Národná stratégia
pre informačnú bezpečnosť v Slovenskej republike

Obsah

1. Úvod

Cieľom dokumentu „Národná stratégia pre informačnú bezpečnosť v SR“ (ďalej len „NSIB“) je vytvoriť základný rámec informačnej bezpečnosti Slovenskej republiky (ďalej len „SR“). Vzhľadom na to, že zaistenie informačnej bezpečnosti (materiál sa zaoberá neutajovanými skutočnosťami) si vyžaduje komplexný prístup, treba definovať jej základnú úroveň s možnosťou rozšírenia v špecifických oblastiach. Správne vymedzenie pojmu informačnej bezpečnosti je dôležité z hľadiska vytvárania primárnych legislatívnych pravidiel v uvedenej oblasti, ako aj ďalším krokom k riešeniu problematiky informačnej bezpečnosti na Slovensku.

Obsahom stratégie sú východiská, kompetenčné rozloženie právomocí, návrh smerovania, priorít a krokov k dosiahnutiu stanoveného cieľa. Súčasťou dokumentu je aj základný popis jednotlivých úloh s cieľom zabezpečiť ochranu celého digitálneho priestoru SR, mimo oblasti utajovaných skutočností, ktoré rieši NBÚ. Patria sem najmä opatrenia proti úniku informácií a ich neoprávnenému použitiu, narušeniu integrity údajov, porušeniu práv občanov na ochranu osobných údajov, ochrana pred poškodzovaním a zneužívaním informačných a komunikačných systémov, poškodzovaním dobrého mena štátnych aj súkromných inštitúcií ako aj opatrenia na presadzovanie príslušných právnych noriem SR a Európskej únie. Nedostatočná úroveň ochrany informácií a informačných a komunikačných technológií vedie k spochybňovaniu spoľahlivosti a dôveryhodnosti informácií, ktoré sú prístupné z prostredia internetu, ktorý v súčasnosti predstavuje sieť vzájomne prepojených počítačových systémov vo viac ako 250 krajinách sveta. Táto najväčšia sieť na svete dnes ponúka prístup k takmer neobmedzenému zdroju informácií a umožňuje ich výmenu a poskytuje veľké množstvo služieb, ako sú elektronická pošta, prenos súborov a pod. Z uvedených dôvodov spoľahlivé fungovanie informačných systémov, spoľahlivá výmena informácií a s tým spätá informačná bezpečnosť predstavuje určitú mieru záruky zabezpečenia základných práv a slobôd občanov a rozvoja konkurencieschopnosti každého štátu. Prijatím opatrení, ktoré stratégia navrhuje sa zároveň zvýši dôveryhodnosť elektronických služieb, elektronického obchodu, konkurencieschopnosť a vážnosť nášho štátu voči zahraničiu.

2. Význam dokumentu

2.1 Význam informačnej bezpečnosti

Informačné a komunikačné technológie (ďalej len „IKT“) výrazne ovplyvňujú vývoj ľudskej spoločnosti. Vzájomne poprepájané informačné a komunikačné systémy tvoria informačnú a komunikačnú infraštruktúru (ďalej len „IKI“), ktorej prostredníctvom sa v súčasnosti vykonávajú operácie prakticky vo všetkých oblastiach života spoločnosti (doprava, finančníctvo a bankovníctvo, energetika, telekomunikácie, zdravotníctvo a sociálne zabezpečenie, obrana, bezpečnosť, vzdelávanie, kultúra, vlastný výkon verejnej správy a pod.). Dosah IKT presahuje rámec samotnej IKI. Nutným predpokladom fungovania spoločnosti je zaistenie informačnej bezpečnosti v štáte. V širšom zmysle to znamená zaistenie informačnej bezpečnosti a ochrany celého informačného priestoru a z praktického hľadiska najmä ochranu IKI štátu a jej informačného obsahu, ktoré sú v stratégii označované pojmom digitálny priestor[1]. Špecifický charakter má kybernetický priestor, ktorého ochranu

[1] pojem digitálny priestor zodpovedá pojmu „cyberspace“ rozšírený štandardy, normy, legislatívu, pre ktorý sa však nehodí doslovný slovenský preklad (kybernetický priestor), pretože tento má užší význam

zabezpečuje NBÚ a ktorý zahŕňa oblasť utajovaných informácií a ďalších skutočností, ktoré určí záväzný právny predpis (smernica EÚ/EK, nariadenie EÚ, zákon a pod., resp. uznesenie vlády).

Informačná bezpečnosť má multilaterálny charakter, t. j. musí zohľadňovať záujmy vlastníkov IKT systémov, potreby ich používateľov, ako aj práva fyzických a právnických osôb, ktorých údaje sa v systémoch spracovávajú. Z hľadiska používateľov sú pri spracovaní informácie najdôležitejšie tieto faktory: účel a obsah informácií, presnosť, aktuálnosť, prístupnosť, autenticita, usporiadanie a kvalita informácií. Z hľadiska vlastníkov a prevádzkovateľov je najdôležitejší spoľahlivý prístup k informačným zdrojom s prístupom on-line a ich zabezpečenie pred únikom informácií, neoprávneným použitím a narušením integrity údajov, ako aj autorita a dobré meno vlastníka systému.

Existuje množstvo činiteľov, ktoré môžu spôsobiť znefunkčnenie IKT systémov a znehodnotenie údajov, ktoré sa v nich spracovávajú. Sú to napr.: prírodné vplyvy, technické poruchy, ľudské chyby a omyly, škodlivý softvér, cieľavedomé útoky, počítačová kriminalita a medzinárodný terorizmus.

Základom IKI je internet, ktorý umožňuje vzájomnú komunikáciu medzi informačnými zdrojmi a žiadateľmi o informácie, či už vo verejnej správe, komerčnej sfére, alebo medzi jednotlivcami. Internet nemá vlastníka, neexistujú žiadne pravidlá a obmedzenia, ktoré by upravovali používanie informácií osobného charakteru a znemožňovali ich prípadné zneužitie tretími subjektmi. Vážne bezpečnostné problémy sú spojené aj s ďalšími službami internetu, ktorými sú elektronická pošta, prenos súborov a pod.

Nezabezpečenie informácií tak môže mať za následok nenahraditeľné straty a narušenie dôveryhodnosti organizácie a štátu. Vzhľadom na to, že štát je garantom kritických procesov, má úlohu starať sa o celkovú úroveň konkurencie schopnosti spoločnosti, a tak chrániť národné bohatstvo, ktorého súčasťou sú aj znalosti a informácie, a preto si nemôže dovoliť mať nízke kritériá úrovne bezpečnosti. Dosahy môžu byť najmä v niektorých oblastiach zničujúce. Povinnosťou štátu je preto zabezpečiť ochranu informácií pred zneužitím a minimalizovať následky v prípade ich zneužitia.

2.2 Informačná bezpečnosť z pohľadu EÚ a nadnárodných organizácií

Pohľad na riešenie bezpečnosti vychádza z nutnosti riešenia problému, ktorý pôvodne vznikol v dôsledku vedecko-technického rozvoja a ktorý sa v súčasnosti v plnej miere prejavuje ako celosvetový spoločenský problém. Spoločnosť sa snaží tento problém riešiť a zabezpečiť tak ochranu svojich cenných aktív ako aj ochranu súkromia občana. Potrebu informačnej bezpečnosti si začínajú uvedomovať aj národné vlády, nadnárodné orgány a organizácie vyspelých krajín sveta (OSN, G8, OECD, ISO). Vytvárajú rôzne inštitúcie a inštitucionálne systémy pre zabezpečovanie ochrany informácií (ENISA, HLIG, CERT a pod.), určujú si strategické ciele, rozpracovávajú ich a prijímajú opatrenia na ich splnenie.

V tejto súvislosti bola v marci 2004 vytvorená Európska agentúra pre informačnú bezpečnosť - ENISA, ktorá združuje všetky členské štáty EÚ a v ktorej SR zastupuje Ministerstvo financií SR.

Na Lisabonskom summite sa v roku 2000 predstavitelia štátov a vlád dohodli na cieli urobiť z EÚ *„do roku 2010 najkonkurencieschopnejšiu a najdynamickejšiu poznatkovo orientovanú ekonomiku sveta, schopnú trvalo udržateľného rastu“* a prijali tzv. Lisabonskú stratégiu e-Europe, ktorá bola v roku 2005 nahradená iniciatívou *„i-Initiative 2010“*

(Európska informačná spoločnosť 2010). Medzi svoje hlavné priority EÚ zaradila aj informačnú bezpečnosť. Vydala množstvo strategických dokumentov, odporúčaní, smerníc a nariadení týkajúcich sa ochrany osobných údajov a počítačových programov, elektronického podpisu, elektronického obchodu, boja s počítačovou kriminalitou, boja so spamom a pod.

2.3 Legislatíva a vzťah k iným dokumentom

NSIB vychádza z poznania reálneho stavu a skúseností vo svete, v SR, z direktív stanovených EÚ, z odporúčaní OECD; z kľúčových medzinárodných noriem a štandardov pre informačnú bezpečnosť (ďalej len „IB"), z právneho rámca ochrany informácií SR a z ďalších dokumentov prijatých vládou SR a Národnou radou SR. V SR sa jedná najmä o nasledovné súvisiace predpisy:

- zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení zákona č. 678/ 2006 Z. z.,
- zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- zákon č. 428/2002 Z. z. o ochrane osobných údajov 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. 618/2003 Z. z. o autorskom práve a právach súvisiacich s autorským právom v znení neskorších predpisov,
- zákon č. 483/2001 Z. z. o bankách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- zákon č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov,
- ďalšie zákony a vykonávacie predpisy uvedené v *Prílohe č. 1*.

Slovenská republika sa oficiálne prihlásila k iniciatíve eEurope+ uznesením vlády SR č. 522 z 13. júna 2001, ktorým bol schválený základný dokument v oblasti informatizácie spoločnosti: *„Politika informatizácie spoločnosti v SR"*. Na základe uvedeného uznesenia vlády SR bol predložený aj *„Návrh Stratégie informatizácie spoločnosti v podmienkach SR a Akčného plánu*", ktorý bol schválený vládou SR uznesením vlády SR č. 43 zo dňa 21. januára 2004.

V súvislosti s riešením problematiky IB bol ratifikovaný Dohovor o kybernetickom zločine CETS č. 185/2001 vydaný Radou Európy, ktorý je zapracovaný do trestného zákona SR, smernica Európskeho parlamentu a Rady 1999/93/ES o rámci spoločenstva pre elektronické podpisy transponovaná do zákona o elektronickom podpise, smernica Európskeho parlamentu a Rady 95/46/EC o ochrane jednotlivcov pri spracovaní osobných údajov a voľnom pohybe týchto údajov transponovaná do zákona o ochrane osobných údajov. V súčasnosti platí aj množstvo ďalších rozhodnutí a smerníc vydaných Radou Európy v oblasti informačnej bezpečnosti.

Najvýznamnejšie strategické dokumenty v SR sú:

- „Bezpečnostná stratégia SR" (NR SR, september 2005).
- „Návrh Koncepcie kritickej infraštruktúry v SR a spôsobu jej ochrany a obrany" (MH SR, 2007).

- Koncepcia ochrany utajovaných skutočností v SR.

Predkladaný dokument je v súlade s kľúčovými relevantnými medzinárodnými bezpečnostnými štandardmi a normami a štandardmi vydanými MF SR, NBÚ, MZ SR, ÚOOÚ SR a ÚNMS SR.

2.4 Oblasti informačnej bezpečnosti a kompetencie

Ucelená koncepcia informačnej bezpečnosti SR zatiaľ nebola prijatá. Napriek tomu existujú čiastkové oblasti, v ktorých je informačná bezpečnosť rozpracovaná (legislatívne, kompetenčne, organizačne aj metodicky). Sú to najmä:

Informatizácia spoločnosti (MF SR) a informačná bezpečnosť verejnej správy spadajúca do kompetencie MF SR, ktoré činnosť v oblasti informačnej bezpečnosti zabezpečuje prostredníctvom Komisie pre informačnú bezpečnosť. V pôsobnosti tejto komisie je „*odborná príprava návrhov a stanovísk pre oblasť informačnej bezpečnosti*“, v rámci čoho komisia o. i. „*navrhuje zavedenie bezpečnostných štandardov, zmenu alebo zrušenie existujúcich platných bezpečnostných štandardov pre informačné systémy verejnej správy*.“ (stránka: http://www.informatizacia.sk).

Ochrana utajovaných skutočností (NBÚ) z hľadiska informačnej bezpečnosti predstavuje klasifikovanú informáciu a systémy pracujúce s klasifikovanou informáciou. Napriek tradičnej terminológie použitej v legislatíve[2], utajované skutočnosti nie sú klasifikované len z hľadiska *dôvernosti* (confidentiality), ale bezpečnostné požiadavky na ich ochranu sú komplexné a zohľadňujú aj potrebu zaistenia *integrity, autentickosti a dostupnosti*. Vo vzťahu k utajovaným skutočnostiam, ktoré sú obsahom kybernetického priestoru a tej časti digitálneho priestoru SR, v ktorom sa nepracuje s klasifikovanou informáciou, sa uplatňuje dvojaký systém riadenia. V záujme ochrany digitálneho priestoru SR bude preto potrebné rozvinúť bližšiu spoluprácu v oblasti ochrany klasifikovanej informácie (utajovaných skutočností) a informačnej bezpečnosti celého digitálneho priestoru SR.

Ochrana osobných údajov (ÚOOÚ SR) a používanie **elektronického podpisu** (NBÚ), tieto oblasti sú upravené zákonmi[3] a príslušné inštitúcie zabezpečujú dohľad nad dodržiavaním zákona.

Elektronický obchod (MH SR) upravuje Zákon č. 22/2004 Z. z. o elektronickom obchode a o zmene a doplnení zákona č. 128/2002 Z. z. o štátnej kontrole vnútorného trhu vo veciach ochrany spotrebiteľa a o zmene a doplnení niektorých zákonov v znení zákona č. 284/2002 Z. z. v znení zákona č. 160/2005 Z. z. (ďalej len „zákon č. 22/2004 Z. z. o elektronickom obchode“), do ktorého bola transponovaná smernica Európskeho parlamentu a rady č. 2000/31/ES o elektronickom obchode, ktorá tvorí spoločný právny rámec elektronického obchodovania pre všetky členské štáty. Ustanovenia a smernice o elektronickom obchode sú značne všeobecné, a preto si vyžadujú prijatie dodatočných právnych noriem. S týmto cieľom Komisia pre Európu - Centrum OSN pre uľahčovanie obchodu a elektronické obchodovania (UN/CEFACT) oficiálne vydala v júli 2005 v Ženeve metodický materiál „*Odporúčanie č. 33*“, s cieľom zavedenia jednoduchého, transparentného a efektívneho procesu pre globálne

[2] Zákon 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení zákona č. 638/2005 Z. z. a zákona č. 255/2006 Z. z. s ním súvisiace predpisy

[3] Zákon č. 428/2002 Z. z. o ochrane osobných údajov v znení neskorších predpisov, Zákon č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov

obchodovanie. Procesy a služby predpisuje smernica Európskeho parlamentu a Rady 2006/123/ES o službách na vnútornom trhu, pričom všetky členské štáty sú povinné uviesť do účinnosti zákony, iné právne predpisy a správne opatrenia potrebné na dosiahnutie súladu s touto smernicou. Uvedené opatrenie si tak vyžiada aproximáciu smernice do nášho právneho poriadku do konca roku 2009.

Počítačová kriminalita (MS SR, MV SR), existujúca legislatíva pokrýva aj túto oblasť. Slovenská republika ratifikovala Dohovor o kybernetickom zločine CETS č. 185/2001 vydaný Radou Európy a jeho princípy boli premietnuté do Trestného zákonníka[4].

Autorské právo (MK SR) a práva súvisiace s autorským právom sú ošetrené autorským zákonom[5].

Normy a štandardy[6]. Medzinárodné štandardizačné organizácie (ISO, IEC, CEN) vydávajú aj normy stanovujúce požiadavky na zaistenie bezpečnosti informačných a komunikačných systémov. Na Slovensku sú kompetencie na vydávanie bezpečnostných noriem rozdelené. Všeobecne platné normy vydáva ÚNMS SR (SÚTN), štandardy pre oblasť utajovaných skutočností a elektronického podpisu stanovuje NBÚ, štandardy pre informačné systémy verejnej správy vydáva MF SR. Bezpečnostné aspekty sa môžu vyskytnúť aj v štandardoch vydávaných inými ústrednými orgánmi verejnej správy, napríklad MZ SR pre vedenie zdravotnej dokumentácie. Koordinácia v štandardizácii medzi jednotlivými inštitúciami je postavená na personálnom zastúpení zainteresovaných inštitúcií v príslušných komisiách MF SR a ÚNMS SR , ale koordinácia štandardizácie v informačnej bezpečnosti na inštitucionálnej úrovni neexistuje.

Medzinárodná spolupráca v oblasti informačnej bezpečnosti je potrebná na zabezpečenie kompatibility riešení a dostatočnej úrovne ochrany globálnej IKI. Dôvodom pre medzinárodnú spoluprácu je aj zložitosť samotnej oblasti informačnej bezpečnosti, čo spôsobuje, že väčšina krajín nemá dostatočné kapacity na samostatné budovanie potrebného know-how a aj tým najvyspelejším môže vývoj a implementácia potrebných riešení trvať nežiaduco dlho.

Slovensko sa v rámci svojich možností zapája do medzinárodnej spolupráce v informačnej bezpečnosti; je zastúpené v agentúre ENISA, pracovných skupinách EÚ (v pracovnej skupine pre informačnú bezpečnosť OECD, pracovné skupiny pre certifikáciu prostriedkov a akreditáciu systémov a sietí určených pre bezpečné a prenos dát v elektronických a komunikačných systémoch EÚ a pod.), v pracovných skupinách NATO, združení FESA a má prístup k pripravovaným informačno-bezpečnostným normám ISO. Jednotlivci a neštátne organizácie sú zastúpené aj v ďalších medzinárodných organizáciách (TC 11 IFIP a i.). Vyjadrené terminológiou ISO, Slovensko je zatiaľ vo väčšine uvedených medzinárodných organizácií pozorovateľom, ale na to, aby sa stalo plnohodnotným aktívnym členom, mu chýbajú odborné kapacity, materiálne podmienky a zázemie schopné plniť úlohy vyplývajúce z plnohodnotného členstva.

[4] Zákon 300/2005 Z. z. trestný zákon, § 247 Poškodenie a zneužitie záznamu na nosiči informácií

[5] Zákon č. 618/2003 Z. z. o autorskom práve a o právach súvisiacich s autorským právom v znení neskorších predpisov

[6] v medzinárodnom prostredí sa používa pojem štandard vo význame norma, v SR pojem norma slúži na označenie štandardizačného dokumentu vydaného SÚTN a štandard je štandardizačný dokument vydávaný ústrednými orgánmi verejnej správy.

3. Stratégia

Hlavnou úlohou v oblasti informačnej bezpečnosti je vytvoriť jednotnú platformu budovania informačnej spoločnosti postavenú na právnych základoch so zabezpečením primeranej ochrany a dôveryhodnosti digitálneho priestoru Slovenska. Nevyhnutnosťou pre úspešné plnenie tejto úlohy je vytvorenie Národnej stratégie pre informačnú bezpečnosť v SR, ako základného dokumentu štátu a následné rozpracovanie a realizácia konkrétnych úloh definovaných stratégiou. Dokument sa opiera o princípy definované Stratégiou pre bezpečnú informačnú spoločnosť – „Dialóg, partnerstvo a aktívne pôsobenie“, ktorú vydala Európska únia v roku 2006, Bezpečnostnej stratégie SR, ako aj o ďalšie strategické dokumenty informačne najvyspelejších štátov, ako napr. USA, Nemecko, Anglicko, Fínsko, Japonsko a pod.

NSIB je trojúrovňový dokument. Prvá úroveň predstavuje **strategické ciele** v informačnej bezpečnosti, ktoré majú dlhodobý charakter a pokrývajú všetky relevantné problémy, ktoré SR v tejto oblasti potrebuje riešiť.

Druhú úroveň predstavujú **strategické priority,** kde sa strategické ciele premietajú do špecializovaných oblastí a v rámci nich následne NSIB na tretej úrovni definuje najdôležitejšie problémy, ktoré sú premietnuté do **kľúčových úloh**.

3.1 Strategické ciele

Podľa stratégie Európskej únie je treba podporovať globálnu spoluprácu v oblasti informačnej bezpečnosti a dosiahnuť to, aby bol európsky priemysel používateľom vyžadujúcim vysokú úroveň bezpečnostných produktov a služieb a súčastne aj ich konkurenčným dodávateľom. Druhou základnou požiadavkou EÚ je štandardizovať vnútroštátne politiky členských štátov súvisiace s informačnou bezpečnosťou. Pri napĺňaní týchto požiadaviek treba dodržiavať princípy demokratickej spoločnosti a zohľadňovať oprávnené záujmy občanov, podnikateľskej sféry a verejnej správy vo vzťahu k občanom. Na zabezpečenie a udržanie potrebnej úrovne informačnej bezpečnosti v zmysle uvedenej stratégie sú stanovené nasledujúce strategické ciele:

1. **prevencia;** zaistenie adekvátnej ochrany digitálneho priestoru Slovenska, aby sa v maximálnej možnej miere predchádzalo bezpečnostným incidentom v ňom,
2. **pripravenosť;** zaistenie schopnosti efektívne reagovať na bezpečnostné incidenty, minimalizovať ich dosah a čas potrebný na obnovu činnosti informačných a komunikačných systémov po bezpečnostných incidentoch,
3. **udržateľnosť;** dosiahnutie, udržiavanie a rozširovanie kompetencie Slovenska v oblasti informačnej bezpečnosti.

Stanovené strategické ciele sú v súlade s Bezpečnostnou stratégiou SR, ktorá bola schválená Národnou radou SR v septembri 2005 a v súlade s prebiehajúcim procesom informatizácie spoločnosti. Podmienkou pre splnenie stanovených cieľov je, aby štát zabezpečil súčinnosť všetkých orgánov verejnej správy, špeciálnej štátnej správy, akademického sektora, súkromnej sféry, ale i občanov štátu. Nezastupiteľnou úlohou štátu v tomto zložitom procese je vytvoriť vhodné legislatívne prostredie, ako aj zabezpečiť organizačné, materiálne a finančné podmienky. Úlohou vlády je taktiež dôsledná kontrola plnenia akčných plánov a vyvodenie sankcií pri neplnení úloh, ako aj pružná reakcia na zmeny podmienok prichádzajúcich zvonku.

3.2 Strategické priority

Pre dosiahnutie stanovených strategických cieľov je potrebné doriešiť legislatívu, kompetencie, technicko-organizačne a finančné záležitosti, hierarchiu a spôsob riadenia, vzdelávanie a mnoho ďalších problémov. NSIB definuje 7 základných strategických priorít, ktorými sú:

1. ochrana ľudských práv a slobôd v súvislosti s využívaním NIKI,
2. budovanie povedomia a kompetentnosti v informačnej bezpečnosti,
3. vytváranie bezpečného prostredia,
4. zefektívnenie riadenia informačnej bezpečnosti,
5. zaistenie dostatočnej ochrany štátnej IKI a IKI podporujúcej kritickú infraštruktúru štátu,
6. národná a medzinárodná spolupráca,
7. rozširovanie národnej kompetencie.

3.2.1 Ochrana ľudských práv a slobôd

Potenciál IKT možno zneužiť, a preto treba hľadať spôsoby ochrany legitímnych záujmov všetkých, ktorých sa používanie IKT dotýka. Do digitálneho priestoru sa však ťažko prenášajú tradičné regulatívne a obranné mechanizmy, ktoré si spoločnosť v minulosti vytvorila. Sú to predovšetkým etika a morálka, ktoré sa vytvárajú postupne, sú vecou jednotlivcov, nanajvýš komunít a nemajú právnu silu. Treba vytvoriť dobré právne predpisy, ktoré umožňujú účinne postihovať zistené zločiny smerujúce k poškodzovaniu ľudských práv a slobôd. Vzhľadom na narastajúce bezpečnostné problémy digitálneho priestoru (počítačová kriminalita, organizovaný zločin, terorizmus) a význam globálnej (a národných) IKI pre spoločnosť, bude preto potrebné vytvoriť pre ochranu digitálneho priestoru právny rámec (v medzinárodnom aj národnom meradle). Aj v tejto oblasti sa však stretávajú záujmy a práva rôznych jedincov a organizácií a navrhované opatrenia (právne úpravy) musia zohľadňovať nielen záujmy štátu, vlastníkov IKT systémov, ale aj práva používateľov a tých, ktorých údaje sa v IKT systémoch nachádzajú[7].

NSIB vychádza z právneho rámca ochrany informácií SR, z direktív EÚ a z odporúčaní OECD zohľadňujúc kľúčové technické normy. Normou najvyššej právnej sily vzťahujúcej sa na ochranu ľudských práv pri zaisťovaní digitálneho priestoru je Listina ľudských práv a slobôd, ktorá občanom priznáva právo na nedotknuteľnosť osoby a jeho súkromia, ochranu ľudskej dôstojnosti, osobnej cti, dobrej povesti a mena, súkromného osobného a rodinného života, ochranu pred neoprávneným zhromažďovaním, zverejňovaním alebo iným zneužívaním údajov o svojej osobe. Ďalším základným dokumentom je Ústava Slovenskej republiky. V oblasti ochrany ľudských práv a slobôd stratégia identifikovala dve kľúčové úlohy:

a) presadzovanie demokratických princípov pri opatreniach na ochranu digitálneho priestoru SR,

[7] The security of information systems and networks should be compatible with essential values of a democratic society. (OECD Guidelines for the Security of Information Systems and Networks*)*

b) legislatívne upraviť prístup k osobným údajom tak, aby žiadna osoba nemala právo zoznamovať sa s nimi v rozsahu presahujúcom účel ich spracovania.

3.2.2 Budovanie povedomia a kompetentnosti v informačnej bezpečnosti

Z analýz vyplynulo, že veľa bezpečnostných incidentov súvisí s nedostatočnou odbornou úrovňou a znalosťami správcov informačných systémov, užívateľov, ale aj riadiacich pracovníkov v oblasti informačnej bezpečnosti. Z uvedeného dôvodu treba riešiť otázku kvalifikácie a vzdelávania. Za kvalifikáciu sa nepovažuje iba vzdelanie, ale predovšetkým prax v príslušnom odbore a získané odborné skúsenosti.

Z hľadiska možných hrozieb je preto na zaistenie ochrany digitálneho priestoru nevyhnutné dosiahnuť potrebnú úroveň *bezpečnostného povedomia* (t.j. poznania potreby a podstaty informačnej bezpečnosti) všetkých jej používateľov, a to s následnou transformáciu bezpečnostného povedomia do *kompetentnosti* (pochopenie a uplatňovanie vlastnej zodpovednosti za informačnú bezpečnosť pri práci s IKT). Stratégia identifikuje nasledujúce kľúčové úlohy na dosiahnutie a udržanie potrebnej úrovne bezpečnostného povedomia a kompetentnosti:

a) zvyšovanie úrovne poznania občanov, komerčných a nekomerčných organizácií, verejných inštitúcií o rizikách spojených s používaní IKT a možnostiach ochrany pred hrozbami pomocou internetu, masovokomunikačných prostriedkov a metodických materiálov,

b) rozšírenie vzdelávania (začlenenie základov informačnej bezpečnosti do výučby informatiky na školách),

c) zavedenie programov zvyšovania bezpečnostného povedomia a kompetentnosti používateľov IKT so zvláštnymi nárokmi na informačnú bezpečnosť.

3.2.3 Vytváranie bezpečného prostredia

Úlohou štátu je vytvárať vhodné podmienky spolupráce medzi všetkými zúčastnenými stranami. Ide predovšetkým o tvorbu legislatívneho rámca, vypracovávanie strategických dokumentov, metodických materiálov, stanovenie kompetencií, povinností a zodpovednosti. Dôležitou úlohou je aj vytváranie jednotných štandardov v oblasti informačnej bezpečnosti a koordinácia ich vydávania. Do procesu prípravy koncepčných materiálov treba zapojiť celú verejnú správu, akademický a súkromný sektor vrátane jednotlivcov. V záujme štátu je zabezpečiť ochranu celého digitálneho priestoru, a to zabezpečením vhodných foriem spolupráce s vlastníkmi a používateľmi. Stratégia v tomto smere identifikuje nasledujúce kľúčové úlohy vedúce k vytváraniu bezpečného prostredia:

a) koordinácia zabezpečenia digitálneho priestoru SR a zaistenia národnej bezpečnosti,

b) vytvorenie[8] dostatočného legislatívneho rámca na zaistenie informačnej bezpečnosti SR, zohľadňujúceho základné práva a slobody a medzinárodné záväzky SR (najmä voči EÚ),

c) posúdenie súčasných kompetencií a stanovenie zodpovednosti/definovanie povinností štátnych orgánov v oblasti informačnej bezpečnosti,

[8] analýza existujúcej legislatívy a jej prípadné doplnenie alebo aktualizácia

d) zosúladenie STN s aktuálnymi medzinárodnými normami z informačnej bezpečnosti, koordinácia vydávania štandardov pre oblasť informačnej bezpečnosti na Slovensku,

e) vytvorenie jednotnej metodiky pre neutajované skutočnosti pre bezpečnostnú kategorizáciu informácie a informačných a komunikačných systémov,

f) vypracovanie základných bezpečnostných požiadaviek na IKT záväzných pre štátnu IKI a odporúčaných pre ostatné komponenty NIKI (najmä systémy e-Health, e-Government a KRIS), kompatibilné s medzinárodnými normami a štandardmi,

g) vypracovanie a sprístupnenie metodických materiálov na dosiahnutie požadovanej/základnej úrovne informačnej bezpečnosti (smerníc a odporúčaných postupov[9]) a podpora zbližovania používaných bezpečnostných procedúr založených na odporúčaných postupoch v štátnom a súkromnom sektore,

h) v záujme zvýšenia dostupnosti bezpečnostných riešení aj pre malé firmy a jednotlivcov, podporovať riešenia a služby založené na dostupných (otvorených) štandardoch,

i) zapojenie komerčnej sféry a odbornej verejnosti do spracovania, pripomienkovania koncepčných materiálov, noriem a štandardov; vytvorenie priestoru na výmenu poznatkov a skúseností.

3.2.4 Zefektívnenie riadenia informačnej bezpečnosti

Pre dosiahnutie a udržanie požadovaného stavu IB je potrebné koordinovať ochranu aktív organizácie a zároveň vytvoriť efektívny systém jej riadenia. Na pozdvihnutie úrovne riadenia je treba poskytovať inštitúciám nielen metodickú pomoc pri riešení koncepčných otázok, ale pomáhať im aj pri riešení konkrétnych aktuálnych problémov (vrátane prípravy nariadení, metodických materiálov, školení, ako aj poradenstvo a odbornú pomoc). Dôležitým predpokladom efektívneho riadenia je preto monitorovanie stavu bezpečnosti, vyhodnocovanie a poskytovanie štatistík bezpečnostných incidentov pre potreby cieľových skupín. Na riešenie uvedených problémov treba stanoviť nasledujúce úlohy:

a) monitorovanie hrozieb,

b) vytvorenie systému včasného varovania (informovanie cieľových skupín o existujúcich hrozbách, varovanie potenciálnych cieľových skupín, vyhlásenie poplachu),

c) pomoc pri riešení bezpečnostných incidentov,

d) identifikácia, zaznamenávanie a vyhodnocovanie bezpečnostných incidentov,

e) monitorovanie efektívnosti navrhovaných opatrení na riešenie bezpečnostných incidentov.

f) koordinácia bezpečnostných stratégií jednotlivých systémov NIKI na zabezpečenie súčinnosti pri riadení NIKI.

[9] Guidelines a Best Practices

3.2.5 Zaistenie dostatočnej ochrany štátnej IKI a IKI podporujúcej kritickú infraštruktúru štátu

Štát ako vlastník informačných a komunikačných systémov, je povinný zabezpečiť ich primeranú ochranu tak, aby ich narušením nevznikli škody, resp. tieto škody boli minimalizované. Ide predovšetkým o systémy spadajúce do kritickej infraštruktúry štátu, zabezpečujúcej chod štátu, služby v priemysle, v energetike, zdravotníctve a sociálnom zabezpečení, doprave, bankovníctve a pod. Z Bezpečnostnej stratégie Slovenskej republiky schválenej Národnou radou SR v roku 2005 vyplýva, že *„Slovenská republika prijme opatrenia na obmedzenie zraniteľnosti prvkov kritickej infraštruktúry, s dôrazom na informačné a komunikačné systémy, a na minimalizáciu negatívnych následkov útokov na ne. Bude pokračovať v aktivitách zameraných na bezpečnosť a integritu informačných a komunikačných systémov, zvlášť systémov nevyhnutných pre bezpečný výkon základných funkcií štátu*“. Na problematiku ochrany informácií v oblasti kritickej infraštruktúry poukazuje aj Národný program pre ochranu a obranu kritickej infraštruktúry v SR schválený uznesením vlády č. 185/2008 z 26. marca 2008. Keďže súčasťou kritickej infraštruktúry sú aj neštátne systémy a štát je partnerom občanov a súkromných spoločností v administratívnych aj obchodných záležitostiach, musí okrem zabezpečenia svojich systémov zaistiť aj šírenie bezpečnostného povedomia v širokej verejnosti a presadzovanie primeraných bezpečnostných požiadaviek na neštátne systémy. Úlohy na zaistenie dostatočnej ochrany štátnej IKI a IKT systémov podporujúcich kritickú infraštruktúru štátu sú nasledujúce:

a) zlepšenie úrovne informačnej bezpečnosti v štátnych inštitúciách zavedením systému riadenia informačnej bezpečnosti,

b) zavádzanie a podpora používania bezpečných IKT produktov a systémov,

c) vypracovanie rámcových podmienok, návodov a odporúčaní (stanovenie záväzných rámcových bezpečnostných podmienok (bezpečnostných štandardov) pre systémy v pôsobnosti jednotlivých štátnych orgánov a návody, ako ich splniť; resp. odporúčania pre systémy, ktoré nie sú v pôsobnosti štátnych orgánov),

d) analyzovať stav zabezpečenia tej časti NIKI, ktorá je súčasťou kritickej infraštruktúry štátu alebo ju podporuje a v prípade potreby zaistiť aktualizáciu prijatých alebo prijatie nových opatrení.

3.2.6 Národná a medzinárodná spolupráca:

Vzhľadom na globálny charakter IB sú lokálne riešenia často nepostačujúce. Treba sa aktívne zapájať do činnosti kľúčových medzinárodných organizácií ENISA, OECD, CERT, ISO a pod. Preto je potrebná:

a) koordinácia národných úsilí pri ochrane digitálneho priestoru SR,

b) efektívne zapojenie sa do medzinárodnej spolupráce na základe analýzy potrieb a možností SR v oblasti informačnej bezpečnosti.

3.2.7 Rozširovanie národnej kompetencie:

Na trvalé udržanie potrebnej úrovne ochrany digitálneho priestoru SR sú dôležití vysoko kvalifikovaní odborníci, spoľahlivé IKT produkty a dôveryhodné IT služby, ďalej záštita a ústretovosť štátu a zainteresovaných subjektov. V tejto oblasti treba:

a) analyzovať kvalifikačné potreby Slovenska v oblasti informačnej bezpečnosti, možnosti školského a mimoškolského vzdelávania a zaviesť systém vzdelávania,

b) podporiť výskum a vývoj zameraný na perspektívne a aktuálne problémy informačnej bezpečnosti (najmä zintenzívnenie spolupráce štátu, súkromnej sféry a akademického prostredia),

c) využiť výsledky medzinárodnej spolupráce na podporu konkurencieschopnosti ekonomiky (sprístupňovanie informácií o problémoch, riešeniach, trendoch, legislatíve a štandardoch, medzinárodných iniciatívach v oblasti informačnej bezpečnosti.)

3.3 Štruktúra riadenia informačnej bezpečnosti

3.3.1 Aktuálna štruktúra riadenia

Aktuálna štruktúra riadenia informačnej bezpečnosti v SR, ktorá vychádza z kompetenčného zákona č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy v znení neskorších predpisov a o zmene a doplnení niektorých zákonov, je 3-úrovňová. Najvyšším orgánom je *vláda SR*, ktorá prerokúva a schvaľuje strategické a koncepčné materiály. Materiály vláde predkladajú rezorty v zmysle svojich kompetencií stanovených príslušnými zákonmi. Na základe kompetencií a svojho určenia nasleduje *ústredný orgán štátnej správy* zodpovedný za informačnú bezpečnosť verejnej správy, ktorým je v súčasnosti MF SR a na rovnakej úrovni ďalšie štátne orgány a úrady zodpovedajúce za špeciálne oblasti informačnej bezpečnosti MO SR, MV SR, MH SR, MK SR, MŠ SR, MZ SR, NBÚ, ÚOOÚ SR, resp. ÚNMS SR. Tretiu úroveň tvoria organizačné útvary štátnych orgánov, ktoré plnia konkrétne úlohy z oblasti informačnej bezpečnosti. Špecifické postavenie má o*dbor legislatívy, metodiky, štandardov a bezpečnosti informačných systémov s*ekcie informatizácie spoločnosti MF SR so svojou zložkou, ktorou je Komisia pre IB pri MF SR, a ktorej predsedá generálny riaditeľ sekcie informatizácie spoločnosti MF SR. Komisia v zmysle svojho štatútu[10] zabezpečuje analytickú a koncepčnú činnosť, prípravu strategických a odborných materiálov z oblasti informačnej bezpečnosti.

3.3.2 Návrh nového možného usporiadania

Návrh novej štruktúry vychádza z existujúcej štruktúry riadenia *„vláda - MF SR, ďalšie ÚOŠS SR a úrady so súčasnými kompetenciami v informačnej bezpečnosti“*. Na základe podrobnej analýzy súčasného zabezpečovania procesov treba vykonať optimalizáciu kompetencií (príprava materiálu na rokovanie vlády SR). Ďalším krokom bude vytvorenie národného strediska pre riešenie počítačových incidentov, CSIRT.SK (časť 3. 4. 1 a príloha č. 4). V časovom horizonte do 5 rokov bude treba doriešiť informačnú bezpečnosť SR po stránke legislatívnej (vytvorenie zákona o IB), organizačnej, personálnej a venovať patričnú pozornosť aj finančnému zabezpečeniu. V záverečnej fáze organizačného zabezpečenia sa odporúča vytvoriť národnú inštitúciu pre informačnú bezpečnosť neutajovanej časti NIKI (Národný úrad pre informačnú bezpečnosť SR, NÚIB SR). Podrobnejší postup riešenia

[10] Štatút Komisie pre informačnú bezpečnosť, *IRA_MFSR_12.2007_ROM.kom.inf.bezpečnosť, Číslo : MF/ 14462/2007 – 23*

informačnej bezpečnosti v SR bude obsahom Akčného plánu k NSIB v SR, ktorý bude vypracovaný do konca roku 2008.

3.4 Aktuálne priority informačnej bezpečnosti v SR

Aktuálne priority informačnej bezpečnosti vychádzajú z nepriaznivej situácie a výrazného zaostávania Slovenska za informačne vyspelými krajinami. Nepriaznivý stav je daný hlavne nedostatočnou implementáciou cieľov uvedených v strategických dokumentoch, chýbajúcou štátnou koncepciou IB a rámcom interoperability v SR, legislatívou, kompetenciami, povedomím, ako aj podporou kompetentných orgánov a ďalšími faktormi.

3.4.1 CSIRT.SK

Cieľom úlohy je vypracovanie návrhu organizačného, personálneho, materiálno-technického a finančného zabezpečenia jednotky kontaktného miesta pre riešenie bezpečnostných incidentov a následné zriadenie špecializovanej organizácie pre riešenie problematiky počítačového zločinu, vzájomnej spolupráce, výmeny informácií a skúseností na vnútroštátnej úrovni s prepojením do celoeurópskeho priestoru. Inštitúcia bude plniť úlohy uvedené v časti 3.2.4 (najmä prvé 4 úlohy). Taktiež sa bude podieľať aj na riešení úloh z časti 3.2.6., úloh Akčného plánu, resp. ďalších. Uvedenú skutočnosť vnímajú aj medzinárodné organizácie zaoberajúce sa IT bezpečnosťou, ktoré zdôrazňovali fakt, že nemajú v prípade IT bezpečnostných incidentov medzinárodného charakteru v SR koho kontaktovať. Vzhľadom na nedostatok odborných kapacít v informačnej bezpečnosti sa v činnosti CSIRT.SK uvažuje aj s využitím kapacít pracovníkov z neštátnych organizácií. Vzhľadom na to, že tento stav bude prechodný, CSIRT.SK bude disponovať obmedzenými právomocami. V ďalšom bude potrebné zvážiť doplnenie výkonných právomocí, ktoré určí zákon.

3.4.2 Koordinácia štandardizačnej činnosti

Štandardy sú nástrojom na dosiahnutie medzinárodnej interoperability všetkých riešení a potrebnej úrovne informačnej bezpečnosti. **Chýba prístup** k pripravovaným medzinárodným štandardom a koordinácia vydávania štandardov v SR, ako **aj prehľad** o relevantných medzinárodných normách, finančné zabezpečenie na ich zavedenie do STN. Aktívna účasť zástupcov SR v medzinárodných štandardizačných organizáciách je len sporadická. Problémom je aj **roztrieštenosť kompetencií**, duálne vydávanie štandardov a ich vzájomná nekompatibilita. Východiskom je doriešenie kompetencií a zabezpečenie koordinácie tvorby a vydávania noriem a štandardov v kľúčových organizáciách, ktorými sú MF SR, MZ SR, MK SR, NBÚ, ÚGKK SR a ÚNMS SR. Pri preberaní schválených štandardov je nevyhnutná účasť zástupcov SR v medzinárodných štandardizačných organizáciách. Z uvedeného dôvodu je nevyhnutné vypracovať prehľad stavu štandardizačnej činnosti v informačnej bezpečnosti v oblasti:

a) kompetencií slovenských orgánov pri vydávaní štandardov,

b) existujúcich slovenských štandardov,

c) medzinárodných štandardizačných organizácií,

d) medzinárodných štandardov, ktoré by Slovensko malo prijať,

e) de facto štandardov[11],

f) kapacít Slovenska na kompetentnú štandardizačnú činnosť.

g) zastúpenia SR v medzinárodných štandardizačných organizáciách a iniciatívach.

Na základe uvedeného prehľadu bude možné navrhnúť rozdelenie kompetencií v štandardizačnej činnosti a koordináciu činnosti pri aktualizácii existujúcich, resp. vydávanie nových noriem a štandardov, ako aj mechanizmu kontroly dodržiavania existujúcich noriem a štandardov.

3.4.3 Budovanie a rozširovanie poznania

Rozširovanie a budovanie poznania je predpokladom zvyšovania kvalifikácie a odbornej úrovne pracovníkov v oblasti informačnej bezpečnosti. Ide tu hlavne o produkciu poznania, ktorá je výsledkom tvorivého, vedecko-technického bádania. Rozširovanie poznania, čiže reprodukcia je spojená s výchovou a vzdelávaním vo vzdelávacích inštitúciách. Poznanie v informačnej bezpečnosti je možné kategorizovať na:

a) všeobecné základné, predstavujúce znalosti na úrovni používateľa, ktorý potrebuje vedieť, čo má a čo nemá robiť a asi prečo, ale nepotrebuje podrobné zdôvodnenie príčin,

b) všeobecné informatické – znalosti na úrovni informatika, ale nie špecialistu v oblasti informačnej bezpečnosti, ktorý pozná systém, vie implementovať a udržiavať jeho bezpečnostné mechanizmy na základe odporučení (bezpečnostných politík) a transformovať bezpečnostné požiadavky do prevádzkových pravidiel systému,

c) špecializované bezpečnostné – poznanie na úrovni špecialistu v oblasti informačnej bezpečnosti, ktorý dokáže analyzovať systém, jeho bezpečnostné okolie, spraviť analýzu rizík a navrhnúť opatrenia na ich elimináciu; alebo posúdiť komplexne zabezpečenie systému (audítor). Špecialista má prehľad o stave a vývoji hrozieb a bezpečnostných riešeniach, manažérskych a právnych aspektoch informačnej bezpečnosti a je schopný tvoriť koncepčné materiály.

d) aplikačno-bezpečnostné – poznanie na úrovni špecialistu v inom odbore (najmä právnici a vyšetrovatelia), ktorý potrebuje pri riešení svojich úloh poznať podstatu bezpečnostných problémov a je schopný spolupracovať so špecialistami všetkých úrovní.

e) inovatívne – poznanie špecialistu výskumníka v oblasti informačnej bezpečnosti (alebo niektorej z jej podoblastí) umožňujúce nachádzať principiálne nové riešenia.

Súčasne s informatickou a odbornou zložkou vzdelania treba zabezpečiť aj jazykovú zložku a v SR venovať primeranú pozornosť vzdelávaniu vo všetkých vyššie uvedených kategóriách.

3.4.4 Medzinárodná spolupráca

Z členstva v EÚ, OECD, ISO a ďalších medzinárodných organizáciách vyplývajú pre SR povinnosti, ale aj možnosť zúčastňovať sa na tvorbe politiky týchto inštitúcií tak, aby

[11] všeobecne akceptovaných technických noriem, ktoré nemajú formálny status štandardu (napr. v oblasti elektronického podpisu a kryptológie sú to PKCS štandardy)

zohľadňovala aj záujmy SR. Treba identifikovať tie orgány medzinárodných inštitúcií, ktoré túto činnosť v oblasti informačnej bezpečnosti vykonávajú a následne zabezpečiť zastúpenie Slovenska kvalifikovanými pracovníkmi. Nutným predpokladom spolupráce je aj vytvorenie priaznivých podmienok pre činnosť a zabezpečovanie účasti zástupcov Slovenska v týchto odborných orgánoch.

Koordinačným orgánom pre oblasť medzinárodnej činnosti v oblasti informačnej bezpečnosti neutajovanej časti NIKI bude Komisia pre informačnú bezpečnosť pri MF SR. Okrem aktívnej činnosti v medzinárodných organizáciách bude potrebné rozvíjať aj bilaterálnu a multilaterálnu spoluprácu na konkrétnych problémoch (napríklad štandardizácia v oblasti informačnej bezpečnosti v SR a ČR, vzájomné uznávanie elektronických podpisov a pod). Medzinárodná spolupráca napomôže rozširovanie poznania a zvyšovanie počtu kvalifikovaných odborníkov na Slovensku.

3.4.5 Vzdelávanie

Kritickým faktorom, od ktorého priamo závisí schopnosť nachádzať a implementovať adekvátne riešenia bezpečnostných problémov, je kompetentnosť ľudí, ktorá úzko súvisí s nadobúdaním vedomostí. V tejto oblasti treba vykonať analýzu stavu:

a) potreby poznatkov jednotlivých kategórií používateľov IKT (laickí používatelia, informatici a odborníci v informačnej bezpečnosti),

b) kapacitné a obsahové možnosti školského a iného vzdelávania (celoživotné vzdelávanie, firemné kurzy, e-learning, ECDL, EUCIP a pod.)

a na základe tejto analýzy navrhnúť:

c) doplnenie, resp. rozšírenie obsahu informatických alebo iných predmetov študijných programov stredných škôl o problematiku informačnej bezpečnosti,

d) systém celoživotného vzdelávania (základný kurz a udržiavacie kurzy) pre informatikov (správcov systémov) zo štátnej a súkromnej sféry,

e) vydávať a podporovať vydávanie odbornej literatúry a metodických dokumentov zameraných na riešenie vybraných problémov informačnej bezpečnosti.

Vzdelávanie a vydávanie odbornej literatúry priamo rieši úloh č. 3 v časti 4. 2. Zjednodušená forma úlohy, ktorú treba aktualizovať, je obsiahnutá pod číslom *3. c. 2* v Akčnom pláne informatizácie spoločnosti.

4. Realizácia stratégie

4.1 Implementácia stratégie

Realizácia spočíva v schválení dokumentu „NSIB vládou SR“, riešení kľúčových úloh definovaných strategickými prioritami, vypracovaním Akčného plánu SR v informačnej bezpečnosti na roky 2008 – 2013 a jeho schválení vládou SR. Kontrola plnenia úloh a ich stav budú predkladané každoročne na rokovanie vlády SR v podobe správ, resp. ďalších návrhov.

4.2 Rámcový návrh plnenia úloh v roku 2008

Úlohy na nasledujúce obdobie vychádzajú zo súčasnej situácie informačnej bezpečnosti v SR v porovnaní so stavom v členských štátoch EÚ, ako aj s porovnaním stavu s

vyspelými štátmi sveta. Ich návrh je v súlade so kľúčovými dokumentmi, smernicami a odporúčaniami EÚ/EK, ako aj stanovenými strategickými prioritami tohto materiálu.

Definované úlohy sú:

1. Vypracovať Návrh organizačného, personálneho, materiálno-technického a finančného zabezpečenia na vytvorenie špecializovanej jednotky (CSIRT.SK) pre riešenie počítačových incidentov v Slovenskej republike. CSIRT.SK bude inštitúciou, ktorá bude:
   - sústreďovať poznatky o aktuálnych hrozbách a možnostiach ich riešenia a zverejňovať ich,
   - slúžiť ako centrum včasného varovania,
   - pomáhať pri riešení bezpečnostných incidentov,
   - zberať informácie o bezpečnostných incidentoch a ich vplyv na území SR,
   - spolupracovať s podobnými inštitúciami v zahraničí,
   - metodicky pomáhať vybudovať podobné inštitúcie v štátnych a súkromných organizáciách na Slovensku,
   - sústreďovať odborníkov v oblasti informačnej bezpečnosti a zapájaním do svojej činnosti pripravovať ďalších odborníkov.

   Podrobnejší popis vzťahov medzi touto úlohou a ďalšími úlohami Akčného plánu a kľúčovými úlohami Národnej stratégie bude popísaný v materiáli „Návrh Akčného plánu na roky 2008 – 2013“.

2. Vypracovať legislatívny zámer zákona o IB verejnej správy v SR a pripraviť novelu výnosu MDPT SR č. 1706/M-2006 o štandardoch pre informačné systémy verejnej správy, t. j. prepracovať jej piatu časť „Bezpečnostné štandardy“.

3. Vypracovať návrh systému vzdelávania v oblasti informačnej bezpečnosti v SR. Cieľom tejto úlohy je zistiť, čo by jednotliví používatelia NIKI mali o informačnej bezpečnosti vedieť, ako ich to naučiť a príprava konkrétneho riešenia pre laikov/informatikov zo štátnej správy. Táto úloha pozostáva z:
   a) vypracovania štúdie uskutočniteľnosti, ktorá bude analyzovať
      - akým spôsobom sa robí príprava odborníkov v informačnej bezpečnosti, informatikov a laikov vo svete,
      - aký je súčasný stav vyučovania informačnej bezpečnosti v SR
      - aké sú vzdelanostné potreby (kto, čo potrebuje vedieť, v akom rozsahu)
      - kto a za akých podmienok by bol schopný potrebné vzdelávanie poskytovať.

   b) návrhu systému vzdelávania pre informatikov zo štátnych orgánov:
      - dve cieľové skupiny (základné vzdelávanie pre laikov, celoživotné aktualizačné vzdelávanie pre informatikov)
      - spracovanie návrhu organizácie a obsahu vzdelávania
      - návrh študijného programu

c) pilotného projektu vzdelávania pre laikov/informatikov z verejnej správy v oblasti informačnej bezpečnosti

4. Vypracovať Návrh Akčného plánu k dokumentu Národná stratégia pre informačnú bezpečnosť v SR na obdobie rokov 2008 až 2013,

5. Vypracovať prehľad stavu štandardizačnej činnosti v oblasti informačnej bezpečnosti. Cieľom úlohy je sprehľadniť všetky normy z oblasti informačnej bezpečnosti, ktoré by mohli byť užitočné pre SR, normy, ktoré existujú, resp. sa pripravujú, aký je stav informačno-bezpečnostných noriem a štandardov v SR, kto ich vydáva. Výsledky tohto projektu by mohli poslúžiť ako základ pre aktualizáciu STN v oblasti informačnej bezpečnosti, zosúladenie a skvalitnenie vydávania noriem a štandardov v SR ako aj činnosti SR v medzinárodných štandardizačných organizáciách. Výstupom riešenia tejto úlohy bude analytická štúdia, ktorá bude obsahovať:

   - prehľad relevantných medzinárodných štandardizačných organizácií a zastúpení SR v nich,
   - prehľad kompetencií slovenských organizácií v štandardizačnej činnosti,
   - prehľad súčasných slovenských noriem (aktuálne a na vyradenie),
   - zoznam noriem, ktoré je potrebné zaradiť do STN,
   - prehľad užitočných štandardov, ktoré nie sú začleniteľné do STN,
   - analýza stavu, nedostatkov a návrhu spôsobu riešenia situácie v oblasti normotvorby v oblasti informačnej bezpečnosti v SR.

   Na základe uvedeného prehľadu bude možné navrhnúť rozdelenie kompetencií v štandardizačnej činnosti a koordináciu činnosti pri aktualizácii existujúcich, resp. vydávanie nových noriem a štandardov.

6. Vykonať analýzu stavu IB v SR. Existujú štyri základné zdroje informácií, umožňujúce charakterizovať stav informačnej bezpečnosti:

   - zverejnené štúdie, štatistiky, analýzy z domácich a zahraničných zdrojov,
   - vlastné analytické štúdie (zamerané buď na analýzu systémov a produktov, alebo na prieskum situácie vo vybraných segmentoch NIKI),
   - údaje z monitoringu bezpečnostných incidentov,
   - povinné hlásenia, napr. o používanom programovom vybavení, bezpečnostných riešeniach, bezpečnostných incidentoch a pod[12].

   Bude treba vytvoriť systém zberu a spracovania informácií na vytváranie priebežnej predstavy o stave informačnej bezpečnosti v SR a na spracovanie výročnej správy, vrátane požiadaviek na informačné zdroje, návrh použitia spracovaných informácií (komu sa čo bude poskytovať, za akých podmienok a čo sa bude zverejňovať). Paralelne s vytváraním systému treba pripravovať priebežné informácie o stave informačnej bezpečnosti aspoň vo vybraných oblastiach (zlomyseľný softvér, spam, nelegálny softvér) a informácie o aktuálnom stave zverejňovať.

[12] minimálne v štátnej časti NIKI by sa dal využívať aj tento zdroj informácií

7. Vydávanie metodických materiálov z oblasti informačnej bezpečnosti. Prvým materiálom bude výkladový slovník informačnej bezpečnosti, ktorého úlohou je najmä zjednotenie odbornej terminológie v oblasti informačnej bezpečnosti pre účely tvorby legislatívnych materiálov a strategických dokumentov. Slovník by sa mal aktualizovať v intervaloch cca raz za dva roky.

4.3 Finančné zabezpečenie a časový harmonogram

4.3.1 Finančné prostriedky pre rok 2008

Finančné prostriedky, ktoré navrhovaný materiál zakladá v roku 2008 na štátny rozpočet sú pokryté v rámci rozpočtovej kapitoly MF SR. Jednotlivé úlohy, odhad pracovných kapacít a termíny sú uvedené v nasledujúcej tabuľke.

Tabuľka: Rámcový odhad nákladov a časovej náročnosti rok 2008

	Názov úlohy	Odhadovaná časová kapacita (človo. / hod)	Odhad nákl. (tis. Sk)	Termín	Zodpoved.	Poznámka
1.	Návrh CSIRT.SK	600		31. 12. 2008	MF SR	návrh
2.	Prehľad stavu štandardizačnej činnosti (stav, normy)	1500		30. 11. 2008	MF SR	štúdia
3.	Analýza stavu IB v SR	600		30. 11. 2008	MF SR	štúdia
4.	Návrh systému vzdelávania vrátane zavedenia pilotného projektu	2000		31. 12. 2008	MF SR	Štúdia, systém, pilot, metodiky
5.	Akčný plán k stratégii	1000		31. 03. 2009	MF SR	návrh
6.	Terminologický slovník IB	1600		31. 12. 2008	MF SR, MK SR	el. vydania
7.	Legislatívny zámer zákona o IB	600		31. 12. 2009	MF SR	návrh
	Rámcové náklady spolu		**6 000**			

4.3.2 Finančné prostriedky pre roky 2009 - 2013

Finančné zabezpečenie 2. fázy úloh na roky 2009 – 2013 vrátane kvantifikácie, termínov a odhadovaných nákladov bude obsiahnuté v Akčnom pláne k stratégii. Financovanie úloh sa navrhuje riešiť čiastočne zo štátneho rozpočtu, z rozpočtovej kapitoly MF SR a z rozpočtových kapitol štátneho rozpočtu, z finančných prostriedkov EÚ zo štrukturálnych fondov Operačného programu informatizácie spoločnosti – OPIS. Z uvedeného dôvodu bude potrebné prispôsobiť čerpanie pre riešenie navrhovaných aktivít v súlade s podmienkami a pravidlami čerpania prostriedkov zo štrukturálnych fondov a budú zabezpečené v rámci schválených limitov. Predpokladá sa, že na realizáciu niektorých aktivít budú použité aj finančné prostriedky z privátneho sektora.

5. Záver

NSIB v SR je koncipovaná na obdobie platnosti 5 rokov, t. j. na roky 2008 – 2013 s predpokladom využitia finančných prostriedkov zo štátneho rozpočtu, zo štrukturálnych fondov OPIS a predpokladá sa aj využitie finančných prostriedkov privátneho sektoru. Dokument bol vytvorený MF SR v spolupráci a akademickým a privátnym sektorom. Následne bol prerokovaný poradným orgánom ministra financií, ktorým je Komisia pre informačnú bezpečnosť. Obsah dokumentu vychádza zo strategických materiálov schválených vládou SR, smerníc, nariadení, odporúčaní a strategických materiálov EÚ/EK.

Prostriedky vynaložené na zaistenie informačnej bezpečnosti nemajú priamo vyčísliteľnú návratnosť, keďže implementácia účinných bezpečnostných riešení redukuje možnosti bezpečnostných incidentov, ktoré by znamenali straty v dôsledku poškodenia, nedostupnosti informačných a komunikačných systémov, zneužitia informácií alebo ohrozenia fungovania riadiacich, výrobných, alebo iných systémov. Meranie účelnosti vynaložených prostriedkov bude možné až vtedy, keď budú k dispozícii údaje o počte a dosahoch bezpečnostných incidentov pred a po zavedení bezpečnostných opatrení. Zatiaľ sa dajú dosahy iba odhadovať na základe poznatkov zo zahraničia[13]. Dosah informačnej bezpečnosti, okrem znižovania finančných vplyvov bezpečnostných incidentov, možno posúdiť z hľadiska dôveryhodnosti Slovenska v zahraničí a vytvárania podmienok pre občanov a podnikateľské subjekty. Znamená to urýchlené riešenie bezpečnostných problémov, pochádzajúcich zo zdrojov na Slovensku (útoky na zahraničné systémy z počítačov na Slovensku, šírenie nelegálneho obsahu zo Slovenska, medzinárodná trestná činnosť využívajúca slovenskú NIKI) a kompetentné zapojenie Slovenska do medzinárodnej spolupráce v oblasti informačnej bezpečnosti. Pozitívne dosahy sú aj z pohľadu realizácie projektov spadajúcich do kategórií eGovernment, eHealth alebo eBusiness, ako aj zaistenie ochrany autorských práv, sprístupnenie budúcich požiadaviek na produkty (budúce štandardy) a pod. Hodnotenie vplyvov informačnej bezpečnosti bude riešené osobitne v spoločnom materiáli[14] pripravovanom MH SR v časti *„6. Popis spôsobu analyzovania vplyvov na informatizáciu spoločnosti“*.

[13] v Holandsku dosiahli 85 % redukciu holandského spamu implementáciou antispamového vybavenia za 570.000 EUR

[14] Materiál „Návrh jednotnej metodiky na posudzovanie vybraných vplyvov“ (ďalej len „jednotná metodika“) bol vypracovaný v súlade s Programovým vyhlásením vlády Slovenskej republiky, uznesením vlády Slovenskej republiky č. 833 z 3. októbra 2007 a Národnou lisabonskou stratégiou, ktorá hodnotenie vplyvov regulácií považuje za jednu z prioritných úloh.
„V záujme dosiahnutia pokroku v tejto oblasti schválila vláda Slovenskej republiky uznesenie č. 833 dňa 3. októbra 2007 k Agende lepšej regulácie v Slovenskej republike *a Akčnému programu znižovania administratívneho zaťaženia podnikania v Slovenskej republike 2007-2012.“*