VYBRANÉ PROBLÉMY ANALÝZY BEZPEČNOSTNÝCH RIZÍK V SYSTÉMOCH OCHRANY INFORMÁCIÍ[1]

SELECTED PROBLEMS OF SECURITY RISKS ANALYSIS IN INFORMATION PROTECTION SYSTEMS

Miroslav BRVNIŠŤAN

ABSTRACT :

Security risk analysis is an integral part of security mechanisms, including information protection systems. The current legal framework for information protection mechanisms defines security risk analysis differently, which has undoubtedly a number of negative impacts. An increase in information security requirements is a reason to think about how to protect information. Analysis of security risks as an essential element of creating an effective information protection system is not coordinated at the level of the state, resulting in inefficiency and ultimately consequenting in a systemic failure of protective measures. The need to streamline procedures and centralise risk analysis appears to be an elementary assumption of effective information protection not only within the security system of the state, but also in the implementation of private sector information security measures.

Keywords: security risk analysis, security risk management, information protection, classified information, sensitive information, personal data, protection, classification, risk

ÚVOD:

Bezpečnostný systém štátu a schopnosť chrániť informácie súvisiace so zabezpečovaním základných funkcií štátu a bezpečnosti občanov sú oblasti, ktorých význam s rastúcim množstvom informácií a s technologickým a technickým rozvojom narastá. Tento stav je zároveň podmienený zmenami bezpečnostného prostredia v ktorom sa Slovenská republika nachádza. Typické bezpečnostné riziká, ktoré boli základom pre konštituovanie systémov ochrany informácií historicky vychádzali z relatívnej stability bezpečnostného prostredia a nízkej dynamiky. Nové (moderné) bezpečnostné hrozby a riziká vytvárajú predpoklady na prehodnotenie a re-definovanie charakteristických metód, foriem a prostriedkov riadenia a fungovania systémov ochrany informácií. Asymetrické a hybridné hrozby, vrátane kybernetických predstavujú nové podnety pre bezpečnostný systém o to viac ak ide o oblasť ochrany informácií. Zároveň aj už známe riziká ako napr. špionáž (vrátane priemyselnej špionáže), sabotáž a terorizmus nadobúdajú nové charakteristiky, ktoré ovplyvňujú systém bezpečnosti informácií. Je zrejmé, že bezpečnostné riziká je potrebné komplexne analyzovať a navrhnúť spôsoby ich efektívnej eliminácie. Dynamika zmien bezpečnostného prostredia je však v ostrom kontraste so schopnosťou bezpečnostného systému reagovať. Zotrvačnosť, komplikovanosť, formálnosť a byrokratickosť bezpečnostného systému sú pravdepodobne len jedným z viacerých aspektov, ktoré

[1] Tento príspevok je podporovaný Agentúrou na podporu výskumu a vývoja na základe Zmluvy č. APVV – 16-0521.

podmieňujú jeho (ne)spôsobilosť reagovať na nové podnety. V oblasti ochrany a bezpečnosti informácií to môže mať veľmi negatívne až fatálne dôsledky.

Vytvorenie efektívneho systému na ochranu informácií je zložitý a sofistikovaný proces. Porozumenie vzťahom medzi jednotlivými kategóriami chránených informácií, dôvodmi ich vzniku a požiadavkami na ich ochranu je založené na porozumení základných, východiskových otázok súvisiacich s analýzou bezpečnostných rizík. Aký je súčasný stav v oblasti vzniku a ochrany vybraných kategórií informácií? Je integrálnou súčasťou opatrení definovaných platnými všeobecne záväznými predpismi analýza a manažment bezpečnostných rizík? Kto zodpovedá za vykonávanie analýzy bezpečnostných rizík na úrovni štátu? Aké je miesto súkromného sektora? Na tieto otázky sa pokúsime rámcovo zodpovedať a zároveň navrhnúť možné riešenia.

Základom pre zodpovedanie položených otázok bude analýza súčasného stavu v oblasti ochrany vybraných kategórií informácií so zameraním na analýzu/manažment bezpečnostných rizík. Vychádzame pritom z predpokladu, že analýza bezpečnostných rizík by mala byť elementárnym východiskom pri vzniku takýchto informácií, ako aj pri zabezpečovaní samotnej ochrany informácií. Identifikácia bezpečnostných rizík, ich analýza a schopnosť primerane a aktuálne reagovať na nové bezpečnostné riziká charakterizujú a zároveň zásadne podmieňujú celkovú efektívnosť systému ochrany informácií.

Na podrobnejšiu analýzu sme vybrali všeobecne záväzné právne predpisy upravujúce ochranu oblasti ochrany informácií - zákon č. 215/2004 Z.z. o ochrane utajovaných skutočností a doplnení niektorých zákonov (ďalej len zákon o OUS), zákon č. 45/2011 Z.z. o kritickej infraštruktúre (ďalej len zákon o kritickej infraštruktúre) a zákon č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej len zákon o ochrane osobných údajov). S cieľom dosiahnuť čo najrelevantnejšie závery porovnáme vybrané časti uvedených všeobecne záväzných právnych predpisov s vybranými právnymi aktami Európskej únie (ďalej len EU) a Severoatlantickej aliancie (ďalej len NATO).

1. POSTAVENIE ANALÝZY BEZPEČNOSTNÝCH RIZÍK V SYSTÉMOCH OCHRANY INFORMÁCIÍ

Určenie postavenia a väzieb analýzy/manažmentu bezpečnostných rizík v ktoromkoľvek systéme ochrany informácií sa odvíja od identifikovania základných znakov systému ochrany ako takej prostredníctvom ich teoretických charakteristík.

Ochrana je oblasť, ktorej funkčný význam možno posudzovať viacerými spôsobmi. Jedným z nich je aj analýza samotného pojmu ochrana, ktorá určuje tzv. funkčnú podstatu ochrany, teda dôvodov a zmyslu jej existencie prostredníctvom odpovedí na tri fundamentálne otázky[2] : *Čo je predmetom ochrany ? Pred kým a pred čím chráni ? Akými nástrojmi sa ochrana vykonáva ?*

Prostredníctvom odpovedí na uvedené otázky je možné komplexne popísať aj ciele a dôvody existencie systémov ochrany informácií. Zároveň je tým možné, podľa nášho názoru, identifikovať a popísať postavenie a širšie väzby analýzy bezpečnostných rizík v systémoch ochrany informácií. V kontexte systémov ochrany informácií je odpoveď na prvú otázku zrejmá. Predmetom ochrany sú informácie. Ich spôsob vzniku však môže byť v jednotlivých

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

systémoch ochrany informácií odlišný, čo môže priamo ovplyvňovať hľadanie odpovedí na ďalšie otázky. *Pred kým a pred čím je potrebné informácie chrániť?* Táto otázka bude predmetom širšieho posudzovania s cieľom objasniť úlohy a dôvody existencie analýzy bezpečnostných rizík vo vybraných systémoch ochrany informácií. Z hľadiska naplnenia cieľa tohoto článku sa nebudeme zaoberať nástrojmi ochrany.

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).[3] 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 následne hovoriť o ochrane ako o systéme pozostávajúcom z troch základných prvkov: predmet ochrany (informácia - utajovaná informácia, osobný údaj a pod.), nástroj ochrany (napr. režim utajenia, šifrovanie, evidencia informácií, personálna bezpečnosť), 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 analýzy a následne manažmentu bezpečnostných rizík a definovania jeho vzťahu k systémom ochrany informácií je možné uviesť, že *identifikácia rizík by mala byť východiskom a integrálnou súčasťou systémov ochrany. V absolútnom ponímaní možno uviesť, že analýza bezpečnostných rizík je dôvodom na vznik režimov ochrany informácií.* Takéto konštatovanie by mohlo byť zároveň aj dôvodom na hľadanie odpovede na otázku - *Aké sú dôvody na kreovanie odlišných systémov ochrany informácií? Existujú tak odlišné bezpečnostné riziká?*

Predpokladáme, že identifikácia rizík a manažment rizík sa prejavili v ich zapracovaní do jednotlivých zákonov, ktoré budú predmetom analýzy. Bezpečnostné riziko[4] sa definuje ako výsledok pôsobenia bezpečnostnej situácie (vnútornej a vonkajšej), ktorej prejavy môžu prerásť do bezprostredného ohrozenia subjektu bezpečnosti (informácia, jedinec, skupina, štát). *Bezpečnostné riziko v systéme ochrany informácií* by malo predstavovať komplexne ponímanú štruktúru, ktorá aktivuje sebaregulačné mechanizmy smerujúce k obnoveniu rovnováhy, a to formou tak preventívnych, ako aj reparačných krokov.[5] Takéto ponímanie umožňuje plnú flexibilitu v závislosti od aktuálnych rizík – priama reakcia na dynamiku bezpečnostného prostredia (napr. platný zákon o OUS uvedené

---

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

[4] 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, 2018.

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

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 to do akej miery sa podarí riziko identifikovať, analyzovať a posúdiť priamo ovplyvní stav ochrany – bezpečnosti informácií. Ak uvedené aplikujeme na posudzované systémy ochrany informácií je zrejmé, že analýza a manažment bezpečnostných rizík by mal byť ich integrálnou súčasťou, *inak nie je možné hovoriť o ochrane, ale len o vytváraní dojmu ochrany informácií.* Zároveň možno dôvodne predpokladať, že takéto systémy (reagujúce na aktuálne bezpečnostné riziká by mali byť, s ohľadom na spôsoby vzniku rizík, dostatočne flexibilné (dynamické). Vychádzame pritom zo všeobecného spôsobu odvodzovania bezpečnostných rizík na základe analýz a hodnotení bezpečnostnej situácie – aktuálneho bezpečnostného prostredia[6].

Osobitnou časťou je schopnosť systému ochrany informácií reagovať na aktuálne zmeny a predpokladané budúce zmeny bezpečnostného prostredia a jeho vývoj, a tým predchádzať vzniku negatívnych následkov.[7] Systém ochrany informácií, 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 informácií, ktorý sa buduje na ich základe[8]. *Čím užšia je väzba medzi bezpečnostným prostredím a rizikami, tým presnejšie možno definovať a vypracovať (jedinečný) systém ochranných opatrení (napr. realizovaných daným stupňom utajenia informácie).*

Bezpečnostné 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 kategóriách rizík – jednoduché, zložité a komplexné riziká. V systémoch ochrany informácií, ktorých základným cieľom je ochrana informácií prostredníctvom opatrení realizovaných napr. 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, zneužitie. Tieto riziká možno eliminovať spravidla jednoduchými administratívnymi, technickými alebo režimovými opatreniami. Medzi zložité riziká môžeme zaradiť napr. krádež s prípravou, sociálne inžinierstvo, hacking, vydieranie (obsahuje prípravu), nežiadúce elektromagnetické vyžarovanie technických prostriedkov, kybernetický útok 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* ako systematické vyhľadávanie, získavanie a zhromažďovanie informácií za využitia sofistikovaných technických a technologických prostriedkov. Špionáž vykonávanú štátmi, priemyselnú špionáž vykonávanú súkromnými subjektami alebo štátmi je možné považovať

---

[6] 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, 2018.

[7] 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, 2018.

[8] „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.

za špecifické riziko a pravdepodobne najvýznamnejšie z hľadiska systémov ochrany informácií[9].

Sme toho názoru, že ak má byť ochrana informácií 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 (napr. v závislosti od možnej ujmy na záujmoch SR[10]) je nedostatočné. *Bezpečnostné opatrenia by mali byť vyjadrením komplexu opatrení vzťahujúcich sa na určitú oblasť bezpečnostných rizík.* Systémy ochrany informácií by mali byť pritom do tej miery flexibilné aby dokázali reagovať v čase na priamo sa meniacu bezpečnostnú situáciu.

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*[11] je základom pre efektívne fungovanie systému ochrany informácií. *Prostredníctvom analýzy rizík a ich hodnotenia je možné identifikovať riziko, určiť jeho mieru*[12] *a pravdepodobnosť (výskytu) a následne navrhnúť ako riziko eliminovať.* Analýza a manažment bezpečnostných rizík, ako proces komplexne zastrešujúci prácu s bezpečnostnými rizikami, by mal byť určujúcim pre správne nastavenie systémov ochrany informácií.

2. MIESTO ANALÝZY BEZPEČNOSTNÝCH RIZÍK VO VYBRANÝCH SYSTÉMOCH OCHRANY INFORMÁCIÍ

Systémy ochrany informácií boli kreované za účelom ochrany špecifických kategórii informácií. Ako sme však v prvej časti uviedli princípy ochrany ako takej sú rovnaké a týkajú sa aj systémov ochrany informácií. Odlišnosti systémov ochrany informácií je možné identifikovať na základe ich posúdenia prostredníctvom odpovedí na otázky tvoriace funkčnú podstatu ochrany. Až následne je možné vyhodnotiť spôsobilosť jednotlivých systémov ochrany informácií eliminovať známe bezpečnostné riziká prostredníctvom manažmentu bezpečnostných rizík *Aký je súčasný stav v systémoch ochrany informácií pokiaľ ide o aplikáciu analýzy a manažmentu bezpečnostných rizík?*

2.1 SYSTÉM OCHRANY INFORMÁCIÍ PROSTREDNÍCTVOM REŽIMU UTAJENIA - ZÁKON O OUS

Predmetom ochrany poskytovanej touto právnou normou sú utajované skutočnosti a ich ochrana. Pod utajovanou skutočnosťou sa rozumie informácia alebo vec určená pôvodcom utajovanej skutočnosti, ktorú vzhľadom na záujem Slovenskej republiky treba chrániť pred

---

[9] Takto sú definované aj príslušnými predpismi Severoatlantickej aliancie a Európskej únie, pozri odkaz č.10.

[10] Pozri bližšie § 3 zákona o OUS.

[11] 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.

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

vyzradením, zneužitím, poškodením, neoprávneným rozmnožením, zničením, stratou alebo odcudzením (ďalej len „neoprávnená manipulácia“) a ktorá môže vznikať len v oblastiach, ktoré ustanoví vláda Slovenskej republiky svojím nariadením[13].

Z hľadiska systému bezpečnosti je zrejmé, že kľúčovým je identifikovanie informácie a jej hodnoty vo vzťahu k záujmom štátu. Až následne jej adekvátnym označením je možné realizovať ochranné opatrenia v závislosti od stupňa utajenia. Samotný systém vzniku utajovanej informácie je zložitý, posudzovanie možnej ujmy na záujmoch štátu ako základ pre určenie stupňa utajenia (stupeň utajenia = definované ochranné opatrenia) je nejasné, pričom ani neexistuje relevantný kontrolný mechanizmus na posúdenie či určitá informácia by mala byť utajovanou skutočnosťou alebo nie. Ak pôvodca informáciu pri jej vzniku neoznačí a teda neutají, spätne to už nie je možné urobiť[14].

Možná analýza bezpečnostných rizík je priamo ovplyvnená spôsobom vzniku utajovaných informácií, vrátane zverejňovania rezortných zoznamov utajovaných skutočností[15]. Systém ochrany informácií definovaný zákonom o OUS však nepredpokladá analýzu bezpečnostných rizík pri vzniku (dôvod) utajovanej informácie, obdobne ani pri stanovovaní stupňa utajenia.

Spôsob ochrany utajovaných informácií je realizovaný prostredníctvom vytvárania podmienok (nástrojov) na personálnu bezpečnosť, administratívnu bezpečnosť, šifrovú ochranu informácií, fyzickú bezpečnosť, objektovú bezpečnosť, bezpečnosť technických prostriedkov a na priemyselnú bezpečnosť**[16].** Ide o fixný systém predpokladaných ochranných opatrení, ktorých zmena je možná iba zmenou zákona o OUS!

Jednotlivé oblasti ochranných opatrení stanovujú opatrenia vyplývajúce z podstaty danej oblasti, napr. personálna bezpečnosť stanovuje opatrenia súvisiace s výberom, určením a kontrolou osôb, ktoré sa môžu oboznamovať s utajovanými skutočnosťmi; oblasť administratívnej bezpečnosti upravuje opatrenia súvisiace s ochranou utajovaných skutočností pri ich tvorbe, príjme, evidencii, preprave, ukladaní, rozmnožovaní, vyraďovaní a uchovávaní alebo pri inej manipulácii. *Je zrejmé, že ide o pokus zameraný na konečný (fixný) výpočet činností smerujúcich k ochrane informácií. S ohľadom na dynamiku bezpečnostného prostredia sa môže vyskytnúť aj nové riziko, ktoré však bez zmeny zákona o OUS nebude možné zohľadniť vo vzťahu k bezpečnosti informácií.*

Zákon o OUS priamo nestanovuje pri realizácii jednotlivých oblastí ochranných opatrení povinnosť analýzy rizík, skôr naopak sa zdá, že tvorcovia pri jeho príprave predpokladali, že navrhnú dostatočne robustný systém odolný voči všetkým známym rizikám. Analýza rizík je čiastkovo riešená prostredníctvom vykonávacích vyhlášok k zákonu o OUS[17], čo však nepredstavuje systémový prístup k ochrane informácií a ani nerieši potrebnú flexibilitu.

Odlišná situácia je v prípade relevantných predpisov EU a NATO. Ide pritom často o ochranu tých istých utajovaných informácií, vznikajúcich na rovnakom teritóriu, v rovnakom bezpečnostnom prostredí a rámci jedného nadnárodného integračného zoskupenia (organizácie).

---

[13] §2 písm. a) zákona o OUS.

[14] Pozri bližšie Brvnišťan, M. : Rozhodnutie o utajení ako základný predpoklad realizácie ochranných opatrení, In Zborník vedeckých a odborných prác, 8. Medzinárodná vedecká konferencia Národná a medzinárodná bezpečnosť 2015, Akadémia ozbrojených síl generála Milana Rastislava Štefánika 2017, str. 324.

[15] Pozri Nariadenie vlády č. 216/2004 Z.z., ktorým sa ustanovujú oblasti utajovaných skutočností.

[16] §6 ods. 2 zákona o OUS.

[17] Pozri napr. Vyhláška č. 336/2004 Z. z. o fyzickej bezpečnosti a objektovej bezpečnosti, Vyhláška č. 339/2004 Z.z. o bezpečnosti technických prostriedkov.

Podľa bezpečnostnej politiky NATO - C-M(2002)49 je predmetom ochrany utajovaná informácia alebo materiál, ktorý vyžaduje *ochranu pred neautorizovaným zverejnením*[18]. Definuje sa tu základný princíp ochrany, ktorým je manažment bezpečnostných rizík a vybudovanie bezpečnostnej autority zodpovednej za zber a hodnotenie spravodajských informácií týkajúcich sa špionáže, sabotáže a podvratných hrozieb[19].
Je zrejmé, že zámerom tvorcov bolo nielen implementovať systém manažmentu rizík priamo do bezpečnostnej politiky NATO (záväznej pre členské krajiny), ale aj vytvorenie vhodných podmienok prostredníctvom zriadenia centrálnej bezpečnostnej autority. Zároveň sú jednoznačne definované a pomenované kľúčové bezpečnostné riziká.
Podľa záväzných predpisov EÚ je predmetom ochrany utajovaná skutočnosť EÚ, ktorou je každá informácia alebo vec označená stupňom utajenia EÚ, *neoprávnená manipulácia* s ktorou by mohla v rôznej miere poškodiť záujmy Európskej únie alebo jedného alebo viacerých členských štátov[20].

Spôsob ochrany je realizovaný rozhodnutím Rady EU, ktorým sa ustanovujú základné zásady a minimálne normy bezpečnosti na ochranu utajovaných skutočností EÚ (jednotlivé oblasti ochranných opatrení sú obdobné ako v systéme SR a NATO)[21]. *Zároveň sa definuje riadenie bezpečnostných rizík, ktoré sa uskutočňuje ako proces.* Tento proces sa zameriava na určenie známych bezpečnostných rizík, stanovenie bezpečnostných opatrení na zníženie týchto rizík na prijateľnú úroveň v súlade so základnými zásadami a minimálnymi normami stanovenými v tomto rozhodnutí a na uplatňovanie týchto opatrení v súlade s koncepciou hĺbkovej ochrany. Účinnosť týchto opatrení sa neustále vyhodnocuje. Bezpečnostné opatrenia na ochranu utajovaných skutočností EÚ počas celého ich životného cyklu zodpovedajú najmä ich stupňu utajenia, podobe a množstvu informácií alebo vecí, miestu, kde sa nachádzajú zariadenia, v ktorých sa utajované skutočnosti EÚ uchovávajú, a ich konštrukcii, stanovenej lokálnej úrovni ohrozenia škodlivými a/alebo trestnými činnosťami vrátane *špionáže, sabotáže a terorizmu*[22]**.** Opätovne je tu jednoznačne určený systém analýzy a manažmentu bezpečnostných rizík a sú pomenované kľúčové bezpečnostné riziká.

Možno konštatovať, že v systéme OUS je analýza bezpečnostných rizík využitá rôzne a je priamo alebo nepriamo definovaná. Vznik utajovanej informácie je z pohľadu eliminácie bezpečnostných rizík a realizácie ochranných opatrení v danom stupni utajenia komplikovaný a nejednoznačný (nekontrolovaný) proces. *Pri samotnom vzniku utajovanej informácie pôvodcom sa nepredpokladá vyhodnocovanie bezpečnostných rizík ako dôvod na zaradenie informácie do utajovaného (ochranného) režimu. Znamená to, že pôvodca nemá vedomosť o tom aké riziká existujú vo vzťahu k určitej informácií, systém to ani nevyžaduje. Naopak, pôvodca informáciu zaradí do režimu utajenia a stanoví stupeň ochrany na základe "vyhodnotenia" možnej ujmy na záujmoch štátu. Takáto konštrukcia je ako sme uviedli nefunkčná a neefektívna.*

---

18 Príloha "A" Annex 1 písm. a) bezpečnostnej politiky NATO.

19 Pozri bližšie bod 5.1 a 5.2. Bezpečnostnej politiky NATO.

20 Článok 2 bod č.1 Rozhodnutia Rady z 23. septembra 2013, č. 2013(488)EU o bezpečnostných predpisoch na ochranu utajovaných informácií.

21 Článok 1 Rozhodnutia Rady z 23. septembra 2013, č. 2013(488)EU o bezpečnostných predpisoch na ochranu utajovaných informácií.

22 Článok 5 Rozhodnutia Rady z 23. septembra 2013, č. 2013(488)EU o bezpečnostných predpisoch na ochranu utajovaných informácií.

Z hľadiska eliminácie bezpečnostných rizík preto zákon o OUS predstavuje snáď nástroj ochrany pred bezpečnostnými rizikami, ktoré existovali v čase jeho vzniku. Zákon o OUS nepredpokladá flexibilitu ochrany informácií v čase a v závislosti od vývoja bezpečnostnej situácie. Spôsob vzniku utajovaných informácií, tvorba zoznamov utajovaných skutočností tomu nasvedčujú. V prípade posúdenia vykonávacích predpisov je zrejmé, že v závislosti od oblasti ochranných opatrení (napr. personálna alebo informačná bezpečnosť) je situácia odlišná. Zatiaľ čo v prípade oblasti personálnej bezpečnosti[23] sú riziká stanovené exaktne (nemenné bez zmeny predpisu), tak napr. v oblasti objektovej bezpečnosti a fyzickej bezpečnosti a bezpečnosti informačnej sa predpokladá vykonanie analýzy bezpečnostných rizík a prispôsobenie úrovne ochrany v danom stupni utajenia bezpečnostným rizikám. Ako nekoncepčné sa javí stav kedy zákon o OUS analýzu bezpečnostných rizík nepozná, no niektoré vykonávacie predpisy áno.

Z predmetnej stručnej analýzy takisto vyplýva, že bezpečnostné riziká sú v systémoch OUS určované rôzne. Zásadné sú uvedené priamo v príslušných predpisoch (NATO a EÚ) a iné sú výsledkom aktuálnej analýzy bezpečnostných rizík. V systéme ochrany utajovaných skutočností SR definovanom zákonom o OUS nie je priamo aplikovaný ani jeden spôsob. Je preto na posúdenie stav zabezpečenia vzájomnej kompatibility systémov OUS SR, NATO a EÚ. Analýza bezpečnostných rizík vo vzťahu k ochrane informácií utajením vyžaduje komplexný prístup, ktorého výsledkom by mal byť kompatibilný proces SR-NATO-EÚ práce s bezpečnostnými rizikami tak, aby bola relevantne zabezpečená ochrana národných a aj spoločných informácií v rámci nadnárodných integračných zoskupení.

Porovnaním predpisov SR, NATO a EÚ je možné konštatovať, že SR tieto dodnes nezosúladila. Ide nielen o chýbajúci manažment bezpečnostných rizík ako základný predpoklad funkčného systému ochrany informácií, ale aj o následne chýbajúcu flexibilitu a aktuálnosť systému ochrany informácií aplikovaného na území SR. Tento nie je spôsobilý reagovať na nové hrozby a riziká a zároveň nie je spôsobilý poskytovať obdobnú úroveň bezpečnosti informáciám zdieľaným v rámci NATO a EÚ.

Analýza bezpečnostných rizík by mala byť integrálnou súčasťou systému ochrany utajovaných skutočností - od dôvodov vzniku utajenia informácie, vzniku a realizácie ochranných opatrení až po ich hodnotenie.

2.2. ZÁKON O KRITICKEJ INFRAŠTRUKTÚRE :

Predmetom ochrany poskytovanej touto právnou normou sú prvky kritickej infraštruktúry a súvisiace citlivé informácie. Bezpečnosť citlivých informácií vychádza z predpokladu, že získanie, zverejnenie určitých informácií o prvku kritickej infraštruktúry môže ohroziť jeho bezpečnosť[24]. Ide o priamu súvislosť medzi bezpečnosťou prvku kritickej infraštruktúry a súvisiacimi informáciami.

---

[23] Systém OUS nepredpokladá flexibilnú reakciu na základe aktuálneho vyhodnotenia bezpečnostnej situácie. Uvedené by mohlo v oblasti personálnej bezpečnosti prakticky znamenať, že napr. príslušnosť k určitej skupine - občianskemu združeniu alebo ich podpora (Slovenský branci, Noční vlci) by mohlo byť považované za bezpečnostné riziko. Pozn. autora.

[24] Pozri bližšie §2 písm. k) Zákona č. 45/2011 Z.z. o kritickej infraštruktúre, ktoré znie: Citlivou informáciou o kritickej infraštruktúre (ďalej len „citlivá informácia“) neverejná informácia, ktorej zverejnenie by sa mohlo zneužiť na činnosť smerujúcu k narušeniu alebo zničeniu prvku.

Prvok kritickej infraštruktúry (ďalej len „prvok“) je definovaný zákonom o kritickej infraštruktúre, ide o najmä inžiniersku stavbu, službu vo verejnom záujme a informačný systém v sektore kritickej infraštruktúry, ktorých narušenie alebo zničenie by malo podľa sektorových kritérií a prierezových kritérií závažné nepriaznivé dôsledky na uskutočňovanie hospodárskej a sociálnej funkcie štátu, a tým na kvalitu života obyvateľov z hľadiska ochrany ich života, zdravia, bezpečnosti, majetku, ako aj životného prostredia[25].
Ochrana prvkov kritickej infraštruktúry je založená na identifikovaní bezpečnostných rizík - §2 pím. i), j) predmetného zákona[26]. Obdobne je možné z §10 - Bezpečnostný plán identifikovať potrebu vykonania bezpečnostnej analýzy.
Z ohľadom na uvedené skutočnosti je zrejmé, že zákon o ochrane kritickej infraštruktúry odvádza samotný vznik a bezpečnosť citlivých informácií od prvkov kritickej infraštruktúry a ich bezpečnosti. Citlivé informácie sú integrálnou súčasťou bezpečnosti jednotlivých prvkov a vzťahuje sa na ne preto rovnaká ochrana ako na samotný prvok kritickej infraštruktúry. Je pritom jednoznačné, že systém bezpečnosti je založený na identifikácii, analýze a manažmente bezpečnostných rizík.
Ako určitý nedostatok sa javí nedostatok metodiky a procesu zjednocovania definovania a analýzy bezpečnostných rizík vo vzťahu k bezpečnosti prvkov kritickej infraštruktúry.

2.3. ZÁKON O OCHRANE OSOBNÝCH ÚDAJOV

Predmetom ochrany sú osobné údaje fyzických osôb[27]. Už zo samotnej definície je zrejmé, že zákon explicitne nevymenúva čo všetko je možné považovať za osobný údaj. Rámcová - otvorená definícia svedčí o snahe vytvoriť flexibilný rámec pre výklad pojmu osobný údaj.

Z hľadiska systému bezpečnosti je zrejmé, že zákon vytvára predpoklady pre bezpečnosť osobných údajov, zároveň však už z podstaty definície je zrejmé, že určité spektrum informácií o osobách na základe ktorých je tieto možné identifikovať, síce v súčasnosti nie je považovaných za osobný údaj, no nie je vylúčené, že v budúcnosti to tak môže byť. Súvisí to najmä s rýchlym technologickým rozvojom, ktorý prináša nové výzvy z hľadiska možností identifikácie osôb (napr. individuálny spôsob písania na klávesnici, nákupné zvyky, biopole, mimika, dynamická IP adresa a pod.). Je diskutabilné či je (bude) možné zabezpečiť ochranu osobných údajov, ktoré sú (boli) dobrovoľne a volne zdielané. Zaujímavým sa javí aj pohľad na samotnú podstatu bezpečnosti osobných údajov, kde imanentným cieľom je zabezpečenie účinnej kontroly jednotlivcov nad svojimi osobnými údajmi.

---

[25] §2 písm a) Zákona č. 45/2011 Z.z. o kritickej infraštruktúre.

[26] Pozri bližšie §2 písm i) a j) Zákona č. 45/2011 Z.z. o kritickej infraštruktúre:
i) ochranou prvku zabezpečenie funkčnosti, integrity a kontinuity činnosti prvku s cieľom predísť, odvrátiť alebo zmierniť hrozbu jeho narušenia alebo zničenia,
j) analýzou rizík sektora dokument, ktorý obsahuje posúdenie hrozby narušenia alebo zničenia sektora, jeho zraniteľné miesta, ako aj predpokladané dôsledky narušenia alebo zničenia sektora.

[27] Pozri bližšie §2 Zákona o ochrane osobných údajov, ktorý znie: Osobnými údajmi sú údaje týkajúce sa identifikovanej fyzickej osoby alebo identifikovateľnej fyzickej osoby, ktorú možno identifikovať priamo alebo nepriamo, najmä na základe všeobecne použiteľného identifikátora, iného identifikátora, ako je napríklad meno, priezvisko, identifikačné číslo, lokalizačné údaje,[1)] alebo online identifikátor, alebo na základe jednej alebo viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú identitu, fyziologickú identitu, genetickú identitu, psychickú identitu, mentálnu identitu, ekonomickú identitu, kultúrnu identitu alebo sociálnu identitu.

Zákon o ochrane osobných údajov vychádza z nariadenia o ochrane osobných údajov - GDPR[28] ktorý sa začal v rámci EÚ uplatňovať 25. mája 2018. Text nariadenia je automaticky záväzný pre členské krajiny a je od dátumu účinnosti priamo vykonateľný. Ako taký, nemusel byť prenesený do národnej legislatívy žiadnou z členských krajín, no SR sa rozhodla vlastnou cestou a nariadenie GDPR „preklopila“ do samostatného zákona. Nakoľko zákon o ochrane osobných údajov podstatnou mierou kopíruje nariadenie GDPR, nebudeme sa ním pre účely tohto článku zaoberať.

Analýza bezpečnostných rizík a manažment bezpečnostných rizík sú explicitne riešené vo viacerých ustanoveniach zákona o osobných údajoch. Umožňujú potrebnú flexibilitu. Vykonávanie analýzy bezpečnostných rizík je definované napr. v §31 ods. 1 nasledovne: ”S ohľadom na povahu, rozsah a účel spracúvania osobných údajov a na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva fyzickej osoby je prevádzkovateľ povinný prijať vhodné technické a organizačné opatrenia. V §32 ods.1 je uvedené: “Prevádzkovateľ je povinný pred spracúvaním osobných údajov zaviesť a počas spracúvania osobných údajov mať zavedenú špecificky navrhnutú ochranu osobných údajov, ktorá spočíva v prijatí primeraných technických a organizačných opatrení…”.

Obdobne, no priamo je predpoklad analýzy rizík stanovený v §39, ktorý definuje opatrenia k bezpečnosti spracúvania osobných údajov[29]. Pričom tu zároveň definuje aké opatrenia sa môžu využiť, napr. pseudonymizáciu a šifrovanie osobných údajov. Zároveň sa v ods.2 uvádza výpočet možných rizík, ktoré je potrebné zohľadniť: “ *prihliada sa na riziká , ktoré predstavuje spracúvanie osobných údajov, a to najmä náhodné zničenie alebo nezákonné zničenie, strata, zmena alebo neoprávnené poskytnutie prenášaných osobných údajov, uchovávaných osobných údajov alebo inak spracúvaných osobných údajov, alebo neoprávnený prístup k takýmto osobným údajom*”.

Ako je zrejmé z uvedeného dosiahnutie potrebnej úrovne bezpečnosti osobných údajov a zachovanie garantovaných práv osôb pri ich spracúvaní je cieľ, ktorý je možné dosiahnúť len vytvorení dostatočne sofistikovaného a flexibilného ochranného systému. Tento musí byť schopný reagovať na aktuálne ako aj budúce bezpečnostné riziká. Práve jasne umožnená flexibilita, založená na analýza rizík je tým správnym nástrojom.

Vzniká tu však zároveň otázka či a ako bude možné kontrolovať spôsob a mieru ochrany osobných údajov. Neustály technický a technologický pokrok je v rukách súkromných spoločností, ktoré nielen spracúvajú osobné údaje ale aj vytvárajú sofistikované prostredie, bezpečnosť ktorého je náročné zabezpečiť (typickým príkladom sú nadnárodné spoločnosti ako GOOGLE, FACEBOOK a iné. Štát a jeho kontrolné a bezpečnostné zložky úplne závisia na súkromných spoločnostiach. Hodnotenie rizík je spravidla vykonávané súkromnými spoločnosťami, ktoré kopírujú vývoj tejto oblasti a to aj pre účely verejnej a štátnej správy. Opätovne možno konštatovať, že v súčasnosti neexistuje zjednocujúci dokument, ktorý by rámcovo poskytoval základné východiská pre analýzu bezpečnostných rizík v oblasti ochrany osobných údajov. Je pritom zrejmé, že analýzu rizík je potrebné vykonať pre množstvo súkromných a štátnych subjektov. *Minimálne v rámci štátu je potrebné pouvažovať nad*

---

[28]Nariadenie Európskeho parlamentu a rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov).

[29] Ods.1 §39 znie: Prevádzkovateľ a sprostredkovateľ sú povinní prijať so zreteľom na najnovšie poznatky, na náklady na vykonanie opatrení, na povahu, rozsah, kontext a účel spracúvania osobných údajov a na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva fyzických osôb primerané technické a organizačné opatrenia na zaistenie úrovne bezpečnosti.

strategickým zastrešením a koordináciou analýzy rizík v záujme dosiahnutia rovnakých štandardov bezpečnosti osobných údajov občanov.

ZÁVER:

Analýza a manažment bezpečnostných hrozieb sú kľúčovými aspektami, ktoré priamo ovplyvňujú kreovanie a celkovú efektívnosť systémov ochrany informácií. **Analýzu bezpečnostných rizík je potrebné vnímať minimálne z dvoch perspektív - ako predpoklad vzniku systému ochrany a ako integrálnu, neodlučiteľnú súčasť realizovaných bezpečnostných opatrení.** Bezpečnosť informácií bez znalosti bezpečnostných rizík nie je možné realizovať. Súčasný stav v oblasti analýzy rizík, napriek niektorým čiastkovým zmenám, zotrváva na prekonaných funkčných, inštitucionálnych, legislatívnych pravidlách, postupoch a väzbách, ktoré nedostatočne reflektujú aktuálny vývoj a dynamiku bezpečnostných hrozieb a prostredia. Analýza bezpečnostných rizík je v systémoch ochrany informácií inkorporovaná rôzne, nerobí sa koordinovane, nie je riadená na štátnej ani výkonnej úrovni. Niektoré právne normy ako napr. zákon o OUS ju ani systémovo nedefinujú. Tento stav je potrebné zmeniť. Vytvorenie efektívneho mechanizmu na ochranu informácií je sofistikovaný proces, ktorý si vyžaduje účinnú stratégiu založenú na komplexnej analýze rizík, permanentnom monitorovaní rizikových faktorov a ich analýze a manažmente. Výsledky analýz by mali byť dostupné v čase pre všetky subjekty podieľajúce sa na ochrane informácií. Práve dôležitosť aktuálnych informácií o bezpečnostných hrozbách a ich spôsobilosti ohroziť bezpečnosť informácií pritom rapídne narastá spolu s meniacou sa dynamikou bezpečnostného prostredia a nárastom moderných bezpečnostných hrozieb.

Systémy ochrany informácií sú súčasťou bezpečnosti štátu a bezpečnostného systému štátu, napriek tomu im nie je venovaná dostatočná pozornosť. Nedostatky, na ktoré sme poukázali je potrebné postupne odstrániť a venovať pozornosť opatreniam na zefektívnenie ochrany informácií. Medzi takéto je možné zaradiť zlepšenie inštitucionálneho a legislatívneho rámca manažmentu bezpečnostných rizík, vrátane určenia ich horizontálnej a vertikálnej štruktúry.

Cieľom by malo byť vybudovanie efektívneho systému manažmentu rizík na úrovni štátu (financovanie, zodpovednosť inštitúcií a subjektov), ktoré umožní riadenie zvládania bezpečnostných rizík v oblastiach bezpečnosti informácií, prípadne využiteľných aj v iných oblastiach bezpečnosti. Za najdôležitejšie však považujeme uvedomenie si a identifikáciu bezpečnostných rizík. Zastávame názor, že pre oblasť bezpečnosti informácií by mal byť v spolupráci so všetkými relevantnými orgánmi, organizáciami a inštitúciami na štátnej úrovni (napr. spravodajské služby, Národný bezpečnostný úrad, Úrad na ochranu osobných údajov, MV SR) vytvorený základný katalóg bezpečnostných rizík. Tento by mal slúžiť na vytvorenie všeobecnej vedomostnej základne pre posudzovanie bezpečnostných rizík, obsahovať identifikáciu bezpečnostných rizík a zabezpečovať ich pravidelnú aktualizáciu. Takto vytvorený systém by mohol umožniť riadenie bezpečnostných rizík pre jednotlivé fázy ochrany informácií - od vzniku chránených informácií, prevencie únikov, varovania a informovania subjektov o aktuálnych rizikách až po zvládanie ohrození a ich hodnotenie.

Základná, na úrovni štátu, analýza bezpečnostných rizík a katalóg bezpečnostných rizík by mal nesporne viacero výhod. V prvom rade by zabezpečil zníženie nákladov na množstvo analýz bezpečnostných rizík, ktoré sa vykonávajú pre rôzne subjekty samostatne a

takisto samostatne ako súčasť rôznych oblastí ochrany informácií. V druhom rade by sa tým zabezpečila jednotná, koordinovaná úroveň bezpečnosti chránených informácií v rámci štátu - rovnaký štandard bezpečnosti pre rovnaké kategórie informácií. V treťom rade by bolo možné takto zabezpečiť kontrolu realizovaných opatrení, porovnanie štandardov ochrany a celkovej efektívnosti systémov ochrany informácií, vrátane efektívneho zapojenia sa do nadnárodných ochranných režimov ochrany informácií a dodržiavanie záväzných predpisov nadnárodných integračných zoskupení. Relevantnou otázkou takisto ostáva či samotné dodržiavanie predpisov o ochrane informácií je postačujúce na ich ochranu - Postup podľa zákona znamená bezpečnosť? Dynamika bezpečnostných hrozieb a napr. rola súkromného sektora v oblasti bezpečnosti informácií sú v príkrom rozpore so "statikou" legislatívneho procesu a inštitúcií. Čoraz viac budeme čeliť situáciám kedy systém identifikuje nové bezpečnostné riziko, ale podľa platných zákonov nebudeme môcť prijať adekvátne opatrenia.
Budúcnosť ochrany informácií preto závisí na správnom pochopení vzťahu medzi bezpečnostnými rizikami a systémami ochrany informácií.

Zoznam bibliografických odkazov

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
Brvnišťan, M. : Rozhodnutie o utajení ako základný predpoklad realizácie ochranných opatrení, In Zborník vedeckých a odborných prác, 8. Medzinárodná vedecká konferencia Národná a medzinárodná bezpečnosť 2015, Akadémia ozbrojených síl generála Milana Rastislava Štefánika 2017, ISBN 978-80-8040-515-1, str.33-41
Murdza, K. : Bezpečnosť a bezpečnostná orientácia v globálnej rizikovej spoločnosti, A PZ Bratislava 2005, 150 str., ISBN 80-8054-335-6
Národná stratégia manažmentu bezpečnostných rizík Slovenskej republiky, schválená uznesením vlády SR č.3 z 13.1.2016
Rozhodnutie Rady z 23. septembra 2013, č. 2013(488)EU o bezpečnostných predpisoch na ochranu utajovaných informácií, OJ L 274/1 z 15.10.2013, Prístupné na internete: www.nbusr.sk, 2017 R
Security within the North Atlantic Treaty Organization (NATO) Bezpečnosť v rámci NATO, C-M(2002)49, NATO Archives – public version, rístupné na internete: www.nato.int, 2017
Zákon č. 45/2011 Z.z. o kritickej infraštruktúre
Zákon č. 215/2014 Z.z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov
Nariadenie vlády č. 216/2004 Z.zz, ktorým sa ustanovujú oblasti utajovaných
Zákon č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov
Nariadenie Európskeho parlamentu a rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
Vyhláška č. 336/2004 Z. z. o fyzickej bezpečnosti a objektovej bezpečnosti
Vyhláška č. 339/2004 Z.z. o bezpečnosti technických prostriedkov
Krátky slovník slovenského jazyka, SAV, Bratislava 1997

http:// www.securityrevue.com, výkladový slovník 2018
https://dataprotection.gov.sk/uoou/sites/default/files/nariadenie_a_prava_obcanov.pdf

Miroslav Brvnišťan, JUDr. PhD.
Akadémia PZ
Sklabinská č. 1, 835 07 Bratislava, Slovenská republika
mob.: 00421903993119
brvnistan@bmsec.sk