Pavel BUČKA[1], Ondřej NOVOSAD[2]

Globálny pohľad na informačnú bezpečnosť v Slovenskej Republike

Globalne spojrzenie na bezpieczeństwo informacji na Słowacji

Streszczenie:
Obecnie, w rozwijającym się świecie, prawdopodobnie jest już współczesny człowiek, rozwijające się organizacje lub proces funkcjonowania, które zmniejszą znaczenie informacji w dynamicznie zmieniającym się społeczeństwie, stale przekształcającym się ze społeczeństwa industrialnego w społeczeństwo informacyjne. W tego typu społeczeństwie, świadomość i zrozumienie konceptu informacji jest nieodzowne aby poprawnie zdefiniować wymagania związanie z bezpieczeństwem informacji. Kiedy pojawia się informacja, ważnym jest aby wiedzieć jak z nią postępować i kiedy staje się nieważna. Zrozumienie konceptu informacji jest również kluczowe do zdobycia umiejętności oceny ważności informacji w celu określenia jej właściwej wartości oraz właściwych poziomów i form ochrony.
Słowa kluczowe: informacja, bezpieczeństwo informacji, technologia informacyjna, systemy informacyjne

A global view of information security in Slovakia

Abstract
In the developed world at present, perhaps there is already a modern man, growing organization, or functioning process, which would reduce the importance of information in dynamically changing society and its gradual transformation from an industrial society to an information society. In such a society is awareness and understanding of the concept of information necessary to adequately define the requirements for information security and in particular of a number of key aspects. When information arises, how to handle information and when the information becomes void. Understanding the concept of information is also a prerequisite for obtaining the ability to assess the importance of information to quantify its fair value and define the desired level and form of its protection.
Keywords: Information, information security, information technology, information systems.

[1] doc. Ing. CSc Katedra bezpečnosti a obrany, Akadémia ozbrojených síl gen. M. R. Štefánika, Liptovský Mikuláš, Slovensko
[2] brig. gen. Ing. Veliteľ Pozemných síl OS SR, Trenčín, Slovensko

ÚVOD

Tak ako sa moderná spoločnosť stala vo všetkých oblastiach nášho života závislou na komunikačných a informačných technológiách, tak isto sa pre modernú spoločnosť stalo nevyhnutnosťou pochopiť, čo je predmetom informačnej bezpečnosti a ako sa nás informačná bezpečnosť dotýka. V článku rozoberieme východiská a priestor pôsobnosti informačnej bezpečnosti, pokúsime sa definovať komplexnosť a zložitosť problematiky. Poukážeme na jednotlivé aspekty informačnej bezpečnosti a to najmä rozsiahlosť a komplexnosť legislatívneho rámca pre informačnú bezpečnosť, odporúčané odborné normatívne akty a možnú postavenie Ozbrojených síl Slovenskej republiky (OS SR) pri zabezpečovaní strategických cieľov Slovenskej republiky (SR), ako aj schopnosti reagovať na možné tendencie vývoja.

Bežným problémom organizácií je nízka pozornosť venovaná informačnej bezpečnosti, nízke materiálne a finančné krytie ako aj nedostatočný počet kvalifikovaných pracovníkov, ktorí by riešili informačnú bezpečnosť. Je zaujímavé, že organizácie sú povinné[3] riešiť bezpečnostného zamestnanca a bezpečnosť ochrany zdravia pri práci pomerne nezávislým postavením funkcie v organizačnej štruktúre ale informačná bezpečnosť takto ponímaná nie je, aj keď by si to určite zaslúžila. Niektorí vedúci pracovníci si dobre uvedomujú nutnosť chrániť informačné systémy, technológie, či aktíva organizácií a uvedomujú si aj potrebu zaoberať sa riešením tejto problematiky. Prax ukazuje, že žiaden systém sa nezaobíde bez technických či procesných kontrolných mechanizmov. Nezávislé objektívne posudzovanie kvality a vyhodnocovania účinnosti riadenia informačnej bezpečnosti v súlade s medzinárodnými štandardmi by malo byť v súčasnosti už nevyhnutnou a neoddeliteľnou súčasťou každej organizácie.

[3] Zákon o bezpečnosti a ochrane zdravia pri práci a o zmene a doplnení niektorých zákonov (v znení č. 309/2007 Z. z., 140/2008 Z. z., 132/2010 Z. z., 136/2010 Z. z., 470/2011 Z. z.)

1. VYMEDZENIE POJMU INFORMÁCIA A INFORMAČNÁ BEZPEČNOSŤ

Podľa Organizácie pre hospodársku spoluprácu a rozvoj OECD[4] (Organisation for Economic Cooperation and Development) je v príručke „*Guidelines for the Security of lnformation Systems and Networks - Towards a Culture of Security* “ uvedené že:

a) **Informácia** je správa, oznam, hodnota, fakty, skutočnosti o určitej udalosti, jave alebo činnosti, ktoré sa ďalej spracovávajú. Informáciou je označovaný aj druh poznania alebo správy, ktorú možno použiť v prospech prijatia rozhodnutia alebo zlepšenia určitej činnosti. Informácie môžu existovať v mnohých formách. Môžu byť vytlačené alebo napísané na papieri, uložené elektronicky (vo forme dát), prenášané poštou alebo pri použití elektronických prostriedkov, premietnuté, či vyslovené v konverzáciách.

b) **Dáta alebo údaj** sú informácie, ktorú sme už zaznamenali nejakým naším zmyslom. Údajmi sú informácie, nachádzajúce sa na digitálnych záznamových prostriedkoch alebo nosičoch, uložené v postupnosti znakov.

Ak v dobe vzniku nevieme informáciu adekvátne ohodnotiť, je veľmi ťažké určiť aj jej požadovaný stupeň ochrany, či možné následky zlyhania informačnej bezpečnosti (napríklad zverejnenie informácií na sociálnych sieťach o práci, nadriadených, pohybe vojakov, ich úlohách, misiách, technike a pod.).

V prípade informačnej bezpečnosti definujeme voči pojmu informácia najčastejšie aspekty ako: aktíva, bezpečnostné okolie, hrozba, zraniteľnosť, riziko, nositeľ hrozby, útok.

Bezpečnostné aspekty informácie sú dôvernosť definovaná ako vlastnosť, na základe ktorej informácie nie sú sprístupňované a odhaľované

[4]www.oecd.org/sti/ieconomy/15582260.pdf

neautorizovaným osobám, entitám alebo procesom, čo znamená, že prístup k informácii majú len oprávnené osoby, systémy a procesy.

Norma ISO/IEC 27005:2011 definuje hrozbu, ako možnú príčinu neželaného incidentu, ktorý môže vyústiť do poškodenia systému alebo celej organizácie. Incident je signalizovaný jednou, alebo viacerými udalosťami, pri ktorých je vysoká pravdepodobnosť kompromitácie aktív organizácie a ohrozenia informačnej bezpečnosti. Mať schopnosť reagovať na hrozbu a minimalizovať jej dopady, znamená mať schopnosť včasne identifikovať udalosti, mať adekvátny dosah na technológie a riadiace procesy, činnosti personálu, alebo jej aktívne predchádzať. Aby hrozba mohla spôsobiť poškodenie systému, alebo organizácie, využíva takzvanú zraniteľnosť systému, procesov, personálu, ktoré sa nazývajú slabé miesta. Slabé miesta sú napríklad v oblastiach: fyzickej, personálnej, organizačnej, riadiacej, legislatívnej, hardvérovej a softvérovej.

Hrozby môžu byť úmyselné ľudské hrozby (hacking, odpočúvanie, zmena/zámena, vymazanie a pod.), neúmyselné ľudské chyby (chyba, zabudnutie, nesprávne adresovanie, nastavenie apod.) a fyzické ako napríklad blesk, požiar. Často opakujúca sa hrozba je ale aj finančné poddimenzovanie servisu a prevádzky technológií a systémov zabezpečujúce informačnú bezpečnosť alebo personálu v oblastiach ich nevyhnutného vzdelania, respektíve nezabezpečenie kontinuity personálnej, procesnej či technologickej ochrany aktív. V týchto prípadoch ide o interné zvyšovanie hrozby vzniku incidentu bez určeného rozsahu dopadu.

Pod informačnou bezpečnosťou väčšina „laikov“ chápe ochranu informačno-komunikačných technológií (IKT) a všetkého s nimi súvisiaceho. Aj keď informačná bezpečnosť nie je samostatným vedným odborom, ako napríklad matematika či fyzika, je dnes minimálne takou istou súčasťou našich

životov, akými sa stali malá násobilka, písanie a čítanie teda gramotnosť[5]. Každý sa snaží chrániť svoje aktíva, logicky predchádzať hrozbám, či strate dôveryhodnosti voči svojmu okoliu.

Informačná bezpečnosť z pohľadu ochrany technológií a informačných systémov sa chápe ako "schopnosť siete alebo informačného systému ako celku odolať s určitou úrovňou spoľahlivosti náhodným udalostiam, nezákonnému alebo zákernému konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu a dôvernosť uchovávaných alebo prenášaných údajov a súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a systémov."[6]

Ak do systému zaradíme ďalšie prvky, akými bezpochyby sú ľudia (správcovia, používatelia, manažéri), relevantné organizačné vzťahy a väzby (verejná, štátna, podnikateľská sféra a ich ekonomické, hospodárske, či iné vzťahy), vlastné a relevantné procesy, rôznorodosť systémov a väzieb. V tomto prípade je informačná bezpečnosť definovaná ako „Komplexná ochrana informácií, schopností, spôsobilostí a zodpovedností, (jednotlivcov a taktiež organizačných jednotiek) komunikačných a informačných technológií, procesov, prostriedkov a zdrojov, ako aj metód, vnútorných a vonkajších väzieb takéhoto systému“.

Príklady incidentov informačnej bezpečnosti sú narušenie obsahu web stránky, inštalácia nežiaduceho softvéru, zmeny nastavení, kradnutie údajov, či často sa vyskytujúce zlyhávanie zamestnancov, ktorí odovzdávajú svoje heslá a strácajú tak v kybernetickom priestore vlastnú elektronickú identitu.

V súčasnosti najrozsiahlejší podiel na porušovaní informačnej bezpečnosti tvoria krádeže, zneužitia a neoprávnené manipulácie s informáciami (osobné, obchodné)[7]. Môžeme povedať, že možnosť získania a zneužitia informácií nastáva vždy, skôr ako vzniká relevantná ochrana

[5] http://www.ecdl.sk/certifikacia-ecdl
[6] http://www.informatizacia.sk/informacna-bezpecnost/
[7] http://www.informatizacia.sk/prieskum-stavu-ib/12772s

a z tohto pohľadu je informatizácia a elektronizácia nášho života (podpora životných činností a aktivít, manipulácia s údajmi, apod.) len vyváženie rizík výhodami v podobe vykonávania činnosti elektronicky. Nie len jednotlivci, ale aj celé spoločnosti[8] smerujú k stále pravidelnejšiemu a významnejšiemu využívaniu IKT v živote a význam informačnej bezpečnosti a jej dodržiavania narastá v rozsahu integrácie geometrickou radou. Informačná bezpečnosť musí pokryť minimálne problematiku bezpečnosti voči technickým prostriedkom, organizačným pravidlám a politikám, definovať právne a ekonomické vzťahy.

Pre správne pochopenie informačnej bezpečnosti ako systému, definujeme nasledujúce prvky a základné vzťahy medzi nimi:

1. Ľudia (laici, informatici a administrátori, manažment, bezpečnostní špecialisti).

2. Nástroje a produkty (IKT pre vznik, zmeny, šírenie, kopírovanie či archiváciu informácií, ale aj IKT pre manažment samotnej informačnej bezpečnosti).

3. Procesy (organizačné, kontrolné, produktívne, bezpečnostné apod.).

4. Interné normatívne akty (stratégie, zákony, doktríny, smernice, metodiky, normy, postupy, prevádzkové a organizačné nariadenia, vyhlášky apod.).

Pri identifikácii informácií musíme vedieť minimálne pochopiť a ohodnotiť hrozbu, určiť zraniteľnosť ako sumár rizík, vedieť definovať všetky mechanizmy a relevantné procesy. Vedieť eliminovať hrozbu, znamená schopnosť použiť všetky dostupné organizačné, finančné, materiálové či personálne zdroje. Vymenované aspekty informačnej bezpečnosti následne definujú schopnosť riadiť a vyhodnocovať stav informačnej bezpečnosti a navrhovať kroky k jej zlepšeniu. K tomu, aby štát, rezorty, či organizácie takúto spôsobilosť získali je nutné implementovať informačnú bezpečnosť do

[8] http://www.informatizacia.sk/egovernment/519s

praxe štátnej a verejnej správy a ich vzťahu k organizáciám pôsobiacich v priestore SR prostredníctvom príslušného legislatívneho rámca, ktorým sa všetky zúčastnené prvky skoordinujú.

U legislatívy budeme vychádzať z predpokladu, že ak je legislatíva obsahovo správna a všetci dodržujú stanovené kritériá, podmienky, ustanovenia, pôsobnosti, zodpovednosti či povinnosti, potom sú dosahované ciele štátu pre takto legislatívne definovaný priestor informačnej bezpečnosti. Táto téza slúži na definovanie problematiky rámca legislatívy a jej vzťahu k aktuálnej vymožiteľnosti voči samotným princípom informačnej bezpečnosti a stanoveným úlohám OS SR v Bezpečnostnej stratégie SR.

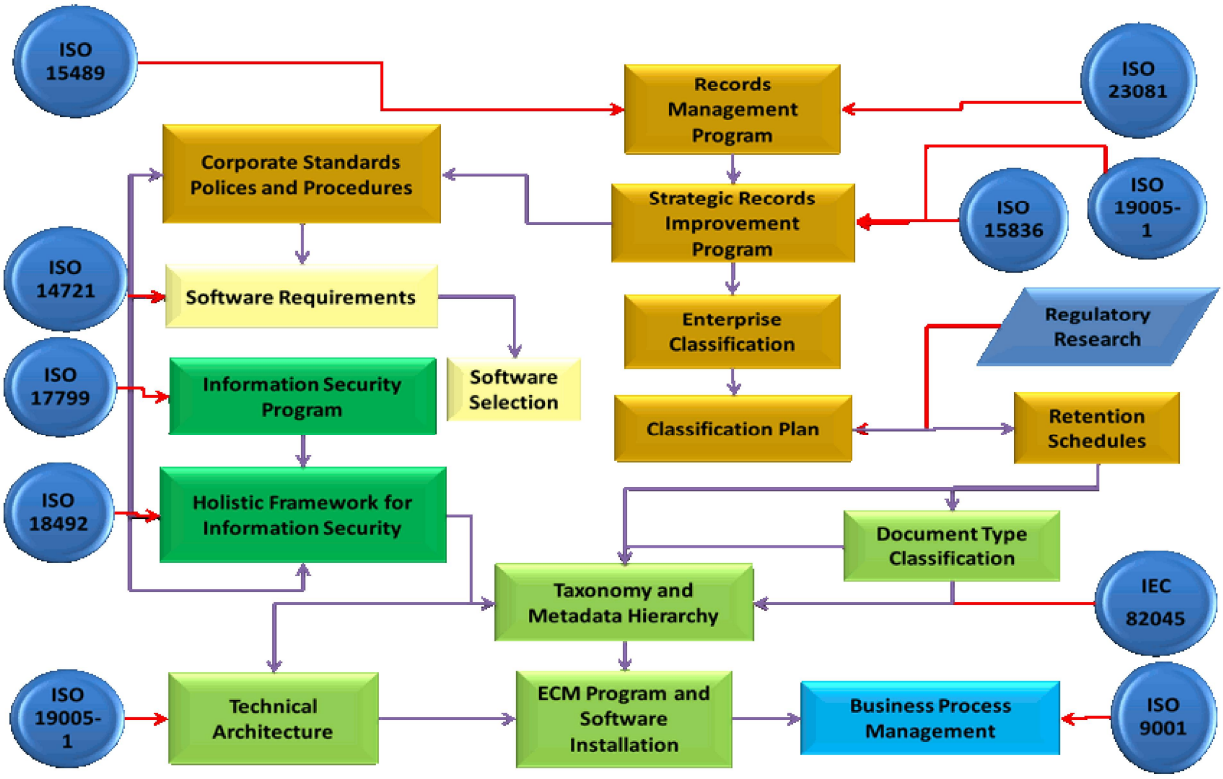
V nasledujúcej časti sa pokúsime priblížiť komplexný pohľad na aktuálny stav informačnej bezpečnosti v SR. Prečo je v štáte nevyhnutná legislatívna koordinácia je definované vysvetlením, že informácia je aktívum, inak povedané majetok organizácie[9]. Keď hovoríme o informačnej bezpečnosti hovoríme doslovne o ochrane financií investovaných do informačných systémov, práce, činností ľudí a výsledkov ich práce, ako aj ochrane základných ľudských práv deklarovaných ústavou SR. Dopady úniku, zneužitia, zmeny údajov, zlyhania informačných systémov, technológií majú väčšinou nezvratný charakter a finančné krytie odstraňovania dopadov a dôsledkov je väčšinou omnoho väčšie ako by bola samotná prevencia. Investícia finančných prostriedkov musí byť priamoúmerná hodnote aktív. V prípade štátnej správy a jednotlivých rezortov ide o adekvátne ohodnotenie ochrany v podobe investícií do informačnej bezpečnosti ako aj riešenie vzájomných kompetencií a pôsobností tak, aby bola dosiahnutá optimálna vymožiteľná informačná bezpečnosť, teda ochrana majetku štátu. Cieľom by malo byť optimálne zabezpečenie spôsobilostí štátnej a verejnej správy voči svojím občanom, tak ako to Slovenská republika deklaruje v strategických dokumentoch.

[9]Zákon č.278/1993 Z.z. Zákon o správe majetku štátu v znení 345/2012 Z. z

Rozpracovanie vymožiteľnosti práva občanov na deklarované strategické ciele SR a garancie istôt, by mala riešiť legislatíva SR.

1.1 Normatívny a strategický rámec informačnej bezpečnosti Slovenskej republiky

Pod štandardom a normou budeme chápať medzinárodný štandard, alebo normu označovanú ako ISO alebo ISO/IEC[10]. Štandard je súbor požiadaviek, metód, postupov, osvedčených kľúčových praktík a znalostí zozbieraných a sformalizovaných do všeobecne a opakovateľne vykonateľnej podoby. Najčastejšie sú normy určené k navrhnutiu, zavedeniu a udržiavaniu vzájomne závislých procesov pre efektívne a cielené riadenie problematiky v pôsobnosti normy (obrázok 1).



Obrázok 1 Mapa ISO štandardov

Zdroj: http://www.leger.ca/GRIS/NormesetStandards.html

[10] www.iso.org

Normy riadenia informačnej bezpečnosti musia zostať efektívne a účinné v dlhodobom horizonte, byť schopné prispôsobovať sa zmenám vo vnútri organizácie ale aj vplyvom vonkajšieho prostredia. V súlade s normami sa najčastejšie certifikujú[11] procesy (postup, účel, plnenie požiadaviek v jednotlivých fázach, metódy a rozsah, udržateľnosť a iné), následne technológie a informačné systémy či ľudia. Všeobecne používané štandardy akými sú napríklad ISO/IEC 27000 dokážu v organizácii nezriedka dosiahnuť 85% minimalizácií škôd vzniknutých z incidentov a bezpečnostných udalostí, navŕšiť návratnosť investícií o 50%, či v 90% zlepšiť procesy, kontinuitu, či schopnosti rozvoja v jednotlivých sférach pôsobností.

1.2 Najznámejšie medzinárodné normy pre riadenie informačnej bezpečnosti

Štandard ISO 17799 je súbor postupov pre management bezpečnosti informácií[12], prostredníctvom ktorých sa zabezpečuje eliminácia rizík pôsobiacich na informačný systém.

ISO 17799: časť 1:1995 Code of Practice for Information Security Management“ je súhrn najlepších bezpečnostných postupov určených na vytvorenie a implementáciu vlastného bezpečnostného systému. Špecifikuje viac ako 100 opatrení v 10 sekciách: bezpečnostná politika, organizácia bezpečnosti, klasifikácia a riadenie aktív, personálna bezpečnosť, fyzická bezpečnosť a bezpečnosť prostredia, správa počítačov a sietí, systém riadenia prístupu, vývoj a údržba systémov, plány kontinuity činností (havarijné plány), zabezpečenie súladu.

ISO 17799: časť 2:1998 Specifications for Information Security Management“ je špecifikácia krokov ako hodnotiť bezpečnostný systém a tvorí základ pre formálne hodnotenie bezpečnostného systému. Druhá časť je

[11] www.qscert.sk
[12] www.itsm.sk

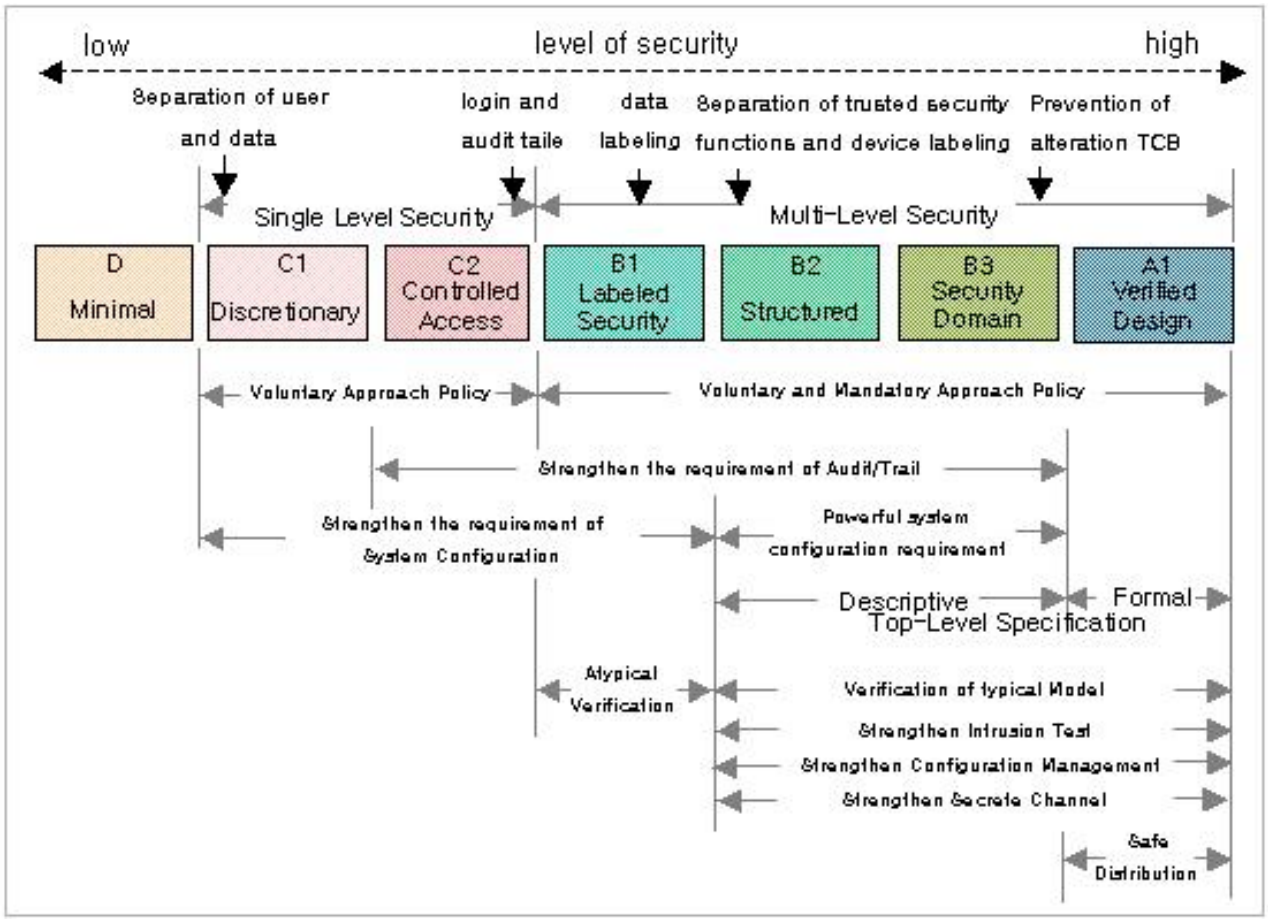
rozdelená do troch sekcií, kde prvá obsahuje výklad pojmov, druhá stanovené požiadavky projektovania a prevádzky bezpečnostného systému a tretia uvádza zoznam aplikovateľných bezpečnostných opatrení.

Štandard STN ISO/IEC 27001 (STN ISO/IEC 27001:2005 - Systémy manažérstva informačnej bezpečnosti) – upravuje konkrétne postupy zabezpečenia informačnej bezpečnosti. Je rozdelená do desiatich kapitol. Postupnou aplikáciou v súlade s touto normou je možné dosiahnuť efektívne a bezpečné riadenie všetkých informácií v pôsobnosti organizácie, respektíve fyzickej osoby a tiež stanovuje aj postupy nakladania s informáciami tretích strán. Pri zavádzaní systému manažérstva informačnej bezpečnosti sa vychádza z normy STN ISO/IEC 17799.

Štandard STN ISO/IEC 27001:2006 popisuje systém manažérstva informačnej bezpečnosti – Information Security Management System (ISMS), založený na podobných princípoch ako systém manažérstva kvality (ISO 9001:2005) a systém environmentálneho manažérstva (ISO 14001:2004). Cieľom tohto systému je riadiť procesy narábania s informáciami pre zabezpečenie dôvernosti, dostupnosti a integrity. Často je ISMS pochopený zle a to ako systém zaoberajúci sa len bezpečnosťou informačného systému alebo informačných technológií. Norma je určená pre všetky typy organizácií bez rozdielu zamerania či veľkosti. Zaviezť ho môžu tak výrobné, obchodné, servisné, montážne, ako aj poradenské či vzdelávacie organizácie zo všetkých oblastí štátnej správy, priemyslu a služieb, teda všetky organizácie a to bez ohľadu na to či používajú informačné technológie[13].

Štandard „Trusted Computer Evaluation Criteria“ (TCSEC) predstavuje kritériá hodnotenia zabezpečenia počítačových systémov, ktorý umožňuje jednotne ohodnotiť stupeň ochrany (obrázok 2).

[13] www.isaca.org



Obrázok 2 Jednotlivé úrovne podľa TCSEC

Zdroj: http://www.tsonnet.co.kr/eng/eng_faq.php?mode=read&id=5&offset=0%3E

Štandard definuje množinu kritérií pre tvorbu a hodnotenie systémov, ktoré poskytujú špecifické sady bezpečnostných funkcií. Informačné systémy sú hodnotené ako jeden celok, nehodnotia sa jeho jednotlivé komponenty. Systémy sú zaraďované do 4 základných tried bezpečnosti a to A, B, C, D, ktoré sa ešte delia na 7 podtried: A1, B1, B2, B3, C1, C2, D, pričom trieda A predstavuje najvyššiu úroveň požadovanej bezpečnosti.

Štandard „International Trusted Evaluation Criteria“ (ITSEC) predstavuje formálne zosúladené kritériá vypracované v spolupráci krajín EÚ, ktoré umožnia používateľom a hodnotiteľom informačných systémov postupovať jednotne pri hodnotení stupňa ochrany systémov a produktov IT a ktoré majú voči TCSEC doplňujúci charakter. Štandard určuje kritériá, ktoré je možné aplikovať na jednotlivé produkty alebo na celé informačné systémy.

Štandard definuje 7 tried miery ručenia bezpečnosti E0, E1, E2, E3, E4, E5, E6, pričom trieda E0 predstavuje najnižšiu úroveň bezpečnosti (obrázok 3).

ITSEC	CC	Security Evaluation
0	EAL1	Functional Tested
1	EAL2	Structural Tested
2	EAL3	Methodically tested and proofed
3	EAL4	Methodically developed, tested and proofed
4	EAL5	Semiformal developed and tested
5	EAL6	Semiformal verification of the design
6	EAL7	Formal verification of the design

Obrázok 3 Jednotlivé úrovne podľa ITSEC

Zdroj: http://www.itwissen.info/definition/lexikon/information-technology-security-evaluation-criteria-ITSEC.html

US TCSEC	European ITSEC	Common criteria	Description
D	E0	EAL1	Functionally tested
C1	E1	EAL2	Structurally tested
C2	E2	EAL3	Methodically tested and checked
B1	E3	EAL4	Methodically designed, tested and reviewed
B2	E4	EAL5	Semi-formally designed and tested
B3	E5	EAL6	Semi-formally verified design and tested
A1	E6	EAL7	Formally verified design and tested

Obrázok 4 Porovnanie ekvivalentného hodnotenia medzi TCSEC a ITSEC

Zdroj: http://www.emeraldinsight.com/journals.htm?articleid=1847135&show=html

Štandard ISO/IEC 15408 (Common Criteria for Information Technology Security Evaluation) predstavuje výsledok medzinárodnej snahy zlúčiť existujúce európske (ITSEC) a americké (TCSEC) štandardy a kritériá hodnotenia informačnej bezpečnosti. Hodnotený je produkt informačného systému, samotný systém alebo jeho časť (obrázok 5). Objekty hodnotenia sú

zaraďované do 8 kvalitatívnych úrovní EAL0 – EAL7, pričom úroveň EAL0 predstavuje najnižšiu úroveň bezpečnosti.

Japan IT Security Evaluation and Certification Scheme

Certificate

is awarded to

Certification Number: C0096

Hitachi, Ltd.

Product Name: HiCommand Suite Common Component

Version: 05-51-01

Type of IT Product: IT Product (Foundational Module Software)

Evaluation Criteria:
- **Common Criteria for Information Technology Security Evaluation Version 2.3 (ISO/IEC 15408:2005)**

Evaluation Methodology:
- **Common Methodology for Information Technology Security Evaluation Version 2.3 (ISO/IEC 18045:2005)**

Assurance Level: **EAL2+ALC_FLR.1**
Protection Profile Conformance: **None**
Name of CCTL: **Electronic Commerce Security Technology Laboratory Inc, Evaluation Center**
Date of Certification: **May 30, 2007**

The IT product identified in this certificate has been evaluated at an approved evaluation facility established under the Japan IT Security Evaluation and Certification Scheme using the *Common Methodology for Information Technology Security Evaluation Version2.3(ISO/IEC 18045:2005)*, for conformance to the *Common Criteria for Information Technology Security Evaluation Version2.3(ISO/IEC 15408:2005)* . This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification/validation report. This evaluation has been conducted in accordance with the provisions of the Japan IT Security Evaluation and Certification Scheme and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by the Information-technology Promotion Agency or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by the Information-technology Promotion Agency or by any other organization that recognizes or gives effect to this certificate, is either expressed or implied.
The misuse of this certificate, including its use regarding the IT Product or system or PP of a version differing from that appearing in this certificate or the use of certificate for publications, such as advertisements and catalogs, in an incorrect or misleading manner may result in withdrawal of this certificate.

Original Signed
Buheita Fujiwara
Chairman

Date : July 11, 2007

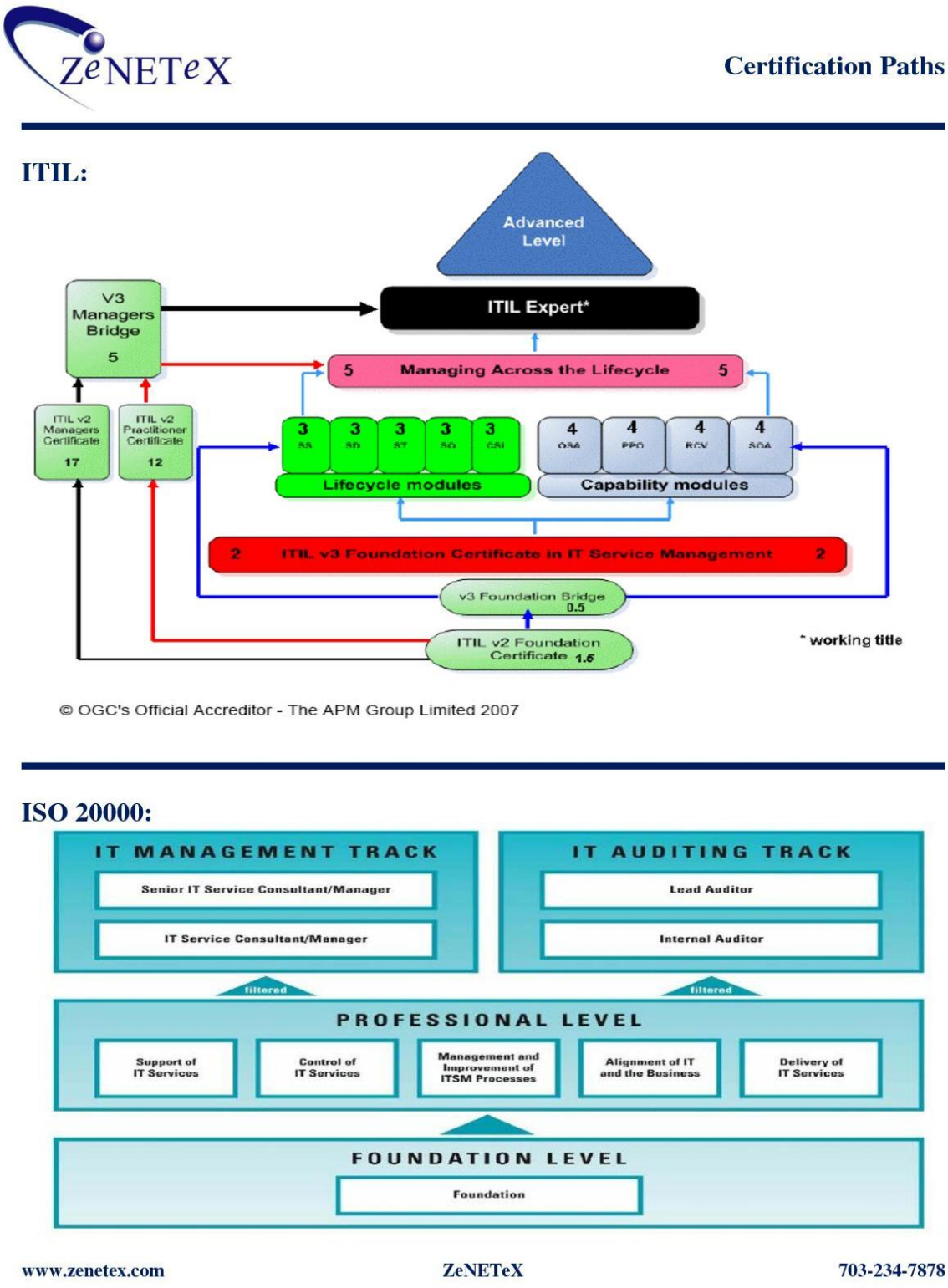
IPA Information-technology Promotion Agency, Japan

Obrázok 5 Vzor certifikátu splnenia ISO/IEC 15408:2005 a ISO/IEC 18045:2005
Zdroj: http://www.docstoc.com/docs/93153561/Certificate-is-Awarded-to-Hitachi-Ltd

Štandard ISO/IEC 20000 (Informačné technológie: Manažment služieb) táto norma definuje požiadavky kladené na poskytovateľa služieb, na dodávanie riadených služieb akceptovateľnej kvality, teda požadovanej úrovne riadenia informačnej bezpečnosti (obrázok 6). Výsledkom spoľahlivej prevádzky IKT pre používateľov sú služby, ktorých informačná bezpečnosť je neoddeliteľnou súčasťou. Služby informačnej bezpečnosti a služby v súlade s ISO/IEC 20000 sú ale dve odlišné problematiky. Zatiaľ čo služby poskytované v súlade s ISO/IEC 20000 sú poskytované takzvane „na požiadanie“, čo

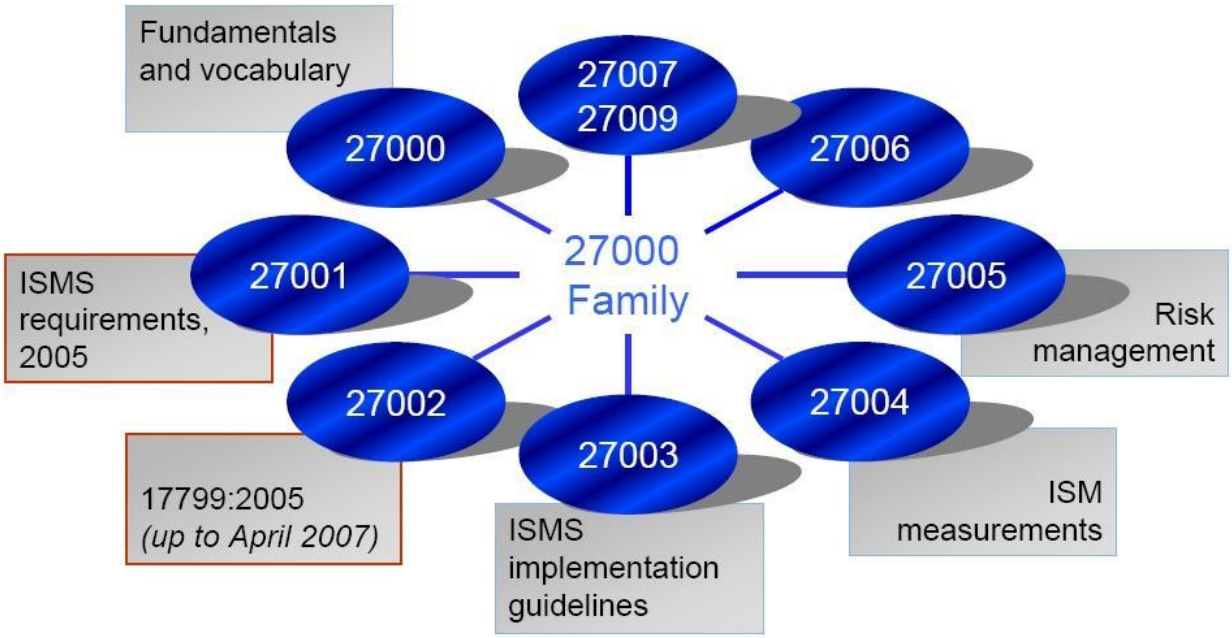
znamená, že vyplývajú z dopytu, služby informačnej bezpečnosti vychádzajú zo strategických cieľov organizácie ochrániť aktíva a sú kontinuálne v rámci riešení jednotlivých incidentov a odoziev na nich.

Základné rozdiely medzi štandardmi riadenia informačnej bezpečnosti ISO/IEC 27000 a štandardmi riadenia služieb informačných a komunikačných systémov ISO/IEC 20000 sú v aplikovateľnosti štandardov. Zatiaľ čo štandard ISO/IEC 27000 (obrázok 7) je určený na strategickú a operačnú úroveň, štandard ISO/IEC 20000 je aplikovateľný len do operačnej úrovne riadenia. ISO/IEC 27000 je všeobecne aplikovateľný, ISO/IEC 20000 je aplikovateľný na IT.



Obrázok 6 Postup certifikácie podľa ISO/IEC 20000

Zdroj: http://www.docstoc.com/docs/32676740/Certification-Paths-ITIL-ISO-20000



Obrázok 7 Zobrazenie ISO štandardov 27000

Zdroj: http://www.leger.ca/GRIS/NormesetStandards.html

Môžeme povedať, že dôležitosť štandardizácie procesov v súlade s medzinárodnými normami nie je zrejmá, až kým nezlyhá systém a odstraňovanie následkov zlyhania nepoukáže na systémové, organizačné, či procesné chyby, vďaka ktorým došlo často k nenávratným škodám.

Prosperujúce a efektívne fungujúce organizácie, však aj v oblastiach riadenia vlastných procesov reagujú aktívne a to zavádzaním, či optimalizáciou procesov v súlade s medzinárodnými normami a tým predchádzajú reaktívnemu riešeniu nedostatkov riadenia a finančných či iných strát. Nie všetkým škodám sa však dá v problematike informačnej bezpečnosti predchádzať, respektíve na ne v potrebnom čase reagovať.

2. HLAVNÉ STRATEGICKÉ DOKUMENTY SR POPISUJÚCE VZŤAH K INFORMAČNEJ BEZPEČNOSTI

V tejto časti budeme vychádzať z dokumentov, v ktorých SR priamo deklarovala potrebu riešiť problematiku informačnej bezpečnosti v rámci zabezpečenia svojich strategických úloh a cieľov.

2.1 Bezpečnostná stratégia SR

Medzi deklarované záujmy SR[14] patria:

- zaručiť bezpečnosť občanov a chrániť ich ľudské práva a základné slobody,
- rozvíjať demokratické štátne zriadenie, právny štát a trhovú ekonomiku,
- vytvárať predpoklady trvalo udržateľného hospodárskeho rastu,
- byť spolu garantom bezpečnosti spojencov,
- prispievať k posilňovaniu a šíreniu slobody a demokracie, dodržiavania ľudských práv, právneho štátu, medzinárodného práva, mieru a stability vo svete.

Poslaním bezpečnostnej politiky SR je aktívne pôsobiť na bezpečnostné prostredie tak, aby chránila, podporovala, obhajovala, bránila a presadzovala bezpečnostné záujmy SR.

Ďalej SR deklarovala, že organizovaný zločin je pre ňu priamou hrozbou. Využíva technologický pokrok, nové komunikačné metódy a snaží sa prenikať do všetkých oblastí verejného života. Jeho aktivity sa sústreďujú na nelegálnu výrobu a distribúciu drog, nelegálnu migráciu, obchodovanie s ľuďmi, prostitúciu, počítačové pirátstvo, krádeže duševného vlastníctva, finančnú kriminalitu a iné. Medzinárodný organizovaný zločin je zdrojom financií a taktiež ľudských zdrojov pre terorizmus, podieľa sa na šírení zbraní hromadného ničenia, aktívne využíva regionálnu nestabilitu pochádzajúcu z konfliktov a nedostatočnú štátnu moc zlyhávajúcich štátov. Ako globálny fenomén ohrozuje nielen bezpečnosť a ekonomickú stabilitu štátov, ale prispieva k destabilizácii svetového hospodárskeho systému. Jeho aktivity

[14] www.mosr.sk/data/files/833.pdf

oslabujú integritu štátu, ohrozujú funkčnosť, nezávislosť, ústavnosť a demokratický charakter jeho orgánov a finančných inštitúcií. Organizovaný zločin pritom využíva a rozširuje korupciu a vytvára nelegálnu ekonomiku.

Miera informatizácie spoločnosti dosiahla vysoký stupeň a stále sa zvyšuje. Výkonnosť techniky, revolučné informačné a komunikačné technológie, nárast rýchlosti prenosu informácií a ich globálnej dostupnosti spôsobujú rýchlu globálnu premenu post industriálnej spoločnosti na spoločnosť informačnú. Zraniteľnosť informačných a komunikačných systémov, ich preťaženie, neoprávnený prístup k informáciám, šírenie počítačových vírusov a dezinformácií sú rastúcou hrozbou pre SR. Aktivity cudzích spravodajských služieb zamerané proti záujmom SR, ktoré využívajú tradičné aj netradičné metódy a nové technológie so záujmom o všetky oblasti spoločenského života predstavujú pre bezpečnosť SR stálu hrozbu. V súvislosti so vstupom SR do NATO a EÚ je pravdepodobné zvýšenie aktivít týchto služieb z krajín, ktoré nie sú členmi euroatlantických integračných zoskupení. Pokračujúca globalizácia prináša pre SR pozitívne aj negatívne vplyvy. Nepripravenosť štátu pružne reagovať na globalizáciu je vážnou bezpečnostnou výzvou. Globalizácia prináša so sebou javy a procesy, ktoré sa vymykajú kontrole štátu, stiera rozdiely medzi vnútornou a vonkajšou bezpečnosťou a hranice medzi domácou a zahraničnou politikou. Globálne operujúce ekonomické subjekty majú stále väčší vplyv na celosvetový vývoj. Rozmach v oblasti informačných technológií a všeobecný prístup k internetu uľahčujú dostupnosť zbraňových systémov a návodov na ich výrobu, ako aj ďalších skúseností potrebných pre plánovanie a uskutočnenie útokov. Globálne operujúce finančné trhy umožňujú teroristickým organizáciám presúvať prostriedky bez pomoci alebo vedomia štátov.

Základným cieľom bezpečnostnej politiky SR je zaručenie bezpečnosti občana a štátu v stabilnom a predvídateľnom bezpečnostnom prostredí. Účinnosť bezpečnostnej politiky SR je podmienená mierou efektívnosti orgánov

štátu, aktívnym pôsobením SR v medzinárodnom prostredí, mierou spolupráce štátnych orgánov a orgánov územnej samosprávy, mimovládnych organizácií, právnických osôb a fyzických osôb, mierou stotožnenia sa občanov s bezpečnostnými cieľmi a schopnosťou vlády získať pre tieto ciele podporu širokej verejnosti. Rozhodujúcim prostriedkom bezpečnostnej politiky SR je jej bezpečnostný systém. Základným predpokladom pre riadenie, výstavbu a rozvoj bezpečnostného systému SR sú efektívne fungujúce zákonodarné, výkonné a súdne orgány. Tieto sú zodpovedné za pripravenosť a akcieschopnosť nástrojov krízového manažmentu a včasné prijímanie a realizáciu opatrení zameraných na zaručenie bezpečnosti občanov a štátu.

2.2 Obranná stratégia SR

Obranná stratégia SR[15], vychádza z Bezpečnostnej stratégie SR. Formuluje politicko-vojenské východiská obrany SR s perspektívou desiatich rokov (schválená NR SR 23. 9. 2005). Obranná stratégia SR identifikuje určujúce tendencie vývoja bezpečnostného prostredia pre oblasť obrany a charakterizuje novú dimenziu jej obrannej politiky. Určuje jej základný cieľ, požiadavky na efektívnu obranu, ako aj na spôsobilosti OS SR a ostatné súčasti systému obrany štátu.

Slovensko sa stalo integrálnou súčasťou euroatlantického bezpečnostného spoločenstva a získalo zmluvne viazané bezpečnostné záruky. Súčasne sa stalo spolu garantom bezpečnosti spojencov. Obhajoba a presadzovanie bezpečnostných záujmov SR v širšom geografickom kontexte sa stáva základným predpokladom jej bezpečnosti a obranyschopnosti. Hrozba teroristických útokov, šírenie zbraní hromadného ničenia, regionálne konflikty, zlyhávajúce štáty, organizovaný zločin, rast možností zneužitia kybernetického priestoru, radikálne ideológie a nevyriešené spory spolu s pôsobením takých faktorov, akými sú globalizácia, demografický vývoj, migrácia, ekologické

[15] www.mod.gov.sk/data/files/832.pdf

zmeny, možnosť získania jadrových zbraní ďalšími štátmi, napätia sprevádzajúce zabezpečovanie životne dôležitých zdrojov spôsobujú nárast nestability a neistoty, ktorý so sebou prináša vysokú mieru neurčitosti, nepredvídateľnosti a možnosť vzniku neočakávaných krízových situácií.

Na základe hodnotenia predpokladaného vývoja bezpečnostného prostredia a charakteru pôsobenia uvedených faktorov možno prijať politicko-vojenský záver, že SR v dlhodobom časovom horizonte nehrozí bezprostredný rozsiahly konvenčný vojenský konflikt a znižuje sa závažnosť a rozsah ďalších hrozieb vojenského charakteru. Zvyšuje sa však pravdepodobnosť a nebezpečenstvo nevojenských hrozieb, predovšetkým útokov medzinárodného terorizmu s možným dopadom na životy, zdravie a majetok občanov, ekonomický rozvoj a prosperitu štátu.

Zmena charakteru obrany SR má zásadný vplyv na schopnosť brániť SR a súčasne prispievať ku kolektívnej obrane NATO a vojenským spôsobilostiam EÚ, podieľať sa na aktivitách medzinárodného spoločenstva zameraných na boj s medzinárodným terorizmom, proti šíreniu zbraní hromadného ničenia, na prevenciu konfliktov a riešenie krízových situácií v nestabilných regiónoch sveta. Ministerstvo obrany SR zintenzívni úsilie pri presadzovaní komplexnosti a efektívnosti obrany, vytvorí predpoklady na zdokonalenie systému riadenia obrany a podmienky na kontinuitu strategického rozhodovania o smerovaní rozvoja a použití ozbrojených síl. Ďalší postup reformy ozbrojených síl podporí transformácia ostatných výkonných a podporných prvkov systému obrany. Cieľom bude zvyšovať úroveň použiteľnosti a operačnej pripravenosti ozbrojených síl, efektívnosť strategického spravodajstva, schopnosť využívať moderné informačné a komunikačné technológie, výkonnosť procedúr akvizície a obstarávania, ako aj procesov plánovania a vykonávania mobilizácie. Tento cieľ je možné

dosiahnuť prostredníctvom obranného plánovania harmonizovaného s obranným plánovaním NATO.

OS SR doposiaľ určené predovšetkým na obranu teritória štátu rozširia svoju pôsobnosť tak, aby okrem obrany SR prispievali aj k obrane spojencov a spolu s nimi dokázali predchádzať konfliktom a urovnávať krízové situácie vo svete. Tieto vojensko-strategické schopnosti ozbrojené sily dosiahnu realizáciou cieľov reformy a dlhodobých plánov rozvoja ozbrojených síl. Ozbrojené sily budú na základe rozhodnutia politického vedenia štátu plniť strategické úlohy, ďalšie úlohy vyplývajúce z prijatých medzinárodných záväzkov a asistenčné úlohy na podporu orgánov verejnej moci.

2.3 Národná stratégia SR pre informačnú bezpečnosť

Cieľom dokumentu[16] „Národná stratégia pre informačnú bezpečnosť v SR“ je vytvoriť základný rámec informačnej bezpečnosti SR.

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.

Národná stratégia pre informačnú bezpečnosť v SR definuje najvýznamnejšie strategické dokumenty týkajúce sa informačnej bezpečnosti v SR ako:

Bezpečnostná stratégia SR, Zákon č.45/2011 Z.z. „O kritickej infraštruktúre a Koncepcia ochrany utajovaných skutočností v SR. 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.

[16] http://www.informatizacia.sk/ext_dok-narodna_strategia_pre_ib/6167c

Národná stratégia pre informačnú bezpečnosť v SR je dokument delený na tri úrovne:

1. Strategické ciele v informačnej bezpečnosti, ktoré majú dlhodobý charakter a pokrývajú všetky relevantné problémy, ktoré SR v tejto oblasti potrebuje riešiť.
2. Strategické priority, kde sa strategické ciele premietajú do špecializovaných oblastí.
3. Definuje najdôležitejšie problémy, premietnuté následne do nosných úloh.

Stanovené strategické ciele sú v súlade s Bezpečnostnou stratégiou SR 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, a taktiež občanov štátu. Nezastupiteľnou úlohou štátu v tomto zložitom procese je vytvoriť vhodné legislatívne prostredie, a tiež zabezpečiť organizačné, materiálne a finančné podmienky. Pre dosiahnutie stanovených strategických cieľov je potrebné doriešiť legislatívu, kompetencie, technicko-organizačné a finančné záležitosti, hierarchiu a spôsob riadenia, vzdelávanie a mnoho ďalších problémov.

Národná stratégia pre informačnú bezpečnosť v SR definuje 7 základných strategických priorít, ktorými sú:

1. Ochrana ľudských práv a slobôd v súvislosti s využívaním národnej informačnej a komunikačnej infraštruktúry.
2. Budovanie povedomia a kompetentnosti v informačnej bezpečnosti.
3. Vytváranie bezpečného prostredia.
4. Zefektívnenie riadenia informačnej bezpečnosti.
5. Zaistenie dostatočnej ochrany štátnej informačnej a komunikačnej infraštruktúry a kritickej infraštruktúry štátu.

6. Národná a medzinárodná spolupráca.

7. Rozširovanie národnej kompetencie.

Aktuálna štruktúra riadenia informačnej bezpečnosti v SR je rozdelená do 3 úrovní.

Prvá úroveň: najvyšším orgánom je vláda SR, ktorá prerokúva a schvaľuje strategické a koncepčné materiály. Materiály vláde predkladajú rezorty v zmysle svojich kompetencií stanovených príslušnými zákonmi.

Druhá úroveň: na základe kompetencií a svojho určenia nasleduje ústredný orgán štátnej správy zodpovedný za informačnú bezpečnosť verejnej správy, ktorým je v súčasnosti Ministerstvo financií SR a na rovnakej úrovni ďalšie štátne orgány a úrady zodpovedajúce za špeciálne oblasti informačnej bezpečnosti Ministerstvo obrany SR, Ministerstvo vnútra SR, Ministerstvo hospodárstva SR, Ministerstvo kultúry SR, Ministerstvo školstva SR, Ministerstvo zdravotníctva SR, Národný bezpečnostný úrad, Úrad na ochranu osobných údajov SR, respektíve Úrad pre normalizáciu, metrológiu a skúšobníctvo SR.

Tretia úroveň: tvoria ju organizačné útvary štátnych orgánov, ktoré plnia konkrétne úlohy z oblasti informačnej bezpečnosti.

Špecifické postavenie má odbor legislatívy, metodiky, štandardov a bezpečnosti informačných systémov sekcie informatizácie spoločnosti Ministerstva financií SR so svojou zložkou, ktorou je Komisia pre informačnú bezpečnosť pri Ministerstve financií SR. Komisia v zmysle svojho štatútu zabezpečuje analytickú a koncepčnú činnosť, prípravu strategických a odborných materiálov z oblasti informačnej bezpečnosti.

2.4 Pripravovaný zákon o informačnej bezpečnosti

Súčasný právny poriadok SR obsahuje viacero noriem, ktoré riešia čiastkové problémy, ale jednotný, všeobecný právny predpis pre informačnú bezpečnosť digitálneho priestoru v slovenskej legislatíve v súčasnosti

neexistuje. Absencia legislatívy a centralizácie sa prejavuje v terminológie, používaní bezpečnostných štandardov, kompetenciách štátnych orgánov či neúplnosti pokrytia problematiky informačnej bezpečnosti. Digitálny priestor SR je súčasťou globálneho, celosvetového priestoru. Vďaka vzájomnej previazanosti technológií je nevyhnutná aj medzinárodná koordinácia ochrany a obrany globálneho digitálneho priestoru. Na riešenie bezpečnostných problémov digitálneho priestoru bola zriadená uznesením vlády č. 479/2009 jednotka pre riešenie počítačových incidentov (Computer Security and Incident Response Team) v SR. Aby si táto jednotka pre riešenie počítačových incidentov mohla plniť stanovené úlohy v domácom aj medzinárodnom meradle, je potrebné legislatívne vymedziť jej kompetencie a vzťahy k ostatným štátnym orgánom SR.

ZÁVER

Môžeme povedať, že aj keď náš digitálny priestor, či kritická infraštruktúra a informačné systémy veľkých spoločností nie sú pre medzinárodný terorizmus a armády s modernými jednotkami špecializovanými na kybernetické útoky zatiaľ natoľko zaujímavé, ako je to u iných krajín, tento trend nemusí platiť navždy. Tendencia vývoja a možné hrozby vtiahnutia SR do takejto konfrontácie sú na dennom poriadku. Na zaistenie svojej informačnej bezpečnosti a teda následne aj štátnej, hospodárskej či ekonomickej stability má SR podstatne menšie zdroje ako iné vyspelé krajiny. SR sa aktivitami sústreďuje na zaistenie informačnej bezpečnosti vo vybraných oblastiach (utajované skutočnosti a osobné údaje, informatizácia, centralizácia služieb používateľom) no v ostatných oblastiach informačnej bezpečnosti sú aktivity štátu nedostatočné. Pripravované rozsiahle štátne projekty z problematiky informačných a komunikačných technológií ako e-Government, e- Health apod. budú požiadavky na komplexné riešenie postupne zvyšovať.

V súčasnosti absentuje inštitúcia, ktorá by sa systematicky venovala všetkým aspektom informačnej bezpečnosti – od jej dizajnu na strategickej úrovni, cez monitoring incidentov skrz celú kritickú infraštruktúru až po jej vyhodnocovanie, či kontinuálne zlepšovanie stavu a pôsobnosti v spoločnosti. Môžeme povedať, že SR potrebuje čím skôr funkčnú jednotku, operujúcu v medzinárodnom priestore, ktorej hlavným cieľom je ochrana a obrana kybernetického priestoru SR a ktorá by bola schopná v maximálnej možnej miere minimalizovať škody a dopady jednotlivých incidentov. Na otázku, kto dnes zodpovedná za ochranu digitálneho priestoru, musíme odpovedať, že všetci.

Počítače dnes nenapádajú len jednotlivci snažiaci sa prostredníctvom svojej inteligencie stať „hrdinom“ ale sú to najmä organizované skupiny, ktoré kradnú údaje a pracujú pre tých ktorí platia. Počty nakazených počítačov a ich celková výpočtová a útočná sila predstavuje hrozbu, akú si málokto z bežných používateľ dokáže predstaviť. Odstavenie od internetu, lámanie hesiel, zlyhávanie distribuovaných sietí, mobilná komunikácia či iné sú dnes už klasickým útokom na infraštruktúru štátu a spoločnosti, ktorá sa vykonáva skôr ako vzniká reálny ozbrojený konflikt (príklady Gruzínsko, Estónsko).

LITERATÚRA

1. PFLEEGER, CH., P.: Security in Computing. 4th edition. Prentice-Hall International, Inc., 2007, ISBN: 0-13-239077-9.
2. BARTKO, F.: Strategické hodnotenie obrany SR a Biela kniha obrany SR, Euro- Atlantic Quarterly: roč. 6, 2/ 2011, s. 29 – 30. ISSN 1336-8761.
3. ORAVEC, M.: Posudzovanie rizík, Ostrava 2009, SPBI Ostrava, ISBN 978-80-7385-043
4. ŠOLC, M., TOMČOVÁ, T.: Prečo uvažovať o zavedení systému manažérstva informačnej bezpečnosti?, Bezpečnosť práce č. 2/2009, ISSN 1335-4078, 28-33.
5. GOLLMAN, D.: Computer Security. 3rd edition.John Wiley & Sons, 2011, ISBN: 978-0-470-74115-3.

6. Bezpečnostná stratégia Slovenskej republiky, NR SR, 2005.
7. Obranná stratégia Slovenskej republiky, NR SR, 2005.
8. Národná stratégia SR pre digitálnu integráciu, MF SR, 2008.
9. Národná stratégia pre informačnú bezpečnosť v Slovenskej republike, MF S, 2008.
10. Smernica pre zabezpečenie informačných systémov a sietí: Za kultúrou bezpečnosti, DSTI/ICCP(2002)12/REV2.
11. Developing ITIL - Mature Security Incident Response With SIEM – "A Plan for CSIRT Maturity Models vi.a
12. Zákon o bezpečnosti a ochrane zdravia pri práci a o zmene a doplnení niektorých zákonov
(v znení č. 309/2007 Z. z., 140/2008 Z. z., 132/2010 Z. z., 136/2010 Z. z., 470/2011 Z. z.).
13. *Zákon č.278/1993 Z.z. Zákon o správe majetku štátu v znení 345/2012 Z. z.*
14. http://www.leger.ca/GRIS/NormesetStandards.html
15. http://www.tsonnet.co.kr/eng/eng_faq.php?mode=read&id=5&offset=0%3E
16. http://www.itwissen.info/definition/lexikon/information-technology-security-evaluation-criteria-ITSEC.html
17. http://www.emeraldinsight.com/journals.htm?articleid=1847135&show=html
18. http://www.docstoc.com/docs/93153561/Certificate-is-Awarded-to-Hitachi-Ltd
19. http://www.docstoc.com/docs/32676740/Certification-Paths-ITIL-ISO-20000
20. http://www.leger.ca/GRIS/NormesetStandards.html
21. http://iso27001security.com/
22. http://csrc.nist.gov/publications/CSD_DocsGuide.pdf
23. *http://www.ecdl.sk/certifikacia-ecdl*
24. *http://www.informatizacia.sk/prieskum-stavu-ib/12772s*
25. http://www.informatizacia.sk/egovernment/519s
26. www.iso.org
27. *www.qscert.sk*
28. *www.itsm.sk*
29. www.isaca.org
30. www.mosr.sk/data/files/833.pdf
31. www.mod.gov.sk/data/files/832.pdf
32. http://www.informatizacia.sk/ext_dok-narodna_strategia_pre_ib/6167c