MANAŽMENT BEZPEČNOSTNÝCH RIZÍK AKO SÚČASŤ OCHRANY INFORMÁCIÍ PROSTREDNÍCTVOM REŽIMU UTAJENIA

Miroslav BRVNIŠŤAN[1]

ABSTRAKT :

Manažment bezpečnostných rizík je elementárnym východiskom pri zabezpečovaní ochrany informácií, o to viac ak ide o ochranu informácií prostredníctvom režimu utajenia. Schopnosť primerane a aktuálne reagovať na nové bezpečnostné riziká charakterizuje a podmieňuje efektívnosť systému ochrany informácií.

Kľúčové slová : manažment bezpečnostných rizík, ochrana utajovaných skutočností, utajovaná informácia, ochrana, stupeň utajenia, riziko, analýza rizík

ABSTRACT :

Management of security risks is a crucial starting point in ensuring the protection of information, even more when it comes to the protection of information through the confidentiality regime. The ability to adequately and timely respond to new security risks characterizes and determines the effectiveness of the information protection system.

Key words: risk security management, protection of classified information, classified information, protection, classification level, risk, risk analyzes

Súčasný stav kedy všeobecne záväzné právne predpisy upravujúce ochranu informácií utajením, najmä zákon č. 215/2004 Z.z. o ochrane utajovaných skutočností a doplnení niektorých zákonov (ďalej len zákon o OUS), systémovo nedefinujú manažment bezpečnostných rizík, ako taký, je neakceptovateľný. Takýto systém ochrany nie je spôsobilý reagovať na aktuálne bezpečnostné riziká, nakoľko nemá vytvorené potrebné nástroje a inštitúty o nastavení potrebných informačných tokov

[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

nehovoriac. Vo svojej podstate ide skôr o akýsi statický model ochrany, ktorý svojou podstatou len eliminuje určité spektrum existujúcich rizík (bez ohľadu na to aké riziká v skutočnosti existujú), to je však nedostatočné. Naopak nesystémové zmienky o hodnotení rizík možného ohrozenia napr. v časti týkajúcej sa fyzickej bezpečnosti a objektovej bezpečnosti[2] zákona o OUS, prispievajú k nesprávnemu pohľadu na miesto a úlohy manažmentu bezpečnostných rizík v systéme ochrany utajovaných skutočností (ďalej len OUS).

Určenie postavenia a väzieb manažmentu bezpečnostných rizík v systéme ochrany informácií utajením sa bude odvíjať od identifikovania niektorých základných parametrov systému OUS prostredníctvom ich teoretických charakteristík.

OUS je pojem, ktorého význam možno posudzovať z viacerými spôsobmi. Jedným z nich je analýza samotného pojmu ochrana smerujúca k popísaniu tzv. funkčnej podstaty ochrany, teda dôvodov a zmyslu jej existencie prostredníctvom odpovedí na tri základné otázky[3] :

1. Čo je predmetom ochrany ?
2. Pred kým a pred čím chráni ?
3. Akými nástrojmi sa ochrana vykonáva ?

Prostredníctvom kombinácie odpovedí na uvedené otázky sa pokúsime o čo najpodrobnejšie vyjadrenie pojmu ochrana, čo by malo byť zároveň nápomocné pri popise možného postavenia a väzieb manažmentu bezpečnostných rizík v systéme OUS.

Samotný **pojem ochrana** sa používa v rôznych oblastiach spoločenského života, pričom následne preberá aj ich charakter. Pod pojmom ochrana najčastejšie rozumieme starostlivosť o odvrátenie nebezpečenstva, prostriedky na chránenie a prevenciu, ako súhrn opatrení na odvrátenie alebo zmiernenie škodlivých vplyvom alebo následkov (angl. PROTECTION – akt chránenia alebo stav jestvovania ochrany).[4]

Pod pojmom ochrana však možno rozumieť aj iné súvislosti. Napríklad bezpečnosť, nakoľko pojem bezpečnosť obsahuje prvky ochrany – stav ochrany pred nebezpečenstvom. Všeobecná literatúra pritom pojmy špecificky neodlišuje, často sú používané s nedocenením ich plného významu. **Z uvedeného však možno rámcovo odvodiť, že ak má existovať ochrana, musí existovať jav – skutočnosť, na ktorý má ochrana pôsobiť, resp. pred ktorým má ochraňovať, pričom ide o vlastnú podstatu ochrany.** Pri hľadaní odpovedí na otázky spojené s funkčnou podstatou ochrany tak, ako sme ich už uviedli, možno hovoriť o ochrane ako o systéme pozostávajúcom z troch základných prvkov: predmet ochrany (informácie), nástroj ochrany (režim utajenia), riziko (ohrozenie, nebezpečenstvo).

Je zrejmé, že z hľadiska funkčnej podstaty ochrany sa základná charakteristika a štruktúra ochrany definuje prostredníctvom uvedených pojmov vcelku jasne. Z hľadiska manažmentu bezpečnostných rizík a definovania jeho vzťahu k OUS je

[2] Pozri bližšie § 53 ods. 2 zákona č. 215/2004 Z.z. o OUS

[3] Porovnaj Murdza, K.,Bezpečnosť a bezpečnostná orientácia v globálnej rizikovej spoločnosti, A PZ Bratislava 2005, str. 80.

[4] Výkladový slovník, www.security revue.com, rovnako Krátky slovník slovenského jazyka, SAV, Bratislava 1997.

možné uviesť, že **identifikácia rizík je integrálnou súčasťou systému ochrany**. Je však potrebné sa vysporiadať s určitou nejasnosťou vzťahov medzi rizikom, nebezpečenstvom a ohrozením.

Ak by sme brali do úvahy významy uvedených jednotlivých slov len podľa zaužívaných slovníkov slovenského jazyka, pravdepodobne by sme nenašli významový rozdiel medzi slovami riziko[5] a nebezpečenstvo[6]. V literatúre sa často uvádzajú dve základné koncepcie rizika, ktoré sa odlišujú prístupmi k jeho interpretácii – realistický a sociokultúrny[7]. Realistický prístup charakterizuje riziko ako objektívny a poznateľný fakt (potenciálna hrozba alebo zapríčinená škoda), ktorý môžeme zmerať. Sociokultúrny prístup kladie dôraz na sociálne a kultúrne kontexty vzniku rizika. Ak uvedené prístupy porovnáme s definíciou rizika tak, ako ho ponímajú oblasti bezpečnostného manažmentu,[8] zistíme, že majú spoločné črty s definíciou rizika podľa realistického prístupu. **To znamená, že riziko by malo byť merateľné a miera rizika adekvátne vyjadriteľná** (vysoké, nízke, stredné, prijateľné, mierne a pod.) Tento prístup umožňuje hodnotenie rizika, jeho vyjadrenie s cieľom vyhnúť sa dôsledkom a stratám a je podľa nášho názoru akceptovateľný pre systém OUS.

Bezpečnostné riziko[9] sa definuje ako výsledok pôsobenia bezpečnostnej situácie (vnútornej a vonkajšej), ktorej prejavy môžu prerásť do bezprostredného ohrozenia subjektu bezpečnosti (informácia, jedinec, skupina, štát). Súhlasíme s vnímaním bezpečnostného rizika ako pravdepodobnej, viac či menej reálnej hrozby ohrozenia integrity určitého subjektu (informácie). **Bezpečnostné riziko v systéme OUS** by malo predstavovať komplexne ponímanú štruktúru, ktorá aktivuje sebaregulačné mechanizmy smerujúce k obnoveniu rovnováhy, a to formou tak preventívnych, ako aj reparačných krokov.[10] V súlade s uvedeným je z pohľadu osoby rizikom možné vyzradenie utajovanej skutočnosti alebo niektoré jej nežiaduce charakterové črty (nečestnosť, nespoľahlivosť), pričom z pohľadu štátu je tieto možné vnímať ako nebezpečenstvo. Na minimalizáciu alebo elimináciu nebezpečenstva pre štát je teda potrebné eliminovať, či minimalizovať riziká osôb. Potrebná flexibilita je napr. v oblasti personálnej bezpečnosti tvorená v predpisoch Európskej únie alebo

---

[5] Riziko - možnosť, nebezpečenstvo straty, škody, Krátky slovník slovenského jazyka, SAV, Bratislava 1997,str. 595.

[6] Nebezpečenstvo – možnosť niečoho zlého, hrozba, riziko, Krátky slovník slovenského jazyka, SAV, Bratislava 1997, str. 362.

[7] Murdza, K.,Bezpečnosť a bezpečnostná orientácia v globálnej rizikovej spoločnosti, A PZ Bratislava 2005, str. 7-8.

[8] Riziko – (možnosť, nebezpečenstvo straty, neúspechu, škody; kombinácia pravdepodobnosti, že nastane neželaná udalosť a následkov neželanej udalosti, kvantitatívne a kvalitatívne vyjadrenie ohrozenia, stupeň alebo miera ohrozenia) – je pojem na označenie skutočnosti, že existuje potenciálna možnosť narušenia bezpečnosti. Výkladový slovník, www.security revue.com,2013.

[9] Bezpečnostné riziko – (možnosť, nebezpečenstvo straty, neúspechu, škody; kombinácia pravdepodobnosti, že nastane neželaná udalosť a následkov neželanej udalosti, kvantitatívne a kvalitatívne vyjadrenie ohrozenia, stupeň alebo miera ohrozenia) – jav sociálneho charakteru, ktorý má potenciál poškodiť subjekt bezpečnosti, alebo môže mať negatívny dopad na záujmy iného subjektu.
Citované podľa : Výkladový slovník, www.security revue.com, 2013.

[10] Pozri aj Murdza, K.,Bezpečnosť a bezpečnostná orientácia v globálnej rizikovej spoločnosti, A PZ Bratislava 2005, str. 34.

severoatlantickej aliancie[11] pomyselnou pyramídou, ktorej základ tvorí previerka osoby (cielená eliminácia relatívne statických rizík), nasleduje poučenie (eliminácia ostaných rizík, spravidla dynamických) a na vrchole je tzv. princíp „need-to-know“, ktorý vo všeobecnosti umožňuje oboznamovanie sa s utajovanými informáciami len osobám, ktoré to potrebujú pre výkon svojej práce. Takéto ponímanie personálnej bezpečnosti umožňuje plnú flexibilitu v závislosti od aktuálnych rizík – súčasný zákon o OUS však toto neumožňuje. Na riziko sa zjavne nazerá z viacerých pohľadov, rovnako ako aj na niektoré vybrané pojmy súvisiace s možným výkladom ochrany a jej podstaty.

Bezpečnostné riziko a do akej miery sa podarí toto identifikovať, analyzovať a posúdiť priamo ovplyvní stav ochrany – bezpečnosti. Platí pritom rovnica, že čím lepšie a dôkladnejšie identifikujeme riziká, tým lepšie vieme nastaviť mechanizmus ochrany. Ak uvedené aplikujeme na systém OUS je zrejmé, že manažment bezpečnostných rizík by mal byť jeho integrálnou súčasťou, **inak nie je možné hovoriť o ochrane, ale len o vytváraní dojmu ochrany informácií.** Zároveň možno dôvodne predpokladať, že takýto systém (reagujúci na aktuálne bezpečnostné riziká by mal byť, s ohľadom na spôsoby vzniku rizík, dostatočne flexibilný (dynamický). Vychádzame pritom zo všeobecného spôsobu odvodzovania bezpečnostných rizík na základe analýz a hodnotení bezpečnostnej situácie – aktuálneho bezpečnostného prostredia[12].

Osobitnou časťou je schopnosť systému ochrany reagovať na predpokladané budúce zmeny bezpečnostného prostredia a jeho vývoj, a tým predchádzať vzniku negatívnych následkov.[13] Systém ochrany, ako už bolo uvedené, priamo závisí od schopnosti práce s rizikami. V tomto zmysle riziká majú priamu nadväznosť na jednak dané bezpečnostné prostredie, z ktorého vyplynuli, a jednak na systém ochrany, ktorý sa buduje na ich základe[14]. Čím užšia je väzba medzi bezpečnostným prostredím a rizikami, tým presnejšie možno definovať a vypracovať systém ochranných opatrení (napr. realizovaných daným stupňom utajenia). Ak pri hodnotení berieme do úvahy komplex všetkých troch funkčných prvkov ochrany, teda predmet, riziká a nástroje ochrany, tak dospejeme k jedinečne identifikovanému systému opatrení viažúcemu sa k určitej informácii (skupine informácií).

Riziká ako také možno členiť podľa viacerých kritérií. Sme toho názoru, že na riziká z hľadiska možnosti ich eliminácie sa dá nazerať prostredníctvom ich vnútornej štruktúry. **V tejto súvislosti môžeme hovoriť minimálne o troch**

---

[11] Security within the North Atlantic Treaty Organization (NATO) Bezpečnosť v rámci NATO, C-M(2002)49, NATO Archives – public version, 2006;Rozhodnutie rady z 31.3.2011 o bezpečnostných predpisoch na ochranu utajovaných skutočností č. 2011/292/EU, OJ L 141/17

[12] Bezpečnostné prostredie – časť spoločenského prostredia, v ktorom sú podmienky existencie a vývoja sociálnych subjektov, ich činnosti, vzťahy a záujmy determinované v prvom rade bezpečnosťou. Bezpečnostné prostredie sa charakterizuje prostredníctvom vyčlenenia určitého územia, geopoliticky relatívne uceleného, ktoré je spravidla podmienené aj ďalšími sociálno-ekonomickými, vojensko-strategickými a kultúrnohistorickými činiteľmi. Citované podľa: Výkladový slovník, www.security revue.com, 2013.

[13] Bezpečnostné výzvy - zhŕňajú situácie, ktoré vyžadujú prispôsobenie sa a adekvátne reakcie na zmeny bezpečnostného prostredia. Ich zvládnutie môže zabrániť vzniku kríz alebo ohrození alebo umožní v budúcnosti ich efektívnejšie riešenie a zaručenie bezpečnosti, Výkladový slovník, www.security revue.com, 2013.

[14] „N**edeliteľný charakter** – bezpečnosť je celostným javom subjektu, ktorý súvisí vždy s jeho systémovými väzbami“. K tomu bližšie pozri: Murdza, K., Bezpečnosť a bezpečnostná orientácia v globálnej rizikovej spoločnosti, A PZ Bratislava 2005, str. 82.

kategóriách rizík – jednoduché, zložité a komplexné riziká. V systéme OUS, ktorého základným cieľom je ochrana informácií prostredníctvom opatrení realizovaných v oblasti personálnej bezpečnosti, objektovej a fyzickej bezpečnosti a informačnej bezpečnosti možno medzi jednoduché riziká zaradiť napr. stratu, náhodnú krádež informácie, zanedbanie základných povinností pri realizácii ochranných opatrení, nehoda, nezodpovednosť. Tieto riziká možno eliminovať spravidla jednoduchými administratívnymi alebo režimovými opatreniami. Medzi zložité riziká môžeme zaradiť napr. krádež s prípravou, sociálne inžinierstvo, hacking, vydieranie (obsahuje prípravu), nežiadúce elektromagnetické vyžarovanie technických prostriedkov a iné. U týchto rizík sa predpokladá použitie zložitejších opatrení a súčinnosti ochranných opatrení z viacerých oblastí, napr. personálnych a administratívnych. **Komplexným rizikom je, podľa nášho názoru napr. špionáž**, ktorú je možné považovať za špecifické riziko a pravdepodobne najvýznamnejšie z hľadiska ochrany informácií prostredníctvom režimu utajenia. **Vychádzame pritom z predpokladu, že bez špionáže by nebolo ani utajovanie.** Podľa nás ide v podstate o dve protichodné a súčasne vzájomne podmienené a ovplyvňujúce sa aktivity. Samotnú špionáž by sme mohli charakterizovať ako cieľavedomú a systematickú činnosť zameranú na získavanie dôležitých informácií[15] (nejedná sa spravidla získavanie verejne dostupných informácii ale o získavanie informácii určených len určitej skupine osôb, čo je v prípade štátu zabezpečované režimom utajenia). Špionáž je spravidla vykonávaná s použitím širokej škály sofistikovaných a prepracovaných metód, foriem činnosti, prostriedkov a nástrojov (často ako utajovaná súčasť oficiálnej spravodajskej činnosti napr. nepriateľských spravodajských služieb).Miera realizácie ochranných protiopatrení systémom OUS závisí od miery poznania ich aktivít a zamerania činnosti. Špionáž predstavuje systém rizík, ktoré by mali byť podľa nášho názoru určujúcimi pre systém ochrany informácií utajením[16].

Sme toho názoru, že ak má byť ochrana informácií utajením efektívna je potrebné prispôsobiť realizáciu ochranných opatrení výsledkom diferencovanému prístupu k hodnoteniu rizík. V súlade s uvedeným možno uviesť, že vytvorenie štandardného balíka rizík a následných ochranných opatrení a ich uplatnenie vo vzťahu k informáciám rôzneho významu (v závislosti od možnej ujmy na záujmoch SR[17]) je nedostatočné. Príkladom je súčasné stanovovanie stupňa utajenia, kde samotný stupeň utajenia sa vzťahuje na možnú ujmu. Tento by mal v prvom rade zohľadňovať komplex opatrení, ktorými je daná informácia chránená a mal by mať preto väzbu na konkrétne riziká vo vzťahu k konkrétnej informácii. **Stupeň utajenia by mal byť vyjadrením komplexu opatrení vzťahujúcich sa na určitú oblasť bezpečnostných rizík.** Prakticky to môže znamenať, že nie výška možnej ujmy by mala by určujúca pre stanovenie stupňa utajenia (stupeň ochrany) ale práve posúdenie možných rizík vzťahujúcich sa k danej informácii. Stanovenie stupňa utajenia má potom za cieľ existujúce riziká eliminovať. Uvedené je možné vnímať aj komplexnejšie a to vo vzťahu k jednotlivým oblastiam ochranných opatrení (personálna bezpečnosť, objektová a fyzická bezpečnosť, informačná bezpečnosť), kedy je zrejmé, že ochrana

[15] Špionáž – výzvedná činnosť, vyzvedačstvo, Krátky slovník slovenského jazyka, SAV, Bratislava 1997.
[16] Takto sú vnímané aj príslušnými predpismi Severoatlantickej aliancie a Európskej únie, pozri odkaz č.12
[17] Pozri bližšie § 3 zákona o OUS

informácie by mala byť realizovaná v závislosti od špecifík situácie (napr. priestor, čas) a identifikovaných rizík. Pritom nie vždy musí dôjsť k aplikácii všetkých oblastí ochranných opatrení súčasne. Tieto by sa mali navzájom dopĺňať. Systém OUS by mal byť pritom do tej miery flexibilný aby dokázal pokryť aj neštandardné situácie (napr. OUS v poľných podmienkach). Predpokladom však je zvládnutie manažmentu bezpečnostných rizík, bez tohto nie je možné prijímať adekvátne opatrenia. Identifikovanie bezpečnostných rizík od tých najjednoduchších až po komplexné, ich vyhodnocovanie a prijímanie vhodných opatrení[18] je základom pre efektívne fungovanie systému ochrany informácií prostredníctvom režimu utajenia. Nie každé riziko však možno automaticky vzťahovať na ochranu každého predmetu ochrany

Prostredníctvom analýzy rizík a ich hodnotenia je možné identifikovať riziko, určiť jeho mieru[19] a pravdepodobnosť (výskytu) a následne navrhnúť ako riziko eliminovať. Manažment bezpečnostných rizík, ako proces komplexne zastrešujúci prácu s bezpečnostnými rizikami, by mal byť určujúcim pre správne nastavenie systému ochrany informácií prostredníctvom režimu utajenia.

LITERATÚRA

[1] Murdza, K. : Bezpečnosť a bezpečnostná orientácia v globálnej rizikovej spoločnosti, A PZ Bratislava 2005, 150 str., ISBN 80-8054-335-6

[2] Brvnišťan. M., Hnat. V.: Bezpečnostný štandard v systéme ochrany utajovaných skutočností, In Zborník zo 17. vedeckej konferencie s medzinárodnou účasťou Riešenie krízových situácií v špecifickom prostredí, Fakulta špeciálneho inžinierstva Žilinskej univerzity v Žiline, 2012, ISBN 978-80-554-0534-6, časť I, str. 63 – 70

[3] Krátky slovník slovenského jazyka, SAV, Bratislava 1997

[4] Rozhodnutie Rady EÚ z 31.3.2011 o bezpečnostných predpisoch na ochranu utajovaných skutočností č. 2011/292/EU, OJ L 141/17

[5] Security within the North Atlantic Treaty Organization (NATO) Bezpečnosť v rámci NATO, C-M(2002)49, NATO Archives – public version, 2006

[6] http:// www.securityrevue.com, výkladový slovník 2013

Článok recenzovali dvaja nezávislí recenzenti.

[18] Pozri aj Brvnišťan. M., Hnat. V.: Bezpečnostný štandard v systéme ochrany utajovaných skutočností, In Zborník zo 17. vedeckej konferencie s medzinárodnou účasťou Riešenie krízových situácií v špecifickom prostredí, Fakulta špeciálneho inžinierstva Žilinskej univerzity v Žiline, 2012, str. 65

[19] Porovnaj s pojmom relatívny charakter ochrany - Murdza, K., Bezpečnosť a bezpečnostná orientácia v globálnej rizikovej spoločnosti, A PZ Bratislava 2005, str. 82.