BEZPEČNOSTNÝ ŠTANDARD V SYSTÉME OCHRANY UTAJOVANÝCH SKUTOČNOSTÍ

Miroslav Brvnišťan[1], Vladimír Hnat[2],

ABSTRAKT
Bezpečnostný štandard je významným prvkom v systéme ochrany utajovaných skutočností. Nastavenie bezpečnostného štandardu je výsledkom analýzy rizík. Náklady na ochranu utajovaných skutočností majú vplyv na nastavovanie bezpečnostného štandardu. Príprava osôb a ich individuálna zodpovednosť v systéme ochrany utajovaných skutočností je najdôležitejším faktorom pri hodnotení rizík a nastavovaní bezpečnostných štandardov.

Kľúčové slová:
utajované skutočností, bezpečnostný štandard, bezpečnostné riziká, analýza rizík,

ABSTRACT
Security standard is a significant element in the protection of classified information system. Setting the security standard is the result of risk analysis. The costs of the protection of classified information have influence on setting the security standard. Preparation of individuals, and their individual responsibility, in the protection of classified information system is the most important factor in assessing risks and setting security standards.

Key words:
classified information, security standard, security risks, risk analysis

[1] Miroslav Brvnišťan, JUDr. PhD., Národný bezpečnostný úrad , Budatínska 30, Bratislava 850 07, Slovenská republika, Tel.:+421-2-68692335, Fax: +421-2-68691700, miroslav.brvnistan@nbusr.sk;
[2] Vladimír Hnat, Ing. CSc., Národný bezpečnostný úrad , Budatínska 30, Bratislava 850 07, Slovenská republika, Tel.:+421-2-68692368, Fax: +421-2-68691700, vladimir.hnat@nbusr.sk

ÚVOD

Ochrana utajovaných skutočností (ďalej len OUS) zohráva významnú úlohu z hľadiska zabezpečovania základných funkcií štátu, ktorých realizácia už zo svojej podstaty predpokladá systémovú ochranu informácií. Právna úprava OUS realizovaná zákonom č. 215/2004 Z.z. o OUS a o zmene a doplnení niektorých zákonov. To, že OUS nadobúda v súčasnej modernej dobe na význame je reálnym dôsledkom nielen exponenciálneho rastu množstva informácií a ich charakteru, ale aj vývojom bezpečnostného prostredia. Analogicky je možné vnímať v tomto kontexte technický vývoj prostriedkov a nástrojov určených na ich ochranu, respektíve nelegálne získavanie. Správne nastavenie systému OUS tak, aby zodpovedal požiadavkám na bezpečnosť informácií je dnes, ako aj v budúcnosti kľúčovým.

Cieľom príspevku je poukázať na význam a miesto bezpečnostného štandardu (ďalej len BŠ) v systéme OUS ako legitímneho nástroja na zabezpečenie efektívnosti tohto systému a zároveň poukázať na dôsledky tzv. mechanického prístupu k jeho stanovovaniu.

V prvej časti sa príspevok zaoberá významom a miestom BŠ v systéme OUS. Druhá časť príspevku je venovaná popisu vzájomného vzťahu nákladov na OUS a BŠ. Na poznatkoch z praxe je v tretej časti poukázané na skúsenosti vyplývajúce z analýz týkajúcich sa nákladovosti na OUS. V závere je prezentovaný návrh (výzva) smerom na vzdelávacie inštitúcie bezpečnostného charakteru k príprave svojich absolventov pre ich budúcu prax v tejto špecifickej oblasti.

1 BŠ AKO SÚČASŤ ZÁKLADNEJ SCHÉMY OUS

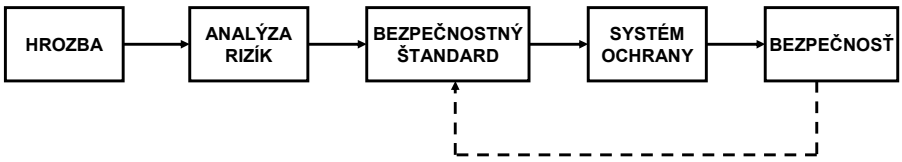
Ochranu informácií utajením možno chápať ako cielenú a bezpečnú distribúciu informácií potrebných pre zabezpečenie fungovania a riadenia štátu. Inak povedané ide o kontrolovaný tok informácií s presne stanovenými štandardami bezpečnosti. Tým sa vo všeobecnosti garantuje, že daná informácia sa dostane len presne určenému – adresnému okruhu osôb a zároveň, že nedôjde napr. k strate takejto informácie alebo jej získaniu neoprávnenou osobou. Je potrebné pri tom zároveň brať v úvahu prapodstatu systému utajovania, ako základného nástroja na zabránenie získavania informácií štátu cudzími (nepriateľskými) spravodajskými službami, čo je možné považovať z pohľadu bezpečnostných rizík za pravdepodobne najsofistikovanejšie bezpečnostné riziko pre utajované informácie..

Správne nastavenie BŠ by malo byť výsledkom systémovej analýzy bezpečnostnej situácie a rizík vyplývajúcich pre dôležité informácie štátu a výsledkom ich kvalitatívneho a kvantitatívneho hodnotenia a posúdenia možných následkov a rizík na predmet ochrany. Hranice bezpečnosti sú potom dané intervalom, v ktorom je

bezpečnosť garantovaná s čo najpresnejšie definovateľnou pravdepodobnosťou eliminácie nežiaduceho stavu.

Súčasná prax v oblasti OUS nepracuje s pojmom BŠ. To však neznamená, že tieto nie sú zavedené, nie sú však explicitne pomenované v platnej legislatíve týkajúcej sa OUS. Platný zákon o OUS pozná síce pojem riziko a riziká v jednotlivých oblastiach OUS - napr. v oblasti personálnej bezpečnosti, objektovej a fyzickej bezpečnosti, avšak tieto tiež jednoznačne a systematicky nevyužíva. Vnímame to ako nedostatok v dôsledku určitého nesystémového vývoja tejto oblasti.[1] Z hľadiska pôvodu by sa BŠ dali rozdeliť na dve skupiny - prevzaté BŠ a empiricky zavedené BŠ. Prvou skupinou je množina tzv. minimálnych BŠ prevzatých zo systémov OUS v EU a NATO. Ich prevzatie a aplikácia v národných podmienkach vyplynula z členstva SR v euroatlantických štruktúrach. Druhú skupinu tvoria BŠ dané národnou legislatívou – zákonom o OUS a z neho vyplývajúcich vyhlášok. Táto druhá skupina BŠ bola zavedená na základe empirického poznania avšak s nie celkom jasne pochopenými dôsledkami. Preto tieto BŠ nie sú z hľadiska väzby na bezpečnostnú situáciu jednoznačne zdôvodnené a ich dodržiavanie je v praxi problematické. Znamená to, že BŠ by mal byť odvádzaný a nie kategoricky určovaný. Skutočnosťou však je že BŠ sú prevažne určované empiricky a intuitívne alebo prevzaté bez bližšieho poznania a odôvodnenia ako v prípade minimálnych štandardov NATO a EÚ. Rovnaký, alebo podobný, stav je v problematike hodnotenia bezpečnostných rizík.

V nasledujúcej schéme je znázornené prepojenie pojmov hrozba, riziko ale aj ochrana a bezpečnosť, pričom je názorne definované aj miesto BŠ v systéme OUS.

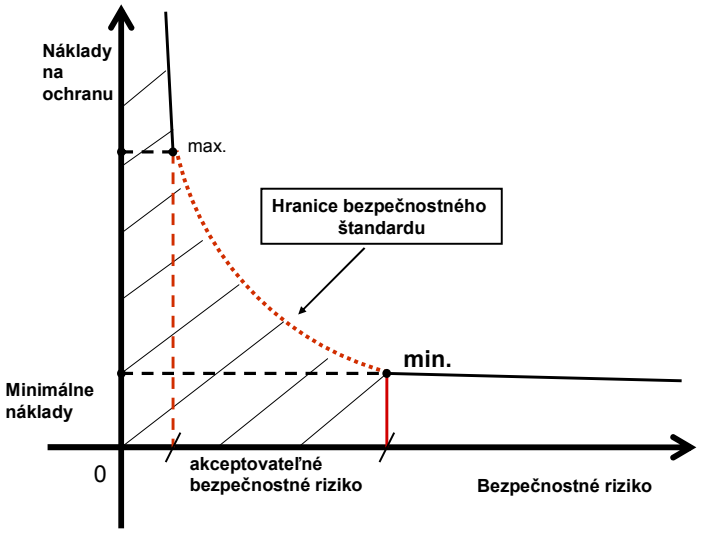


Obr. č. 1: BŠ a jeho miesto v systéme OUS

Schéma, okrem jednoduchého vyjadrenia základných prvkov a atribútov, znázorňuje aj uzavretú systémovú väzbu, ktorá zachytáva podstatu dynamiky zmien systému ochrany informácií podľa spravidla dynamicky sa meniacej hrozby (vyplývajúcej z bezpečnostnej situácie). Cyklus začína analýzou hrozieb vyplývajúcich z bezpečnostnej situácie a stanovením príslušného rizika, následne sa konfrontuje úroveň bezpečnosti podľa nastaveného bezpečnostného štandardu a upravuje (nastavuje) sa systém ochrany. V prípade, že nie je dosiahnutá požadovaná úroveň bezpečnosti, musí sa zvýšiť- upraviť BŠ.[2]

2 BŠ A NÁKLADY NA OUS

Závislosť nákladov na ochranu informácií a bezpečnostným rizikom je nesporná. Táto závislosť je však pre správne navrhnutie BŠ ochrany informácií kľúčová. Nasledujúca schéma ukazuje predpokladaný vzťah medzi kvalitatívnou úrovňou bezpečnosti (vyjadrenou nákladmi na ochranu) a veľkosťou bezpečnostného rizika. Uvedené investície do ochrany predstavujú hmotné a nehmotné prostriedky (technika, financie, ľudský potenciál, softvér), ktoré sú predpokladom pre kvalitu ochrany.



Obr. č. 2: BŠ ako kompromis nákladov a bezpečnostného rizika.

Prostredníctvom schémy je znázornené, že kvalita OUS vyjadrená nákladmi na ňu je ovplyvňovaná veľkosťou bezpečnostného rizika. Je zrejmé, že sa nedá dosiahnuť absolútna bezpečnosť, pretože bezpečnostné riziko sa nedá úplne eliminovať. Priebeh závislosti bezpečnostného rizika od investícii do ochrany informácii znázorňuje krivka. Na schéme je to vyjadrené v ľavej časti kde sa krivka blíži k zvislej osi, ale nikdy ju nedosiahne. Znamená to, že zvyšovanie nákladov na ochranu informácií od istej hodnoty je už neefektívne, nakoľko neprinesie výrazný efekt. Veľké zvýšenie nákladov na ochranu prinesie len zanedbateľné zníženie bezpečnostných rizík.

Body na krivke predstavujú hranice nastavenia BŠ. Minimálny BŠ predstavuje hranicu, pod ktorú by bezpečnostné riziko nemalo klesnúť, pretože nebude zaručená bezpečnosť. Optimálny BŠ predstavuje hranicu, ktorá sa môže považovať za dosiahnutý kompromis medzi veľkosťou nákladov a veľkosťou bezpečnostného rizika (akceptovateľné riziko). Je pritom nespochybniteľné, že náklady, ktoré sú vynakladané na ochranu informácií budú vždy zohrávať určitú (často zásadnú) úlohu. Systém ochrany utajovaných informácií by však mal byť do tej miery flexibilný aby umožnil vhodnú kombináciu ochranných opatrení, ktoré by zohľadňovali nielen nákladovosť ale aj schopnosť vysporiadať sa s reziduálnym rizikom alebo opatreniami zameranými na

odstránenie možného škodlivého následku.

Hranice minimálneho, optimálneho, alebo iného BŠ vždy musí stanoviť subjekt, ktorý rozhoduje o spôsobe ochrany informácie a ktorý podstupuje riziká a čelí hrozbe, vrátane prijatia rozhodnutia o protiopatreniach ako sa s hrozbou vyrovnať.

Stanovenie stupňa utajenia ako systémovej ochrany informácie je v tomto kontexte potrebné vnímať ako jedinečný a pravdepodobne s ohľadom na dynamickosť bezpečnostného prostredia neopakovateľný proces.

3 PROBLÉM V PRAXI - TENDENCIA NEUTAJOVAŤ

BŠ pre OUS podľa vyššie uvedenej schémy a pre účel tohto príspevku je treba vnímať ako tzv. komplexný BŠ zastrešujúci všetky oblasti ochranných opatrení – personálnu, priemyselnú, administratívnu, informačnú a fyzickú a objektovú bezpečnosť. Je zrejmé, že tieto oblasti sú vzájomne prepojené a podmienené, avšak s ohľadom na možnosť jednoznačného a jednoduchého posúdenia a vyhodnotenia nákladovosti, bude pozornosť v ďalšej časti príspevku venovaná najmä dvom oblastiam ochranných opatrení a to najprv fyzickej a objektovej bezpečnosti v spektre nákladov na zabezpečenie OUS a následne personálnej bezpečnosti v kontexte pripravenosti osôb (nie preverovania) vstupujúcich do systému OUS.

Svet sa zmenil. Toto krátke slovné spojenie sa častokrát používa na vyjadrenie dynamiky vývoja. Platí to samozrejme aj pre bezpečnostné prostredie s úzkou väzbou na systém OUS. Z pohľadu systému OUS a to i napriek jeho komplexnosti bola častokrát sústredená pozornosť (chybne) na fyzickú a objektovú bezpečnosť. Na prvý pohľad išlo o logické dôvody, ktoré pri povrchnom posudzovaní boli aj čiastočne logické. Utajované skutočnosti boli z veľkej časti tvorené utajovanými písomnosťami., ktoré bolo potrebné schovať za mreže, zámky a do trezorov – vyjadrenie nákladovosti bolo veľmi jednoduché. Situácia sa zmenila nástupom a rozvojom IT technológií. Utajované informácie majú z dnešného hľadiska nielen svoju elektronickú podobu ale čoraz častejšie sú vo forme elektronickej utajovanej informácie a sú súčasťou komunikačných a informačných systémov. Neoprávnená manipulácia s utajovanými informáciami takto nadobudla oveľa väčší a širší rozmer. Týmto vôbec nie je povedané, že opatrenia fyzickej a objektovej bezpečnosti nie sú potrebné. Do konfrontácie s nimi sa však dostávajú stále rafinovanejšie spôsoby neoprávnenej manipulácie cestou moderných technológii, vrátane zlyhávania ľudského faktora: Prečo je tomu tak? Odpoveď je jednoduchá. Potenciálny zlodej utajovanej informácie hľadá efektívny a rafinovaný spôsob k dosiahnutiu svojho cieľa bez rušivých elementov búrania stien a fyzických zábran.

Z dostupných štatistických údajov vyplýva že za posledné obdobie nedošlo k úniku utajovanej informácie zlyhaním opatrení fyzickej a objektovej bezpečnosti.

Rovnako tak nie je známy prípad, kedy neoprávnená osoba získala utajovanú informáciu zo zabezpečeného - certifikovaného počítača. Pritom ale náklady na objektové a fyzické opatrenia a na technické prostriedky systému OUS predstavujú najväčšiu položku. V praxi je následne možné pozorovať určitú disproporciu medzi potrebou chrániť informácie a nákladovosťou systému na jednej strane a skutočnými bezpečnostnými rizikami na strane druhej. Takéto systémové nedorozumenie je príčinou (dôsledkom) stavu, kedy je jednoduchšie (lacnejšie) neutajovať informácie, respektíve utajovať v čo najnižších stupňoch utajenia. Ako ospravedlnenie sa používajú argumenty, že utajovanie je drahé – predovšetkým priestory, mreže, zámky, zložité je projektovanie a ešte zložitejšie organizačné a technické, administratívne a iné opatrenia. Týmto spôsobom sú ovplyvnené aj analýzy rizík, hlavne „cieleným“ hodnotením veľkosti ujmy na záujmoch štátu. Problém „neutajovania“ vzniká už pri tvorbe tzv. „Zoznamov utajovaných skutočností“. Zaradenie utajovaných skutočností podľa jednotlivých stupňov utajenia smeruje predovšetkým do stupňa Vyhradené. Nižšie uvedená tabuľka vyjadruje percentuálne rozdelenie US podľa zoznamov utajovaných skutočností vybraných subjektov.

Tabuľka 1: Zaradenie US do jednotlivých stupňov utajenia podľa Zoznamov utajovaných skutočností vydaných vybranými rezortmi. Percentuálne vyjadrenie.

	Vyhradené	Dôverné	Tajné	Prísne tajné
Ministerstvo vnútra SR	100,0	34,0	4,6	0,9
Ministerstvo obrany SR	91,4	49,0	27,0	4,3
Ministerstvo zahraničných vecí SR	85,0	89,0	57,0	14,2
Ministerstvo hospodárstva SR	85,4	65,4	36,3	1,8

V zoznamoch utajovaných skutočností sú jednotlivé položky označené aj viacerými stupňami utajenia, preto sumár za jednotlivé rezorty je vždy väčší ako 100 percent. Typickým príkladom je Ministerstvo vnútra SR, kde každá utajovaná skutočnosť môže byť označená aj stupňom Vyhradené. Z tabuľky je zrejme, že prevažná časť utajovaných skutočností je označovaná nižšími stupňami utajenia. Označenie jednotlivých položiek viacerými stupňami utajenia vyplýva aj z toho, že vytváranie „Zoznamov utajovaných skutočností“ je v kompetencii rezortov pričom absentuje centrálne metodické usmernenie národnej autority pre určovanie stupňov utajenia utajovaných skutočností. Výsledkom je deformácia systému ochrany informácií a jeho nesprávne využívanie v dôsledku neznalosti systému OUS v priamom kontexte neprimeraného zohľadňovania nákladovosti.

Berúc v úvahu obrázok č. 2 o nákladovosti systému a nutnosť správneho nastavenia systému OUS sme toho názoru, že na zlepšenie tohto stavu **je potrebné sa seriózne venovať vzdelávaniu (bezpečnostnému vzdelávaniu),** vysvetľovaniu a na úrovni národnej bezpečnostnej autority komunikácii so všetkými zainteresovanými

subjektmi.

4 PRÍPRAVA OSÔB, ÚLOHA VZDELÁVACÍCH INŠTITÚCIÍ

Tendencia nesprávneho utajovania a neutajovania čiastočne súvisí aj so slabou odbornou erudovanosťou, fundovanosťou a pripravenosťou osôb prichádzajúcich do systému OUS. Ide pritom o všetky osoby, ktoré sa zúčastňujú na budovaní systému OUS, vrátane osôb, ktoré tento využívajú na ochranu informácii. **Veľmi dôležitým faktorom (pravdepodobne najdôležitejším) je aj zodpovednosť (dôveryhodnosť) jednotlivca v systéme OUS.** Tu je obrovská bezpečnostná diera. Proces prípravy personálu (bezpečnostného vzdelávania) by mal zohľadňovať aj prípravou študentov na školách. Na niektorých školách s profilom v oblasti bezpečnosti neexistuje ani predmet, ktorý by sa zaoberal problematikou ochrany informácií vo všeobecnom zmysle, nehovoriac o ochrane informácií prostredníctvom ich utajenia. Ak áno, tak v tom lepšom prípade len ako súčasť iného predmetu. Stáva sa bežnou praxou, že čerstvý absolvent školy sa s problematikou ochrany informácií stretne po prvýkrát až vo svojom zamestnaní. Pritom ochrana informácií a informačný manažment sú elementárnou súčasťou všetkých riadiacich procesov. Ochrana informácii pritom už len s ohľadom na exponenciálny rast ich množstva nadobúda na význame.

Sme toho názoru, že absolvent školy bezpečnostného zamerania by mal ovládať problematiku ochrany informácií, vrátane problematiky OUS.

Cieľom študijného predmetu by malo byť:

Naučiť študentov znalostiam o OUS na úrovni nutného minima ako súčasť profilu absolventa školy bezpečnostného zamerania, ktorá pripravuje ľudské zdroje pre bezpečnostnú prax.

Poskytnúť študentom vedomostný základ pre ďalší rozvoj ich poznania vo všeobecnej úrovni a v špecifických oblastiach problematiky OUS v rámci ich budúceho profesijného pôsobenia v tejto oblasti.

Správne nastavenie systému OUS prostredníctvom príslušných BŠ je pre celkovú efektívnosť tohto systému zásadné. BŠ, jeho vyjadrenie, vrátane nákladov na jeho realizáciu sú atribútmi, ktoré v kontexte vzdelaného a správne vyškoleného personálu môžu nadobudnúť nový význam.

LITERATÚRA

[1] Brvnišťan, M., Polák, P.: Vývoj ochrany utajovaných skutočností na území SR, In Právny obzor, 92/2009, č.3, s. 262-288

[2] Mesároš, J, Hnat, V.: Metodika tvorby bezpečnostných štandardov pre utajované skutočností. Národný bezpečnostný úrad 2009, s. 13

Článok recenzoval:
doc. Ing. T. Loveček, PhD.