dosiahnuť jednotný systém bezpečnosti nestačí študovať jednotlivé oblasti len samostatne, ale aj vo vzťahu k iným oblastiam a to ako v národnom tak aj v medzinárodnom prostredí. Bude potrebné prehodnotiť vstupy, vnútorné procedúry (postupy, metodiky, projekty, certifikáciu, systém riadenia) a výstupy.

Vo všetkých podsystémoch bezpečnosti je nevyhnutné dosiahnuť taký cieľový stav, že pri manipulácii s utajovanou skutočnosťou bude zabezpečená ochrana utajovaných skutočností. Pritom sú v jednotlivých podsystémoch bezpečnosti podstatné:

- pravidlá a postupy, kde základnou zásadou je, že s vytvorením podmienok a systémom opatrení ochrany utajovaných skutočností sa musí začať skôr, než sa začne manipulovať s utajovanou skutočnosťou,
- požiadavky, kde základnou je poznanie zásad ochrany utajovaných skutočností a povinností s dôsledným plnením povinností zainteresovanými osobami na úseku ochrany utajovaných skutočností,
- obmedzenia, pre manipuláciu s utajovanými skutočnosťami podľa štandardov.

6.1. Podsystém personálnej bezpečnosti

Personálna bezpečnosť 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 ochrany utajovaných skutočností predstavovať potenciálne riziko a ochrana utajovaných skutočností pred takýmito osobami, ktorými môže byť pôvodca, príjemca alebo prepravca. Na zabezpečenie ochrany utajovaných skutočností v oblasti personálnej bezpečnosti 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.

Osobitné miesto v podsystéme personálnej bezpečnosti 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.

Ministerstvo životného prostredia Slovenskej republiky v systéme ochrany utajovaných skutočností má vytvorené osobitné pracovisko zaradené v odbore krízového riadenia a kritickej infraštruktúry, ktoré je priamo riadené ministrom životného prostredia Slovenskej republiky a funkciu bezpečnostného zamestnanca, ktorý je poverený vykonávaním týchto úloh vo vymedzenom rozsahu. Osobitné pracovisko plní funkciu analytickú, plánovaciu, legislatívnu, metodickú, kontrolnú a vzdelávaciu v systéme ochrany utajovaných skutočností.

Na postupné znižovanie počtu preverovaných osôb, ktoré je vo výlučnej zodpovednosti ministra (ďalej len „vedúceho"), je pri stanovovaní funkcií, pri ktorých je predpoklad oboznamovania sa s utajovanými skutočnosťami potrebné uplatňovať zásadu „need to know" („potreba vedieť"). Zo strany vedúceho je preto potrebné pri uplatňovaní spomenutej zásady žiadať o vykonanie bezpečnostných previerok zamestnancov ako predpokladu na výkon funkcie, ktorá je uvedená v zozname funkcií, pri výkone ktorých sa oprávnené osoby môžu zoznamovať s utajovanými skutočnosťami. Rovnako je potrebné, aby vedúci žiadal pre navrhované osoby vykonanie bezpečnostnej previerky vyššieho stupňa len ak je reálny predpoklad, že navrhovaná osoba sa bude s utajovanými skutočnosťami tohto stupňa utajenia v budúcnosti oboznamovať.

Právomoc vykonávať bezpečnostné previerky pre stupeň utajenia „Vyhradené" je zverená vedúcemu, od stupňa utajenia „Dôverné" a vyššie je zverená Národnému bezpečnostnému úradu. Bezpečnostné previerky sa zo systémového hľadiska musia skúmať ako proces v troch fázach:

- príprava na bezpečnostnú previerku,
- vykonávanie bezpečnostnej previerky,
- overovanie podmienok po vydaní osvedčenia.

Obsahom prvej fázy je všeobecne získavanie informácií od žiadateľov o previerku. Fáza prípravy na bezpečnostnú previerku končí podaním žiadosti žiadateľa.

Obsahom druhej fázy je všeobecne analýza informácií získaných od žiadateľov a vyžiadaných od ostatných informačných zdrojov a rozhodovanie o výsledku bezpečnostnej previerky. Fáza vykonávania bezpečnostnej previerky končí vydaním (nevydaním) osvedčenia.

Obsahom tretej fázy je monitorovanie informácií o držiteľoch osvedčenia, overovanie dodržiavania podmienok bezpečnosti utajovaných skutočnosti a kontrola ochrany utajovaných skutočností.

6.2. Podsystém fyzickej bezpečnosti a objektovej bezpečnosti

Fyzická bezpečnosť a objektová bezpečnosť predstavuje systém opatrení, ktorými sa zabezpečujú utajované skutočností pred prístupom nepovolaných osôb a zároveň sa umožňuje prístup k utajovaným skutočnostiam oprávneným osobám na základe potreby vedieť. Opatreniami fyzickej bezpečnosti a objektovej bezpečnosti sa identifikujú pokusy o vstupe narušiteľa a eliminujú sa bezpečnostné narušenia. Fyzická bezpečnosť a objektová bezpečnosť sa dosahuje aplikovaním mechanických zábranných prostriedkov a technických zabezpečovacích prostriedkov, fyzickej ochrany a režimových opatrení.

Cieľom fyzickej bezpečnosti a objektovej bezpečnosti je vytvoriť plnohodnotné bezpečnostné prostredie, v ktorom zamestnanci s plnou zodpovednosťou dobrovoľne a vedome dodržiavajú organizačné a režimové opatrenia stanovené pre daný objekt a chránený priestor.

Samotná realizácia opatrení fyzickej bezpečnosti a objektovej bezpečnosti tvorí cyklus, ktorý pozostáva z jednotlivých procesov. Východiskom je špecifikácia aktív a následná identifikácia objektu a chráneného priestoru, kde sú umiestnené. Analýzou rizík sa identifikujú potenciálne riziká, klasifikujú sa, vyhodnotia sa a určí sa miera rizika ohrozenia utajovanej skutočnosti. Navrhnutím a prijatím vyvážených protiopatrení, ktoré zabezpečia minimálne požiadavky na ochranu utajovaných skutočností sa dosiahne optimalizácia finančných nákladov.

Realizované opatrenia je nutné pravidelne monitorovať a vyhodnocovať. Na základe hodnotenia reálneho stavu je nutné operatívne realizovať nápravné opatrenia. To sa týka najmä platnosti certifikátov jednotlivých mechanických zabraných prostriedkov a technických zabezpečovacích prostriedkov, overovania ich bezpečnostných parametrov a pod..

Ochrana utajovaných skutočností z hľadiska fyzickej bezpečnosti a objektovej bezpečnosti je realizovaná formou „hĺbkovej ochrany“ vo vrstvách. Vnútornú vrstvu tvoria opatrenia na ukladanie utajovaných skutočností, ďalšiu vrstvu tvoria opatrenia na ochranu chráneného priestoru, v ktorom sa manipuluje s utajovanými skutočnosťami, nasledujúcu vrstvu tvoria opatrenia na ochranu objektu.

Pri určovaní primeraných a efektívnych opatrení fyzickej bezpečnosti a objektovej bezpečnosti sa vychádza z hodnotenia rizika, možného ohrozenia utajovaných skutočností, ktoré sa určuje po zhodnotení stupňa utajenia utajovaných skutočností, množstva a formy utajovaných skutočností, úrovne osvedčenia personálu a zhodnotenia ohrozenia utajovaných skutočností vonkajšími a vnútornými vplyvmi. Preto je prioritou uvážlivý manažment bezpečnostných rizík a je potrebné reagovať na zmenu bezpečnostnej situácie a s tým súvisiacu zmenu bezpečnostného rizika tak, aby zohľadňovali reálny stav.

Bezpečnostné opatrenia fyzickej bezpečnosti a objektovej bezpečnosti predstavujú len jeden aspekt ochrany utajovaných skutočností a realizujú sa v kooperácii s opatreniami informačnej bezpečnosti, administratívnej bezpečnosti a personálnej bezpečnosti. Vyvážené aplikovanie jednotlivých opatrení zaručuje vysokú efektívnosť ochrany utajovaných skutočností.

6.3. Podsystém informačnej bezpečnosti

Informačná bezpečnosť v systéme ochrany utajovaných skutočností 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 informačnej bezpečnosti.

Informačná bezpečnosť v pôsobnosti Ministerstva životného prostredia Slovenskej republiky je v súčasnosti riešená len v počítačovej oblasti, a to certifikovaným samostatným technickým prostriedkom pre stupeň utajenia Vyhradené, ktorý spĺňa požiadavky súčasnej národnej legislatívy, avšak nespĺňa požiadavky legislatívy EÚ a NATO.

Informačná bezpečnosť utajovaných informácií 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.

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 a administratívnej bezpečnosti utajovaných informácií v elektronickej forme. V rámci zabezpečenia interoperability Slovenskej republiky s krajinami NATO a EÚ je budúcnosť medzinárodnej ale aj národnej výmeny utajovaných informácií v ich bezpapierovej forme. Prechod z papierovej formy na bezpapierovú má za následok zmenu prostredia, v ktorom sa utajované informácie doteraz nachádzajú. To prinesie so sebou aj výrazne zmeny v evidencii a manipulácii s utajovanými informáciami.

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

Pri budovaní informačnej bezpečnosti 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 najvýznamnejším nástrojom eliminujúcich hrozby, súvisiace s ľudským faktom je stanovenie bezpečnostnej politiky, ktorej súčasťou je aj proces budovania bezpečnostného povedomia a permanentného vzdelávania.

Určenie vhodnej bezpečnostnej architektúry a jej implementácia má výrazný vplyv na úroveň informačnej bezpečnosti 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 informačnej bezpečnosti sú monitoring prevádzky, audit systému a kontrola jednotlivých prvkov informačných systémov.

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

Bezpečnostné produkty pre informačné systémy

V súčasnosti existuje zreteľná deliaca čiara medzi produktmi v oblasti utajovaných skutočnosti na spracovanie a prenos informácií v národnom prostredí a produktmi pre použitie na spracovanie a prenos informácií NATO a EÚ. Ministerstvo životného prostredia Slovenskej republiky v súčasnom období spracováva utajované informácie na certifikovanom samostatným technickým prostriedkom, ktorý spĺňa požiadavky súčasnej národnej legislatívy, avšak pre budúcnosť je potrebné riešiť zakúpenie nového technického prostriedku, ktorý bude spĺňať všetky požiadavky bezpečnosti. Zároveň je potrebné riešiť aj vytipovanie a zakúpenie prostriedkov zabezpečujúcich bezpečné prenášanie utajovaných informácií. Na financovanie týchto služieb je nutné vyčleniť viazané finančné prostriedky v rozpočte Ministerstva životného prostredia Slovenskej republiky.

Backbone (chrbticová sieť)

V súvislosti s predpokladanou národnou, resp. medzinárodnou výmenou utajovaných skutočností bezpapierovou formou, je potrebné vytvoriť jednotný systém prenosu a elektronickej registratúry utajovaných informácií a vybudovať personálne aj materiálne sieťovú zložku informačnej bezpečnosti.

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

Riešenie bezpečnostných incidentov

V Slovenskej republike neexistuje inštitúcia, ktorá by poskytla kvalifikovanú podporu používateľom informačných technológií ochrany utajovaných skutočnosti 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.

Nakoľko Ministerstvo životného prostredia Slovenskej republiky v rámci svojej organizačnej štruktúry nedisponuje expertmi na riešenie následkov bezpečnostných incidentov v oblasti informačnej bezpečnosti spĺňajúcich súčasne podmienku oprávnenia oboznamovať sa s utajovanými skutočnosťami a mohlo by dôjsť k neadekvátnemu správaniu sa oprávnených osôb Ministerstva životného prostredia Slovenskej republiky a tým zvýšeniu úrovne materiálnych i nemateriálnych škôd, je potrebné touto otázkou sa zaoberať. V mnohých prípadoch sú procesy poškodenia nezvratné.

6.4. Podsystém administratívnej bezpečnosti

Úlohou administratívnej bezpečnosti je zabezpečiť dodržiavanie predpísaných bezpečnostných opatrení, ktoré umožnia bezpečné vytvorenie utajovanej skutočnosti, jej bezpečné využívanie po nevyhnutnú dobu a jej korektné vyradenie.

Základným cieľom v oblasti administratívnej bezpečnosti je obmedziť neodôvodnenú tvorbu utajovaných písomností tak, aby boli vytvárané len v nevyhnutných prípadoch. Špecifikovať len veľmi obmedzený okruh osôb, ktoré sa budú oboznamovať s utajovanými písomnosťami. V praxi veľmi dôsledne uplatňovať princíp „need to know“, a naďalej skvalitňovať postupy pri manipulácii s utajovanými písomnosťami, zamerané na uplatňovanie osobnej zodpovednosti všetkých zamestnancov rezortu Ministerstva životného prostredia Slovenskej republiky.

Dôležitým prvkom pri tvorbe utajovaných skutočností musí byť podmienka, aby každá písomnosť označená ako utajovaná, utajované informácie aj obsahovala. Do budúcna má rozhodujúci význam zamedzenie utajovaniu informácií, ktoré neobsahujú skutočnosti, zodpovedajúce ustanoveniam zákona a ktorých zneužitie nebude mať žiadny vplyv na záujmy Slovenskej republiky. Vyšší stupeň utajenia má za následok nutnosť zabezpečiť technické prostriedky a systémové prostriedky certifikované na vyšší stupeň utajenia, takisto potrebu preveriť osoby na vyšší stupeň, čo spôsobuje neporovnateľne vyššie náklady na celý systém zabezpečujúci ochranu utajovaných skutočností.

Pre potreby a podmienky Ministerstva životného prostredia Slovenskej republiky je spracovaný zoznam utajovaných skutočností, ktorý je v zásade flexibilný a je možné ho prispôsobovať tak, aby reagoval na nové situácie a odrážal skutočné potreby Ministerstva životného prostredia Slovenskej republiky. V tejto súvislosti je opäť v popredí otázka informovanosti oprávnených osôb a hlavne riadiacich funkcionárov o potrebe efektívneho prístupu k utajovaným skutočnostiam, ktorý ich nebude nútiť neodôvodnene utajovať. Veľmi dôležitým prvkom určovania stupňa utajenia je uvedomenie si potreby určiť dobu, po ktorú musí utajovaná skutočnosť byť utajovaná, resp. môže sa zmeniť jej stupeň utajenia. V tomto smere má významnú úlohu bezpečnostný zamestnanec, ktorý pravidelne vyhodnocuje utajované skutočnosti a zabezpečuje zmenu stupňa ich utajenia.

Dôsledným sledovaním bezpečnostných rizík v oblasti administratívnej bezpečnosti sa zabezpečí eliminácia porušení právnych predpisov v oblasti ochrany utajovaných skutočností smerujúcich k vyzradeniu zneužitiu, poškodeniu, neoprávnenému rozmnoženiu, zničeniu, strate alebo odcudzeniu utajovanej skutočnosti, 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.

Z hľadiska eliminácie bezpečnostných rizík je potrebné vytvárať aktívne väzby aj na ostatné oblasti bezpečnosti. V prípade uloženia a uschovávania utajovaných písomností ide o aktívnu väzbu na oblasť fyzickej bezpečnosti a objektovej bezpečnosti. Nesprávna manipulácia s utajovanými písomnosťami 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 utajovaných písomností na necertifikovaných technických prostriedkoch a porušovaní zásad informačnej bezpečnosti. Udržiavanie funkčného systému ochrany utajovaných skutočností do budúcnosti vyžaduje neustále sledovanie interakcie jednotlivých oblastí bezpečnosti.

Národný ekvivalent EÚ LIMITÉ a NATO UNCLASSIFIED

Vo všeobecne záväzných právnych predpisoch 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, obchodné rokovania).

Potreba systémového riešenia (inštitucionalizácie) v tejto oblasti úzko súvisí aj so vstupmi zo systémového okolia – neutajovanými informáciami s obmedzenou možnosťou manipulácie, ktoré Slovenská republika prijíma z inštitúcií či orgánov NATO a EÚ. Napriek tomu, že nejde o utajované informácie, na ktoré by sa vzťahovali štandardy NATO a EÚ platné pre utajované skutočnosti, tieto dokumenty nie sú všeobecne zverejniteľné (sú označované ako EU LIMITÉ, 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 NATO a EÚ je Národný bezpečnostný úrad garantom dodržiavania zásad manipulácie s ich informáciami a Slovenská republika pristúpila na dodržiavanie ich záväzných noriem, ukazuje sa ako nevyhnutné riešiť mechanizmy ich ochrany pod gesciou Národného bezpečnostného úradu.

Vytvoreniu národného ekvivalentu musí predchádzať vnútorná diskusia na úrovni Národného bezpečnostného úradu, ako aj externá diskusia s ústrednými orgánmi štátnej správy. Z diskusií vyplynie rozhodnutie, či sa táto oblasť stane platnou súčasťou systému ochrany utajovaných skutočností alebo bude riešená samostatne mimo jeho rámca.

V oboch prípadoch je potrebné rozhodnúť o zmenách vo všeobecne záväzných predpisoch (novelizácia zákona a zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a novelizácia, prípadne úprava vyhlášky o administratívnej bezpečnosti), určiť mieru zodpovednosti Národného bezpečnostného úradu a vedúcich, implementovať súvisiace normy NATO a EÚ, stanoviť oblasti, ktorých sa to bude týkať, vytvoriť kompaktný systém manipulácie a evidencie a spracovať metodické pomôcky pre externé prostredie.

6. 5.Podsystém priemyselnej bezpečnosti

Priemyselná bezpečnosť je súhrn opatrení podnikateľa na ochranu utajovaných skutočností, ktoré mu boli postúpené z Ministerstva životného prostredia Slovenskej republiky, s ktorými sa bude oboznamovať, ktoré mu budú odovzdané alebo zaslané alebo ktoré bude vytvárať podľa požiadavky Ministerstva životného prostredia Slovenskej republiky.

Podnikateľ sa môže oboznámiť s utajovanou skutočnosťou Ministerstva životného prostredia Slovenskej republiky, môžu mu byť postúpené utajované skutočnosti rezortu alebo môže vytvárať utajované skutočnosti podľa požiadavky Ministerstva životného prostredia Slovenskej republiky, iba na základe zmluvy o postupovaní utajovaných skutočností (ďalej len „zmluva“).

Rezort môže uzatvoriť zmluvu len s podnikateľom, ktorému Národný bezpečnostný úrad vydal potvrdenie o priemyselnej bezpečnosti.

Hlavným cieľom Ministerstva životného prostredia Slovenskej republiky v oblasti priemyselnej bezpečnosti je zabezpečiť dôslednú ochranu utajovaných skutočností postúpených podnikateľom pred neoprávnenou manipuláciou.

Na splnenie tohto cieľa musí Ministerstvo životného prostredia Slovenskej republiky uviesť do praxe súbor požiadaviek, obmedzení, pravidiel a postupov, ktoré určujú spôsob a rozvoj všetkých oblastí ochrany utajovaných skutočností.

Hlavné požiadavky, obmedzenia a pravidlá pri postupovaní utajovaných skutočností Ministerstva životného prostredia Slovenskej republiky podnikateľovi

Ministerstvo životného prostredia Slovenskej republiky je pri postupovaní utajovaných skutočností podnikateľovi povinné dodržiavať najmä požiadavky, obmedzenia a pravidlá:

- postupovanie utajovaných skutočností nesmie byť v rozpore so záujmami alebo záväzkami Slovenskej republiky,
- utajované skutočnosti postupovať len na základe zmluvy a to iba v miere (rozsahu, stupňa utajenia a času) nevyhnutne potrebnej na plnenie úloh, o ktorých splnenie Ministerstvo životného prostredia Slovenskej republiky podnikateľa požiadalo (dodržiavanie zásady „need to know“),
- kontrolovať distribúciu utajovaných skutočností medzi Ministerstvom životného prostredia Slovenskej republiky a podnikateľom, viesť zoznam podnikateľov, ktorých Ministerstvo životného prostredia Slovenskej republiky požiadalo o vytvorenie utajovaných skutočností alebo ktorým postúpil utajované skutočnosti, viesť zoznam utajovaných skutočností postúpených podnikateľom alebo vytvorených u podnikateľov, viesť evidenciu zmlúv uzatvorených s podnikateľmi,
- pravidelne vykonávať kontrolu dodržiavania ochrany utajovaných skutočností u podnikateľa v rozsahu dohodnutom v zmluve; pri zistení nedostatkov neodkladne vykonať opatrenia na zabezpečenie ochrany postúpených alebo vytvorených utajovaných skutočností, vrátane odňatia utajovaných skutočností,
- pri zániku platnosti potvrdenia o priemyselnej bezpečnosti podnikateľa alebo pri zániku platnosti zmluvy, zabezpečiť neodkladné odobratie utajovaných skutočností, ktoré boli na základe zmluvy podnikateľovi odovzdané alebo ktoré u podnikateľa vznikli.

Postupnosť plnenia cieľov koncepcie v podsystéme priemyselnej bezpečnosti

V krátkodobom časovom horizonte:

- spolupracovať s Národným bezpečnostným úradom pri vytváraní a zavádzaní postupov platných pre zahraničné právnické osoby pri ich participácii na projektoch Ministerstva

životného prostredia Slovenskej republiky a pre slovenské právnické osoby pri ich participácii na medzinárodných projektoch s dôrazom na postupy platné v rámci NATO a EÚ; Ministerstvo životného prostredia Slovenskej republiky bude mať pri plnení uvedenej úlohy nezastupiteľné miesto s cieľom zabezpečiť ochranu utajovaných skutočností na medzinárodnej úrovni,

- spolupracovať s Národným bezpečnostným úradom pri harmonizácii existujúcich zoznamov utajovaných skutočností s cieľom vydania jednotného zoznamu utajovaných skutočností vo forme všeobecne záväzného právneho predpisu.

V strednodobom časovom horizonte v úzkej spolupráci a s metodickou podporou Národného bezpečnostného úradu zadefinovať a uviesť do praxe zdokonalený systém kontroly, ktorý zabezpečí vyššiu účinnosť kontroly ochrany utajovaných skutočností u podnikateľov.

7. Kontrola a riešenie bezpečnostných incidentov

Efektívne zabezpečenie ochrany utajovaných skutočností 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 žiaducim stavom. Pokiaľ ide o spätnú väzbu v riadení a zabezpečovaní ochrany utajovaných skutočností, vo významnej miere ide o informácie, ktoré sú výsledkom kontrolnej činnosti. Teda aj v oblasti zabezpečenia ochrany utajovaných skutočností 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.

Kontrolná činnosť

Veľké množstvo týchto informácií má vo svojej kvalifikovanej podobe kontrolný charakter. Je dôležité vnímať platnosť uvedenej zákonitosti v dvoch rovinách. Prvou rovinou je kontrolná činnosť Ministerstva životného prostredia Slovenskej republiky, zadefinovaná v systéme vonkajšej kontroly vo vzťahu k podnikateľskému subjektu, s ktorými má Ministerstvo životného prostredia Slovenskej republiky zmluvu o postupovaní, resp. spracovávaní utajovaných skutočností. V druhej rovine ide o vlastnú kontrolnú činnosť Ministerstva životného prostredia Slovenskej republiky v oblasti ochrany utajovaných skutočností, ktorá je vykonávaná v rámci systému vnútornej kontroly.

V rovine vnútornej kontroly je potrebné zosúladiť a následne dodržiavať spôsob vykonávania kontrol stanovený v jednotlivých bezpečnostných dokumentoch, pomôckach a metodických pokynoch (tak vlastných ako aj národných).

Riešenie bezpečnostných incidentov

Napriek tomu, že v pôsobnosti Ministerstva životného prostredia Slovenskej republiky nedošlo v období súčasnej platnej legislatívy v oblasti ochrany utajovaných skutočností k bezpečnostným incidentom je potrebné byť pripravený na ich riešenie. Riešenie bezpečnostných incidentov je potrebné vykonávať komplexne v rámci ochrany utajovaných skutočností, nielen samostatne v rámci niektorých podsystémov bezpečnosti. K tomu je potrebné sa zamerať na zlepšenie vedomostí všeobecne záväzných právnych predpisov na úseku ochrany utajovaných skutočností, čím dosiahnuť ich správnu aplikáciu v praxi a využiť nielen vlastné možnosti a prostriedky, ale aj inštitúcie, ktoré sú schopné poskytnúť kvalifikovanú podporu pri riešení následkov bezpečnostného incidentu pri jeho vzniku, v priebehu alebo po skončení.

Kontrolnú činnosť je potrebné zamerať na zistenie objektívneho stavu a špecifikáciu

zistených nedostatkov, vo väčšom rozsahu ju zamerať na prevenciu a vytvorenie podmienok na účinnejšie plnenie konkrétnych úloh na úseku ochrany utajovaných skutočností v súlade so zákonom.

8. Systémové prostredia

Postavenie Ministerstva životného prostredia Slovenskej republiky v systéme ochrany utajovaných skutočností v Slovenskej republike je dané kompetenciami určenými vládou Slovenskej republiky v súlade so zákonom č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy v znení neskorších predpisov. Ministerstvo životného prostredia Slovenskej republiky nemá vo svojej pôsobnosti organizácie, ktoré priamo riadi a kontroluje v oblasti ochrany utajovaných skutočností a nemá ani zriadený register utajovaných skutočností na ukladanie a uschovávanie utajovaných písomností poskytnutých a prijímaných v rámci medzinárodnej spolupráce. Všetky utajované skutočnosti poskytnuté i prijaté v rámci medzinárodnej spolupráce sú v centrálnom registri utajovaných skutočností vedenom Národným bezpečnostným úradom. V prípade, že medzinárodná spolupráca si bude vyžadovať zriadiť vlastný register utajovaných skutočností bude nevyhnutné na jeho zriadenie vyčleniť finančné prostriedky a aj personálne obsadenie.

Systém ochrany utajovaných skutočností Ministerstva životného prostredia Slovenskej republiky je obklopený národným a 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 Ministerstvu životného prostredia Slovenskej republiky).

Vzhľadom na záväzky, ktoré sa Slovenská republika zaviazala plniť a rezort na ich plnení participuje, sú prvkami systémového okolia, okrem NATO, EÚ a štátov, s ktorými má Slovenská republika podpísanú dohodu o výmene utajovaných skutočností, aj medzinárodné organizácie (napr. JRC EC, OECD, EHK OSN, WHO, UNEP, UNDP a FAO,UNESCO).

Kritéria na výber bezpečnostných zamestnancov sú dnes stanovené platnou legislatívou v oblasti ochrany utajovaných skutočností. Dlhodobým cieľom však musí byť vytvorenie ucelenej teórie ochrany utajovaných skutočností a z toho plynúca koncepcia vzdelávania a rozvoja ľudských zdrojov potrebných na udržanie optimálneho stavu ochrany utajovaných skutočností, čo bude viesť k pružnej reakcii na zmeny bezpečnostného prostredia, v ktorom sa utajované skutočnosti nachádzajú a zároveň aj na finančnú efektívnosť.

Na zvyšovanie odbornej úrovne vlastných zamestnancov je potrebné využiť všetky formy školení a kurzov, ktoré ponúkajú akreditované pracoviská, seminárov, prípadne stáží a postgraduálneho štúdia, zaoberajúcimi sa problematikou ochrany utajovaných skutočností, ktoré sú dostupné na Slovensku a v EÚ.

Podiel na príprave bezpečnostných noriem Slovenskej republiky

Ministerstvo životného prostredia Slovenskej republiky z pozície ústredného orgánu štátnej správy musí na národnej pôde aktívnym prístupom ovplyvňovať tvorbu bezpečnostných predpisov a noriem Slovenskej republiky v oblasti ochrany utajovaných skutočností, predkladať stanoviská odborne podopreté a snažiť sa argumentovať v prospech riešení, ktoré sú výhodné pre Ministerstvo životného prostredia Slovenskej republiky a Slovenskú republiku. Na to je potrebné citlivo vnímať legislatívny proces EÚ a NATO.

9. Postupnosť plnenia cieľov koncepcie ochrany utajovaných skutočností v časových horizontoch

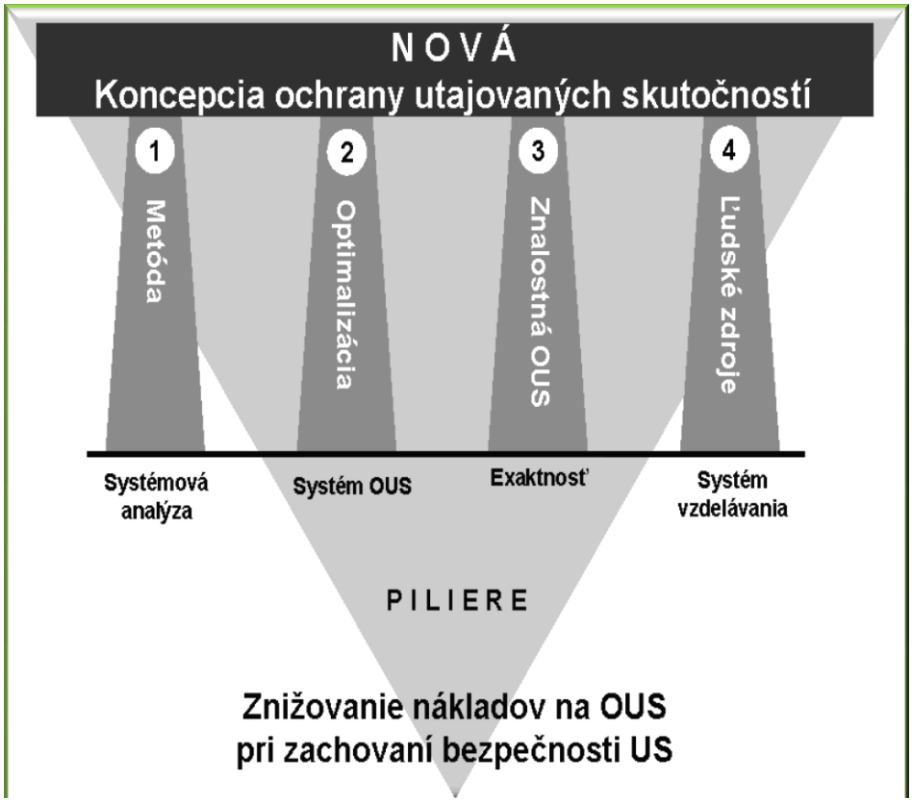
V postupnosti plnenia cieľov koncepcie v podmienkach Ministerstva životného prostredia Slovenskej republiky pri realizácii jednotlivých projektov ochrany utajovaných skutočností je potrebné vychádzať zo súčasného stavu, z požiadaviek, potrieb v súlade s plánom Ministerstva životného prostredia Slovenskej republiky.

Spoločné zovšeobecnené koncepčné problémy rozložené v časových horizontoch sú uvedené v prílohe č. 1. V dlhodobom časovom horizonte je cieľom optimálny systém ochrany utajovaných skutočností, dosahovaný v strednodobom časovom horizonte optimalizáciou, ktorej v krátkodobom časovom horizonte predchádza systémová analýza.

Záver

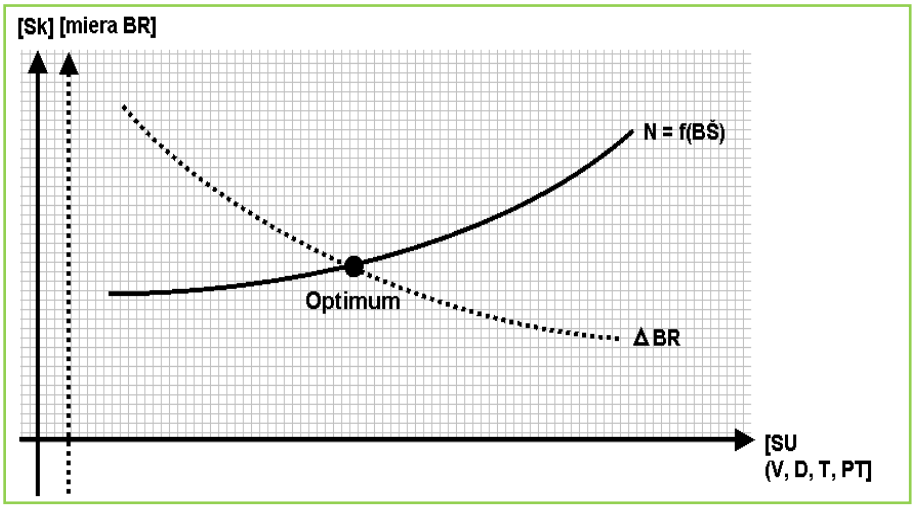
Dlhodobá koncepcia ochrany utajovaných skutočností je postavená na štyroch základných pilieroch:

1. Systémová analýza a syntéza ako nepretržitá *metóda* riešenia ochrany utajovaných skutočností.
2. *Optimalizácia* systému ochrany utajovaných skutočností ako prostriedok znižovania nákladov pri udržaní požadovaného stupňa bezpečnosti - bezpečnostného štandardu.
3. *Znalostná* ochrana utajovaných skutočností ako nevyhnutná podmienka exaktnosti systému ochrany utajovaných skutočností.
4. *Kvalita ľudských zdrojov* a ich systematické celoživotné vzdelávanie ako nástroj dlhodobo udržateľného rozvoja systému ochrany utajovaných skutočností.



Obrázok 7 -Piliere OUS

Výsledkom realizácie koncepcie ochrany utajovaných skutočností Ministerstva životného prostredia Slovenskej republiky bude optimálne vynakladanie prostriedkov na ochranu utajovaných skutočností s uvážením prípustnej miery rizika pre daný stupeň utajenia utajovaných skutočnosti.



Obrázok 1 - Graf závislosti nákladov na OUS a miery rizika od stupňa utajenia

Príloha č. 1 k č. 3355-53/2013

Harmonogram plnenia cieľov koncepcie v časových horizontoch

KH		SH		DH
Podieľanie sa na systémovej analýze OUS SR		Systémová analýza OUS MŽP SR		
Podieľanie sa na štruktúre Systému OUS SR		Realizácia organizačného systému OUS a systému zabezpečenia rezortu MŽP SR		
Podieľanie sa na tvorbe teórie OUS SR		Podieľanie sa na tvorbe teórie OUS SR a jej uplatňovanie v praxi		
Podieľanie sa na tvorbe terminologického slovníka OUS SR		Používanie nového terminologického slovníka OUS		**Optimálny systém OUS**
Projekt vzdelávania a kariérneho rastu MŽP SR		Realizácia Projektu vzdelávania a kariérneho rastu		
NORMOTVORBA		**NORMOTVORBA**		Optimálna **legislatíva**
Podieľanie sa na formulácii princípov OUS SR		Formulácia princípov OUS MŽP SR		
Formulácia bezpečnostných rizík – pružný zoznam utajovaných skutočností MŽP SR s pevným jadrom		Optimalizácia zoznamu utajovaných skutočností rezortu MŽP SR		
Podieľanie sa na tvorbe formulácii bezpečnostných štandardov pre stupne utajenia		Podieľanie sa na optimalizácii bezpečnostných štandardov		
Podieľanie sa na tvorbe Bezpečnostnej politiky utajovaných skutočnosti SR		Vypracovanie implementácie Bezpečnostnej politiky utajovaných skutočnosti SR na podmienky rezortu MŽP SR		
Podieľanie sa na tvorbe nového zákona o OUS a nových vyhlášok		Aktualizácia interných normatívnych aktov MŽP SR v súlade s novým zákonom o OUS a novými vyhláškami		
PROJEKTOVANIE BUS		**PROJEKTOVANIE BUS**		Optimálne **projektovanie** BUS
Podieľanie sa na tvorbe zásad projektovania OUS SR a štruktúre bezpečnostného projektu		Podieľanie sa na optimalizácii projektu pre OUS		
Podieľanie sa na harmonizácii oblastí BUS SR v bezpečnostnom projekte		Štruktúra bezpečnostného projektu v rezorte MŽP SR		
Podieľanie sa na tvorbe metodiky posudzovania bezpečnostného projektu		Podieľanie sa na optimalizácii metodiky posudzovania bezpečnostného projektu		
Podieľanie sa na tvorbe analýzy systému certifikácie prostriedkov		Podieľanie sa na vypracovaní návrhu nového systému certifikácie prostriedkov		
VYKONAVANIE BEZPEČNOSTNEJ PREVIERKY		**VYKONAVANIE BEZPEČNOSTNEJ PREVIERKY**		Optimálne **preverovanie** podmienok BUS
Podieľanie sa na analýze používaných formulárov		Zavedenie nových formulárov		
Podieľanie sa na metodike overovania informácií		Zavedenie systému overovania informácií		
OVEROVANIE PODMIENKY BUS		**OVEROVANIE PODMIENKY BUS**		Optimálny systém **overovania** podmienok BUS a kontroly
Podieľanie sa na návrhu systému kontroly OUS v SR		Realizácia nového systému kontroly OUS v rezorte MŽP SR		

Príloha č. 2 k č. 3355-53/2013

Postupnosť uplatňovania zásad ochrany utajovaných skutočností v časových horizontoch

Krátkodobý horizont
Oboznamovanie sa s utajovanou skutočnosťou nie je právom ale výsadou
Oboznamovanie sa s utajovanou skutočnosťou 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
Strednodobý horizont
Cyklická systémová analýza a optimalizácia systému ochrany utajovaných skutočností
Exaktnosť spracovávania informácií a zároveň neurčitosť vstupov
Odvádzanie organizačnej štruktúry od požadovaných funkcií, na základe analýzy potrebných činností
Návrh rozhodovania o výsledku bezpečnostnej previerky je exaktný
Kvantifikácia a merateľnosť
Pevné jadro a relatívna pružnosť bezpečnostných rizík, bezpečnostných štandardov a zoznamu utajovaných skutočností
Minimalizácia nákladov na ochranu utajovaných skutočností pri zachovaní bezpečnostných štandardov
Projektovanie aplikovaného systému ochrany utajovaných skutočností
Vykonávanie analýz informácií a rozhodovanie o výsledku bezpečnostnej previerky na základe primárnych alebo overených informácií z nezávislých zdrojov
Dlhodobý horizont
Povinnosť všetkých osôb, ktoré sa budú oboznamovať s utajovanou skutočnosťou, podrobiť sa bezpečnostnej previerke bez výnimky
Celoživotné vzdelávanie v oblasti ochrany utajovaných skutočností
Bezpečnostnú previerku, okrem úzko určeného okruhu osôb, vykonáva jediná inštitúcia
Flexibilita bezpečnostných rizík a zároveň stabilnosť legislatívy
Apolitickosť

Zoznam použitých skratiek	
AB	Administratívna bezpečnosť
BePol	Bezpečnostná politika
BePro	Bezpečnostný projekt
BŠ	Bezpečnostný štandard
BR	Bezpečnostné riziká
BP	Bezpečnostná previerka
BUS	Bezpečnosť utajovaných skutočností
D	Dôverné
DH	Dlhodobý horizont
FOB	Fyzická objektová bezpečnosť
IB	Informačná bezpečnosť
IS	Informačný systém
KH	Krátkodobý horizont
KOUS	Koncepcia ochrany utajovaných skutočností
MŽP SR	Ministerstvo životného prostredia Slovenskej republiky
NBÚ	Národný bezpečnostný úrad
OUS	Ochrana utajovaných skutočností
PeB	Personálna bezpečnosť
PoB	Podmienky bezpečnosti
PoAB	Podsystém administratívnej bezpečnosti
PoBUS	Podmienky bezpečnosti utajovaných skutočností
PoFOB	Podsystém fyzickej a objektovej bezpečnosti
PoIB	Podsystém informačnej bezpečnosti
PoPeB	Podsystém personálnej bezpečnosti
PrB	Priemyselná bezpečnosť
PT	Prísne tajné
ReBePro	Realizácia bezpečnostného projektu
SOUS	Systém ochrany utajovaných skutočností
SH	Strednodobý horizont
SU	Stupeň utajenia
T	Tajné
tm	Doba manipulácie s utajovanou skutočnosťou
tv	Čas vzniku utajovanej skutočnosti
tz	Čas zániku utajovanej skutočnosti
tž/US	Doba života utajovanej skutočnosti
US	Utajovaná skutočnosť
V	Vyhradené