

Národný bezpečnostný úrad v bezpečnostnom systéme Slovenskej republiky

Anotácia: Stav bezpečnostného systému Slovenskej republiky zodpovedá základným kritériám Organizácie Severoatlantickej zmluvy a Európskej únie. V oblasti vnútornej bezpečnosti, poriadku a ochrany je Slovenská republika schopná reagovať na výzvy, ohrozenia a riziká, ktorým môže byť vystavená. Súčasný legislatívny rámec vytvára základný predpoklad na zabezpečenie vnútornej bezpečnosti, poriadku a ochrany Slovenskej republiky, a tak je súčasná pozornosť zameraná aj na postupné skvalitňovanie legislatívnych, organizačných a materiálno-technických podmienok.

Kľúčové slová: bezpečnostný systém Slovenskej republiky, Národný bezpečnostný úrad, ochrana utajovaných skutočností, personálna bezpečnosť, priemyselná bezpečnosť, administratívna bezpečnosť a centrálny register, informačná bezpečnosť, fyzická bezpečnosť a objektová bezpečnosť, nežiaduce elektromagnetické vyžarovanie.

Úvod

Zásadné kvalitatívne zmeny spoločnosti v poslednom desaťročí 20. storočia a následná integrácia Slovenskej republiky (ďalej len „SR“) do rôznych medzinárodných a najmä nadnárodných štruktúr, vyvolali vzhľadom na vyvíjajúce medzinárodné a vnútropolitické situácie potrebu upraviť rôzne oblasti spoločenského života, vrátane zabezpečenia vnútornej a vonkajšej bezpečnosti štátu.

V oblasti vonkajšej bezpečnosti prispieva naša aktivita aj členstvom v OSN, v Organizácii pre bezpečnosť a spoluprácu v Európe, v Organizácii Severoatlantickej zmluvy a iných regionálnych organizáciách a zoskupeniach. Vstupom do Organizácie Severoatlantickej zmluvy sa SR stala súčasťou systému kolektívnej obrany a bezpečnosti ako piliera transatlantickej bezpečnosti a stability a jej bezpečnosť je aj garantovaná spojeneckými záväzkami, ku ktorým SR pristúpila. Vyvrcholením úsilia slovenskej zahraničnej politiky bol vstup SR do Európskej únie. Významnými a na verejnosti málo známymi prioritami prípravy na členstvo bolo skvalitnenie ochrany utajovaných skutočností, pričom bola predložená podmienka vytvorenia samostatného orgánu pre oblasť ochrany utajovaných skutočností – **Národného bezpečnostného úradu** (ďalej len „NBÚ“), čo zároveň ovplyvňuje aj vnútornú bezpečnosť SR.

1 Bezpečnostná politika a bezpečnostný systém Slovenskej republiky

V posledných dvoch desaťročiach zaznamenal svet dynamické zmeny vo všetkých oblastiach spoločenského života. Svedkami najrozsiahlejších zmien sme v oblasti geopolitickej, ekonomickej, bezpečnostnej, sociálnej a ekologickej, ktoré navzájom úzko súvisia a ovplyvňujú sa. Jednou z najdôležitejších oblastí je „bezpečnosť“ štátu.

Bezpečnosť ako pojem je v teoretickej rovine chápaný mnohostranne a jeho definovanie možno nájsť vo viacerých zdrojoch.¹ Vzhľadom na spojitosť pojmu „bezpečnosť“ s objektom „štát“ pre vymedzenie obsahu tohto článku možno použiť definovaný pojem „**bezpečnosť**“ ako stav, v ktorom je zachovaný mier, demokratický poriadok štátu a jeho zvrchovanosť, územná celistvosť, nedotknuteľnosť hraníc štátu, ekonomická stabilita, základné práva a slobody, a v ktorom sú chránené životy a zdravie osôb, majetok a životné prostredie.

¹ Pozri napr. MIKOLAJ, J., et al. *Terminológia bezpečnostného manažmentu*, výkladový slovník s. 24, BUZALKA, J. *Krízový manažment vo verejnej správe*, s. 123, Ústavný zákon č. 227/2002 Z. z. o bezpečnosti štátu v čase vojny, vojnového stavu, výnimočného stavu a núdzového stavu v znení neskorších predpisov.

Zodpovednosť za zaručenie bezpečnosti SR majú v rozsahu vymedzenej pôsobnosti zodpovedné orgány zákonodarné, výkonné, súdnej moci, prokuratúry, miestnej štátnej správy, územnej samosprávy a vecne príslušné právnické osoby a fyzické osoby.²

Východiskom pre definovanie efektívneho bezpečnostného systému v jeho podstate je bezpečnostná politika. Toto východiskové analyzovanie a spracovanie informácií predstavuje komplexný súbor činností, opatrení, postupov a pravidiel smerujúcich k dosiahnutiu potrebnej bezpečnosti objektu pred pôsobením bezpečnostných rizík a ohrození. Takto cieľavedomé spracovanie prístupných údajov a informácií o prostredí (spravidla po predchádzajúcej analýze bezpečnostných rizík, identifikácií a vyhodnotení bezpečnostných výziev a ich včasnom rozpoznaní tendencie vývoja) je základným a štartovacím bodom projektovania bezpečnostného systému.

Bezpečnostná politika SR ako komplexný súbor cieľov, zásad a opatrení štátu bola vytvorená na účel dosiahnutia cieľa – zaručenie bezpečnosti občana a štátu, ochrana záujmov štátu prezentovaných tak vnútri, ako aj navonok a formovanie obsahu na vytvorenie bezpečnostného potenciálu SR. Účinky realizácie bezpečnostnej politiky SR sú ovplyvňované podielom efektívnosti subjektov štátu (počnúc štátnymi orgánmi, orgánmi samosprávy, mimovládnych organizácií až po právnické osoby a nevynímajúc fyzické osoby – občanov štátu). Treba však zdôrazniť, že je nevyhnutné stotožnenie sa subjektov štátu s bezpečnostnými požiadavkami na naplnenie bezpečnostných cieľov.

Zatiaľ čo zásadné východiská realizácie bezpečnostnej politiky SR s cieľom zaručiť požadovanú úroveň bezpečnosti občana a štátu poskytuje Bezpečnostná stratégia SR, inštitucionálnym nástrojom bezpečnostnej politiky SR je **bezpečnostný systém SR**.

Bezpečnostný systém v teoretickom vymedzení možno chápať ako účelovo vytvorený systém, ktorého štruktúru tvoria subjekty podieľajúce sa na realizácii bezpečnostnej politiky, ich vzájomné vzťahy a činnosti (definované určitými pravidlami) s cieľom zaistiť bezpečnosť objektu.

Autori v Bezpečnostnej stratégii SR vymedzili, že bezpečnostný systém SR „predstavuje mnohorozmerný komplex, ktorý sa skladá zo zahraničnopolitických, ekonomických, vojenskoobránných, vnútrobezpečnostných, záchranných, zdravotníckych, humanitných, právnych, sociálnych, kultúrnych, historických a ekologických prvkov a ich vzájomných väzieb“. Definované orgány štátu (zákonodarné, výkonné a súdne v duchu trojdelenia štátnej moci – vyvážených brzd a protiváh) sú zodpovedné za činnosti (plánovanie, riadenie, kontrolovanie a koordinovanie úloh, opatrení a aktivít) zamerané na zaručenie bezpečnosti občana a štátu nielen v čase mieru, ale aj v krízových situáciách, pričom nezanedbateľný podiel má efektívne využitie zdrojov a prostriedkov štátu aj v spolupráci s medzinárodnou podporou.

Z iného pohľadu je možné bezpečnostný systém štátu chápať ako inštitucionálny nástroj na tvorbu a realizáciu jeho bezpečnostnej politiky, založený na komplexnom poňatí zaistenia bezpečnosti štátu a opiera sa o platné právne úpravy.³

Vzájomnú podmienenosť bezpečnostnej politiky a bezpečnostného systému v ich vnútorných a vonkajších dimenziách vyjadruje skutočnosť, že inštitucionálnym nástrojom na tvorbu a realizáciu bezpečnostnej politiky štátu sú prvky jeho bezpečnostného systému.

Jeden z pohľadov členenia bezpečnostného systému „štátu“ je jeho rozdelenie na:

- a) subsystém obrany (subsystém vonkajšej bezpečnosti), realizovaný s cieľom zaručiť zvrchovanosť, suverenitu, nezávislosť a územnú celistosť nášho štátu;
- b) subsystém vnútornej bezpečnosti a ochrany verejného poriadku, realizovaný s cieľom zaručiť vnútornú bezpečnosť štátu a ochranu verejného poriadku v súlade

² Koncepcia bezpečnostného systému Slovenskej republiky 2002, str. 1.

³ BUZALKA, J. *Všeobecné otázky krízového manažmentu*, s. 91.

s právnymi normami, princípmi demokracie a humanity. Tvorba jednotného bezpečnostného systému a obranného systému našej krajiny, výstavba bezpečnostného systému a obranného systému vyplýva z princípu nedeliteľnosti a jednoty vnútornej a vonkajšej bezpečnosti.⁴

Toto hľadisko vyplýva z rozdelenia bezpečnosti na bezpečnosť vonkajšiu a bezpečnosť vnútornú, ktoré sú do určitej miery od seba závislé.

Z pohľadu iného, štrukturálneho, bezpečnostný systém „štátu“ možno diferencovať podľa funkčných oblastí na:

- a) podsystem riadenia bezpečnostného systému,
- b) podsystem zahraničnej a bezpečnostnej politiky a spolupráce,
- c) podsystem obrany,
- d) podsystem ochrany vnútornej bezpečnosti a poriadku,
- e) podsystem spravodajstva,
- f) podsystem zabezpečenia.

Medzi jednotlivými podsystemami je vzájomná previazanosť a závislosť, pričom cieľ ostáva definovaný, a to bezpečnosť občana, štátu a ochrana jeho záujmov.

Záujmy štátu sú v oblasti bezpečnosti ohrozované rôznymi formami. V súčasnosti môže ísť o útoky teroristických, extrémistických, radikálnych skupín, aktivít organizovaného zločinu a činnosti cudzích spravodajských služieb na našom území, ktorá nie je v súlade so záujmami SR. Z pohľadu SR ako zvrchovaného, demokratického a právneho štátu je záujmom vytvoriť efektívny bezpečnostný systém, ktorý by eliminoval útoky na bezpečnosť a integritu SR. Na dianie na medzinárodnej scéne v oblasti bezpečnosti SR reagovala prijatím viacerých strategických a legislatívnych opatrení smerujúcich k vybudovaniu efektívneho bezpečnostného systému štátu, ktorý by dokázal čeliť bezpečnostným rizikám.⁵

2 Základné úlohy Národného bezpečnostného úradu a jeho postavenie v bezpečnostnom systéme Slovenskej republiky

Vzhľadom na orientáciu SR v zahraničnej politike – členstvo v Organizácii Severoatlantickej zmluvy, ako aj Európskej únii vznikla požiadavka na zriadenie NBÚ⁶ ako samostatného ústredného orgánu štátnej správy v oblasti ochrany utajovaných skutočností, šifrovej služby a neskôr elektronického podpisu.

Vymedzenie NBÚ v bezpečnostnom systéme SR špecifikuje jeho najzákladnejšia úloha – ochrana utajovaných skutočností,⁷ ktorá je dôležitým pilierom bezpečnosti SR a zároveň

⁴ BLAŽEK, V. *Album názorných pomôcok a vybraných materiálov k otázkam obrany a krízového manažmentu regiónu*. s. 12.

⁵ Napr. Bezpečnostná stratégia Slovenskej republiky, Obranná stratégia Slovenskej republiky, Národný akčný plán boja proti terorizmu, Národný program pre ochranu a obranu kritickej infraštruktúry v Slovenskej republike, Koncepcia kritickej infraštruktúry v Slovenskej republike, ústavný zákon o bezpečnosti štátu v čase vojny, vojnového stavu, výnimočného stavu a núdzového stavu v znení neskorších predpisov.

⁶ NBÚ bol zriadený v roku 2001 zákonom č. 241/2001 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. Predkladateľom tohto zákona bolo Ministerstvo vnútra SR, ktoré do doby zriadenia NBÚ bolo ústredným orgánom štátnej správy na ochranu utajovaných skutočností a šifrovú službu. V prípade, že by sa SR nestala členskou krajinou Organizácie Severoatlantickej zmluvy a Európskej únie, nevznikla by požiadavka na zriadenie NBÚ (z dôvodu členstva v Organizácii Severoatlantickej zmluvy a Európskej únie) a o gestorovi ochrany utajovaných skutočností by rozhodli predstavitelia štátnej moci (možno by to bolo naďalej Ministerstvo vnútra SR).

⁷ Vymedzenie utajovanej skutočnosti pozri zákon č. 215/2004 Z. z., § 2.

článkom systému transatlantickej a európskej bezpečnosti. Fakt, že transatlantická a európska bezpečnosť má vplyv aj na bezpečnosť národnú – slovenskú, nemožno opomenúť.

V spojitosti s ochranou utajovaných skutočností vo všeobecnosti sa spájajú aj úlohy čiastkové, ktoré sú v cykle ochrany utajovaných skutočností úlohami podpornými a potrebnými. Tieto jednotlivé úlohy NBÚ možno vymedziť na úseku ochrany utajovaných skutočností, ochrany zahraničných informácií, šifrovej ochrany informácií a elektronického podpisu v jednotlivých bodoch:

- a) predkladanie národného legislatívneho rámca pre oblasť ochrany utajovaných skutočností, čím sa stanovujú požiadavky na ochranu utajovaných skutočností vyplývajúcich z minimálnych požiadaviek Organizácie Severoatlantickej zmluvy a Európskej únie,
- b) vykonávanie previerkovej činnosti (bezpečnostnej previerky navrhovanej osoby, bezpečnostnej previerky podnikateľa), čím zároveň vymedzuje určitý okruh subjektov, ktoré sú oprávnené oboznamovať s utajovanými skutočnosťami (za splnenia ďalších legislatívnych požiadaviek),
- c) ochrana utajovaných skutočností je proces, ktorý je dynamický a v ktorom dochádza neustále k zmenám. Na tieto zmeny treba adekvátne reagovať, a to napr. formou školenia (bezpečnostných zamestnancov), metodického usmernenia (na úseku ochrany utajovaných skutočností), vydávaním bezpečnostných štandardov, skúšobných postupov,
- d) na ochranu utajovaných skutočností sa používajú mechanické zábranné prostriedky, technické zabezpečovacie prostriedky, technické prostriedky, ktoré za určitých podmienok musia spĺňať kritérium – byť certifikované. NBÚ má vytvorenú sieť autorizovaných osôb, ktoré vykonávajú skúšky týchto prostriedkov, na základe ktorých je vydaný záverečný protokol, ktorý je podkladom vydania certifikátu NBÚ na prostriedok,
- e) zriadený centrálny register na NBÚ a jeho spravovanie má v oblasti ochrany utajovaných skutočností tiež svoje opodstatnenie. Prostredníctvom neho dochádza k výmene utajovaných skutočností v súlade s medzinárodnými zmluvami,
- f) jeden zo spôsobov zabezpečenia ochrany utajovaných skutočností je ich šifrovanie. V tejto oblasti NBÚ plní funkciu ústredného šifrového orgánu SR, gestora zabezpečovania prostriedkov šifrovej ochrany informácií, stanovuje zásady šifrovej ochrany informácií a plní iné činnosti uložené zákonom na tomto úseku,
- g) oblasť elektronického podpisu je v poslednej dobe často skloňovaná, najmä s jej nedoceneným využívaním. NBÚ na tomto úseku vystupuje ako koreňová certifikačná autorita a plní ďalšie úlohy vyplývajúce z jej postavenia,⁸
- h) v neposlednom rade do procesu patrí aj kontrola dodržiavania podmienok ochrany utajovaných skutočností. Únik utajovaných skutočností by mohol zapríčiniť ohrozenie záujmov SR a tým spôsobiť určitú ujmu.

Tento výpočet úloh NBÚ je explicitný. Jeho ďalšie úlohy sú stanovené okruhom legislatívy upravujúcim oblasť ochrany utajovaných skutočností.

Postavenie NBÚ v rámci bezpečnostného systému SR vyplýva z plnenia jeho špecifickej činnosti a možno ho chápať z dvoch hľadísk. Na národnej úrovni má NBÚ postavenie orgánu štátnej správy s ústredným postavením pre oblasť ochrany utajovaných skutočností, pričom vystupuje ako tvorca a garant systému ochrany utajovaných skutočností v SR. Na medzinárodnej úrovni NBÚ vystupuje ako národná bezpečnostná autorita, ktorá je partnerom

⁸ Pre úlohy NBÚ na tomto úseku pozri zákon č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov v znení neskorších zmien a doplnkov.

národných bezpečnostných autorít a medzinárodných bezpečnostných štruktúr Organizácie Severoatlantickej zmluvy a Európskej únie, z čoho vyplýva aj povinnosť podieľať sa na určovaní spoločných bezpečnostných predpisov dôležitých pre garanciu dodržiavania zásad manipulácie s utajovanými skutočnosťami postúpených SR cudzou mocou.

Systém ochrany utajovaných skutočností

Vzhľadom na postavenie NBÚ je slovenský model riadenia ochrany utajovaných skutočností považovaný za značne **centralizovaný**. NBÚ je tvorcom a garantom systému ochrany utajovaných skutočností v SR, čo sa prejavuje najmä prípravou a kontrolou národnej legislatívy pre ochranu utajovaných skutočností a tvorbou strategických koncepčných dokumentov v tejto oblasti.

Systém ochrany utajovaných skutočností SR tvoria podsystemy oblastí ochrany utajovaných skutočností, ktoré sú vytvorené v súlade s bezpečnostnými záujmami SR. Podsystemy treba chápať ako jednotlivé prvky, ktoré v systéme nepôsobia samostatne, ale sa navzájom prelínajú, dopĺňajú a medzi ktorými sú vzájomné väzby. Bezpečnostné záujmy SR, ktoré reprezentujú jednotlivé rezorty v rámci ich kompetencií, stanovujú bezpečnostné riziká v systéme bezpečnosti SR a bezpečnostné opatrenia na ich odstránenie.

Podsystemy ochrany utajovaných skutočností

V systéme ochrany utajovaných skutočností možno vnímať jednotlivé oblasti ochrany utajovaných skutočností ako podsystemy, ktorých cieľom je dosiahnutie ochrany utajovaných skutočností prostredníctvom opatrení v oblasti:

- a) personálnej bezpečnosti,
- b) priemyselnej bezpečnosti,
- c) administratívnej bezpečnosti a centrálneho registra,
- d) informačnej bezpečnosti,
- e) fyzickej bezpečnosti a objektovej bezpečnosti.

V jednotlivých podsystemoch je potrebné zosúladiť ich funkcie, vnútorné prvky a vzájomné vzťahy medzi nimi. Na účel dosiahnutia vhodného systému ochrany utajovaných skutočností nepostačuje skúmať jednotlivé oblasti ochrany utajovaných skutočností samostatne, ale v ich komplexnosti a kontinuite s ostatnými oblasťami ochrany utajovaných skutočností, a to tak v národnom, ako aj v medzinárodnom prostredí.

V oblasti ochrany utajovaných skutočností podmienka vykonávania bezpečnostnej previerky osoby spadá do oblasti **personálnej bezpečnosti**, ktorá je tvorená súhrnom opatrení súvisiacich s výberom, určením a kontrolou osôb, ktoré sa môžu v určenom rozsahu oboznamovať s utajovanými skutočnosťami, tvorí oblasť personálnej bezpečnosti.

Účelom personálnej bezpečnosti je identifikácia osôb ako potenciálne rizikových osôb v oblasti ochrany utajovaných skutočností, pričom takou osobou môže byť pôvodca, príjemca alebo prepravca utajovanej skutočnosti.

Oprávnenie na oboznamovanie sa s utajovanými skutočnosťami môže vzniknúť osobe za taxatívne splnených podmienok uvedených v § 10 ods. 1 zákona č. 215/2004 Z. z., pokiaľ nie je stanovené inak. Predpoklady na vznik oprávnenia musí táto osoba spĺňať počas platnosti osvedčenia alebo určenia. Na oboznamovanie sa s utajovanými skutočnosťami stupňa utajenia vyhradené úrad osvedčenie nevydáva, avšak ostatné predpoklady na oboznamovanie sa s utajovanými skutočnosťami musia byť splnené.

Priemyselnú bezpečnosť upravuje súhrn opatrení právnickej osoby alebo fyzickej osoby, ktorá je podnikateľom, na ochranu utajovaných skutočností, ktoré jej boli odovzdané alebo ktoré u nej vznikli.

Podnikateľ je podľa zákona povinný požiadať úrad o vydanie potvrdenia o priemyselnej bezpečnosti, ak je odôvodnený predpoklad, že bude požiadaný štátnym orgánom o vytvorenie utajovanej skutočnosti, alebo ak bude potrebné podnikateľovi utajovanú skutočnosť postúpiť.

Bezpečnostnou previerkou podnikateľa úrad zisťuje, či spĺňa zákonné podmienky priemyselnej bezpečnosti. Bezpečnostná previerka podnikateľa, ktorú vykonáva úrad pre všetky stupne utajenia na základe žiadosti jeho štatutárneho orgánu, ako aj vydanie potvrdenia o priemyselnej bezpečnosti podnikateľa a jeho platnosť, je viazaná na splňanie podmienok priemyselnej bezpečnosti, t. j. spôsobilosť zabezpečiť ochranu utajovaných skutočností, ekonomickú stabilitu, bezpečnostnú spoľahlivosť.

Prepojenie personálnej bezpečnosti a priemyselnej bezpečnosti je významné, pretože pokiaľ štatutárny orgán – v tomto prípade fyzická osoba – nemá platnú previerku personálnej bezpečnosti, nie je možné, aby podnikateľ získal potvrdenie o priemyselnej bezpečnosti.

Administratívna bezpečnosť je súhrn opatrení, ktorých cieľom je ochrana utajovaných skutočností pri ich tvorbe, prijíme, evidencii, preprave, ukladaní, rozmnožovaní, vyradovaní a uchovávaní alebo pri inej manipulácii.⁹

Administratívna bezpečnosť sa podieľa na ochrane utajovaných skutočností, ktoré sú listinného charakteru, resp. v tzv. elektronickej podobe, a dosahuje sa súborom opatrení, realizáciou postupov a zásad oprávnenými osobami v časovom období „existencie“ utajovanej písomnosti. Cieľom opatrení administratívnej bezpečnosti je minimalizovanie bezpečnostných rizík utajovaných skutočností a ich ohrozenia pred nepovolanými osobami a cudzou mocou. „Existencia“ utajovanej písomnosti je ohraničená vznikom utajovanej písomnosti (vytvořením) a fyzickým zničením alebo zrušením stupňa utajenia utajovanej písomnosti.

V súlade s uzatvorenými medzinárodnými dohodami sú utajované skutočnosti poskytované, vymieňané a prijímané prostredníctvom **centrálneho registra**. Pre výkon tejto úlohy vo vzťahu k NATO bolo vytvorené pracovisko centrálneho registra¹⁰ na Stálej delegácii SR pri NATO a na Stálom zastúpení SR pri EÚ, prostredníctvom ktorého je zabezpečené poskytovanie a prijímanie utajovaných skutočností NATO a EÚ v „elektronickej podobe“.

Pod oblasť **informačnej bezpečnosti** zákon zaraďuje:

- a) **bezpečnosť technických prostriedkov** – systém opatrení na zabezpečenie ochrany utajovaných skutočností, ktoré sa tvoria, spracúvajú, prenášajú alebo ukladajú na technických prostriedkoch,¹¹
- b) **šifrovú ochranu informácií** – systém na zabezpečenie ochrany utajovaných skutočností kryptografickými metódami a prostriedkami šifrovej ochrany informácií,¹²
- c) **elektronický podpis** – informácia pripojená alebo inak logicky spojená s elektronickým dokumentom, ktorá musí spĺňať tieto požiadavky:
 - a) nemožno ju efektívne vyhotoviť bez znalosti súkromného kľúča a elektronického dokumentu,

⁹ Zákon č. 215/2004 Z. z., § 6 ods. 5

¹⁰ Centrálny register pôsobí ako príjemca a odosielateľ utajovaných skutočností v rámci medzinárodnej spolupráce (výnimku tvoria tzv. spravodajské utajované skutočnosti poskytnuté v rámci spravodajskej činnosti).

¹¹ Zákon č. 215/2004 Z. z., § 6 ods. 7.

¹² Zákon č. 215/2004 Z. z., § 6 ods. 9.

- b) na základe znalosti tejto informácie a verejného kľúča patriaceho k súkromnému kľúču použitému pri jej vyhotovení možno overiť, že elektronický dokument, ku ktorému je pripojená alebo s ním inak logicky spojená, je zhodný s elektronickým dokumentom použitým na jej vyhotovenie.¹³

Ochrana utajovaných skutočností v informačnej bezpečnosti v pôsobnosti úradu sa vykonáva používaním bezpečnostných opatrení v oblasti počítačov, komunikačných prostriedkov, v kryptografii a tam, kde sa údaje, v našom prípade utajované skutočnosti, spracovávajú, uchovávajú, prenášajú, zobrazujú v inej ako papierovej (fyzickej) forme.¹⁴

Významnú úlohu v budovaní informačnej bezpečnosti zohráva prostredie, v ktorom sú informačné aktíva umiestené, a preto je dôležité

- a) definovanie informačných aktív, ich vlastníctva a zodpovedností pri ich využívaní,
- b) definovanie hodnoty informačných aktív prostredníctvom bezpečnostnej analýzy rizík, ktorá identifikuje potenciálne hrozby a zraniteľnosti a stanovuje úrovne rizík,
- c) stanovenie bezpečnostnej politiky, ktorej súčasťou je aj proces budovania bezpečnostného povedomia a trvalého vzdelávania (cieľom je eliminovanie hrozby súvisiacej s ľudským faktorom),
- d) stanovenie vhodnej bezpečnostnej architektúry a jej implementácia, ktorá má výrazný vplyv na úroveň informačnej bezpečnosti a efektívnosť vynaložených prostriedkov,
- e) riadenie bezpečnosti (integrálna súčasť bezpečnostnej architektúry),
- f) vykonávanie monitoringu prevádzky, auditu systému a kontroly jednotlivých prvkov informačných systémov (potrebné činnosti na dosiahnutie a udržanie požadovanej úrovne informačnej bezpečnosti),
- g) adekvátne reagovať na bezpečnostné incidenty a následne vykonávať nápravu následkov v reálnom čase a prostredí.

Fyzická bezpečnosť a objektová bezpečnosť ako súhrn opatrení slúžiacich na ochranu utajovaných skutočností vo fyzickej podobe a prvkom informačných systémov, v ktorých sa utajované skutočnosti spracovávajú, uchovávajú, prenášajú, zobrazujú pred nepovolnými osobami a pred neoprávnenou manipuláciou v objektoch a chránených priestoroch sa zabezpečuje fyzickými opatreniami.

Atribútmi fyzickej bezpečnosti a objektovej bezpečnosti sú mechanické zábranné prostriedky, technické zabezpečovacie prostriedky, aplikovanie fyzickej ochrany a režimových opatrení. Ochrana utajovaných skutočností sa realizuje formou prijatých opatrení vo vrstvách. Vnútrošnú vrstvu tvoria opatrenia na ukladanie utajovaných skutočností, ďalšiu vrstvu tvoria opatrenia na ochranu chráneného priestoru, nasledujúcu vrstvu tvoria opatrenia na ochranu objektu a poslednú vrstvu tvoria opatrenia na ochranu perimetra. Optimálna ochrana utajovaných skutočností z pohľadu fyzickej bezpečnosti a objektovej bezpečnosti sa dosahuje kombináciou uvedených atribútov. V záujme optimálnej ochrany utajovaných skutočností z pohľadu fyzickej bezpečnosti a objektovej bezpečnosti bol vytvorený bezpečnostný štandard fyzickej bezpečnosti a objektovej bezpečnosti, ktorý stanovuje minimálne požiadavky na zabezpečenie objektov a priestor na ochranu utajovaných skutočností prostredníctvom bodového ohodnotenia.

¹³ Zákon č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, § 3 ods. 1.

¹⁴ Ochrana utajovaných skutočností vo fyzickej podobe zabezpečuje oblasť fyzickej bezpečnosti a objektovej bezpečnosti, resp. oblasť administratívnej bezpečnosti.

Ochrana pred nežiaducim elektromagnetickým vyžarovaním

Fyzikálny jav „elektromagnetické vyžarovanie“ je nerozlučne spojený s činnosťou všetkých elektrických a elektronických prístrojov a zariadení. V plnej miere sa to vzťahuje aj na výpočtovú a komunikačnú techniku. Elektromagnetické vyžarovanie môže prenášať aktuálnu informáciu spracovávanú zariadením (napr. obrazový signál počítača). Ak je elektromagnetickým vyžarovaním prenášaná utajovaná skutočnosť (informácia), hovoríme o nežiaducom elektromagnetickom vyžarovaní.

Nežiaduce elektromagnetické vyžarovanie (skratka „NEV“) možno charakterizovať ako elektromagnetické vyžarovanie elektrických a elektronických zariadení, ktoré môže spôsobiť únik utajovanej informácie. Medzinárodne používané označenie pre výskum a štúdium nežiaduceho elektromagnetického vyžarovania (angl. compromising emanations) je TEMPEST.

Ochrana pred nežiaducim elektromagnetickým vyžarovaním je tvorená systémom opatrení na zabezpečenie ochrany utajovaných skutočností pred ich únikom prostredníctvom nežiaduceho elektromagnetického vyžarovania.

„Útok“ prostredníctvom nežiaduceho elektromagnetického vyžarovania je pasívny, preto nemôže byť detekovateľný. Zariadenie generuje nežiaduce elektromagnetické vyžarovanie, ktoré môže byť zachytené a zrekonštruované zo vzdialenej pozície. Inak povedané, „odpočúvanie“ z nežiaduceho elektromagnetického vyžarovania sa prakticky nedá zistiť. Všetko, čo robíme na svojom počítači, môže byť zachytené a „odpočúvané“ technikou na monitorovanie nežiaduceho elektromagnetického vyžarovania.

Na zabezpečenie adekvátnych protiopatrení na elimináciu hrozby úniku utajovaných skutočností prostredníctvom nežiaduceho elektromagnetického vyžarovania je potrebné znížiť úroveň „užitočného“ signálu v mieste, kde sa môže potenciálny „útočník“ dostať so svojou technikou na takú úroveň, aby nebol schopný z tohto signálu zrekonštruovať „užitočnú“ informáciu. Kontrolovateľným priestorom na účely ochrany pred nežiaducim elektromagnetickým vyžarovaním sa rozumie trojrozmerný priestor obklopujúci zariadenie, v ktorom je zabezpečené, že v ňom nebude nepovolaná osoba vykonávať činnosť s cieľom získať utajované informácie prostredníctvom nežiaduceho elektromagnetického vyžarovania.

Z uvedeného vyplýva, že nežiaduce elektromagnetické vyžarovanie je z hľadiska informačnej bezpečnosti veľmi nebezpečnou hrozbou, s ktorou pri analýze rizík v oblasti ochrany utajovaných skutočností treba počítať.

Základné princípy a zásady ochrany utajovaných skutočností, ktoré vytyčuje Koncepcia ochrany utajovaných skutočností SR, je potrebné podľa vývoja bezpečnostnej situácie neustále analyzovať a prijímať adekvátne bezpečnostné opatrenia s cieľom zabezpečenia bezpečnosti občana a štátu vsúlade so zákonmi a našimi medzinárodnými záväzkami v oblasti bezpečnostnej politiky. Cieľový systém ochrany utajovaných skutočností má preto byť flexibilný, homogénny, adaptívny a apolitický.

Záver

Bezpečnostné prostredie v regióne strednej Európy je stabilizované. V európskom a globálnom prostredí však stále existujú bezpečnostné hrozby ako napríklad: medzinárodný terorizmus, informačný terorizmus, organizovaná kriminalita, hromadná migrácia, nelegálne obchodovanie s ľuďmi a drogami.

Integráciou SR do medzinárodných ekonomických a bezpečnostných štruktúr sa na jednej strane zvýšila možnosť SR ovplyvňovať bezpečnostné prostredie v našom okolí a na druhej strane nám vyplynula zodpovednosť prispievať k zaisteniu bezpečnosti okolo nás bez ohľadu priameho alebo nepriameho efektu na bezpečnosť SR.

V bezpečnostnom systéme SR plní ochrana utajovaných skutočností podstatnú úlohu. Na únik informácií spoločnosť reaguje citlivo, pretože si je vedomá možných negatívnych následkov. Únik utajovaných skutočností, ktorý môže byť spôsobený laxným prístupom k ich zabezpečeniu a ktorým dôjde k ohrozeniu chráneného záujmu, má vplyv aj na súkromný sektor.

Na dosiahnutie dôvernosti, integrity, autenticity a dostupnosti utajovaných skutočností (ochranu utajovaných skutočností) musia byť vyvážené implementované opatrenia z oblasti bezpečnosti personálnej, priemyselnej, informačnej, fyzickej a objektovej a administratívnej tak, že žiadna oblasť ochrany utajovaných skutočností nemôže v danom systéme ochrany utajovaných skutočností vystupovať samostatne, nadradene nad ostatné oblasti. Iba takýmto uceleným a koordinovaným spôsobom možno zabezpečiť fungujúci systém ochrany utajovaných skutočností. Iba vyváženosť v aplikácii jednotlivých oblastí ochrany utajovaných skutočností môže zaručiť vysokú efektívnosť ochrany utajovaných skutočností.

Literatúra

BLAŽEK, V. *Album názorných pomôcok a vybraných materiálov k otázkam obrany a krízového manažmentu regiónu /metodická pomôcka/*. Bratislava : Akadémia PZ, 2009, 131 s. ISBN 978-80-8054-462-1.

BUZALKA, J. *Krízový manažment vo verejnej správe*. 1. vyd. Bratislava : Akadémia PZ, 2008, 296 s. ISBN 978-80-8054-451-5.

MIKOLAJ, J., HOFREITER, L., MACH, V., MIHÓK, J., SELINGER, P. *Terminológia bezpečnostného manažmentu, výkladový slovník*, Multiprint s.r.o., 2004. 191 s. ISBN 80-96914-1-2.

Ústavný zákon č. 227/2002 Z. z. o bezpečnosti štátu v čase vojny, vojnového stavu, výnimočného stavu a núdzového stavu v znení neskorších predpisov.

Zákon č. 241/2001 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

Zákon č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy v znení neskorších predpisov.

Zákon č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

Zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

Koncepcia bezpečnostného systému Slovenskej republiky prijatá vládou SR 9. 10. 2002.

Bezpečnostná stratégia Slovenskej republiky schválená Národnou radou 27. septembra 2005.

Koncepcia ochrany utajovaných skutočností v Slovenskej republike schválená vládou SR 30. 05. 2007.

www.nbusr.sk

Key words: security system of the Slovak Republic, National Security Authority, protection of classified information, personnel security, industrial security, administrative security and central registry, information security, physical and building security, unwanted electromagnetic emission /TEMPEST/.

Summary

The National Security Authority (NSA) is a National Authority for protection of classified information in security system of the Slovak Republic. NSA creates a legal frame, designates basic principles and conditions in this field. Within NATO and EU participates in

creation of security rules of protection of classified information and hereby assists to form of multinational security system that is transformed and implemented into national one.

*npor. Mgr. Peter Grebáč
Sekcia informačnej bezpečnosti
a elektronického podpisu
Národný bezpečnostný úrad
e-mail: peter.grebac@nbusr.sk*

Recenzent: prof. PhDr. Ján Buzalka, CSc.