UNIVERZITA KOMENSKÉHO V BRATISLAVE
FAKULTA MATEMATIKY, FYZIKY A INFORMATIKY

Štandardizácia v oblasti informačnej bezpečnosti

Martin Kralovič **2008**

Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky
Katedra informatiky

Štandardizácia v oblasti informačnej bezpečnosti

DIPLOMOVÁ PRÁCA

Martin Kralovič

Študijný odbor: Informatika

Vedúci diplomovej práce:
Doc. RNDr. Daniel Olejár, PhD.

BRATISLAVA 2008

Týmto vyhlasujem, že som túto záverečnú prácu vypracoval samostatne, len s použitím uvedenej literatúry

V Bratislave, 7.5.2008

.....

Martin Kralovič

Na tomto mieste by som sa rád poďakoval vedúcemu mojej diplomovej práce, Doc. RNDr. Danielovi Olejárovi, PhD., za podnetné pripomienky a rady, ktoré nepochybne prispeli k skvalitneniu tejto práce.

Abstrakt

Kralovič, Martin: Štandardizácia v oblasti informačnej bezpečnosti. [Diplomová práca]. Univerzita Komenského v Bratislave. Fakulta matematiky, fyziky a informatiky; Katedra informatiky. Vedúci diplomovej práce: Doc. RNDr. Daniel Olejár, PhD. Bratislava, 2008. 71 s.

Diplomová práca sa zaoberá štandardizáciou v oblasti informačnej bezpečnosti. Poskytuje stručný prehľad o štandardizácii v oblasti IB vo svete a na Slovensku. Rozoberá možnosti na zlepšenie stavu štandardizácie IB na Slovensku. Navrhuje kategorizáciu, zjednodušujúcu orientáciu vo veľkom množstve bezpečnostných štandardov vydávaných rôznymi štandardizačnými organizáciami a špecifikáciu aplikácie na podporu činnosti štandardizačnej komisie SÚTN.

Kľúčové slová: informačná bezpečnosť, štandardizácia, kategorizácia štandardov

Predhovor

S významom IKT systémov vzrastá aj potreba ich adekvátnej ochrany. Rozsah a zložitosť IKT systémov prakticky vylučuje možnosť individuálneho riešenia informačnej bezpečnosti jednotlivých IKT systémov. Štandardizácia v oblasti informačnej umožňuje prejsť od nesystematického riešenia bezpečnosti (ad-hoc) k systematickému prístupu. Bezpečnostné štandardy sa stávajú dôležitým nástrojom na dosiahnutie potrebnej úrovne informačnej bezpečnosti.

Táto práca vznikla s cieľom vytvoriť základný prehľad o stave štandardizácie v oblasti informačnej bezpečnosti vo svete a na Slovensku. Pri popise stavu boli identifikované niektoré problémy spôsobujúce nedostatočnú úroveň štandardizácie v oblasti informačnej bezpečnosti na Slovensku. V práci navrhujeme možné riešenia niektorých z identifikovaných problémov; zavádzame kategorizáciu štandardov umožňujúcu vytvorenie prehľadu o kandidátoch na zaradenie do sústavy STN. Vychádzajúc z poznatkov získaných počas niekoľkoročného pôsobenia v TK 37 SÚTN navrhujeme možné riešenie užšieho prepojenia štandardizačného a legislatívneho procesu, ktoré umožní využiť odbornú úroveň relevantných štandardov v zákonoch a podzákonných predpisoch.

Súčasťou práce je návrh aplikácie umožňujúcej udržať prehľad o veľkom počte dokumentov štandardizačného charakteru a sledovať proces vývoja štandardov. Špecifikácia slúži ako zadanie záverečnej práce bakalárskeho štúdia informatiky na Fakulte matematiky, fyziky a informatiky Univerzity Komenského.

Výsledky práce boli využité pri práci subkomisie SK 02 TK 37 SÚTN a boli prezentované aj na odbornej konferencii SASIB *Informačná bezpečnosť '08*.

Obsah

Zoznam obrázkov a tabuliek

Zoznam obrázkov

Zoznam tabuliek

1 Úvod

Diplomová práca sa zaoberá problémami štandardizácie v oblasti informačnej bezpečnosti vo svete a na Slovensku. V prvom rade je určená pre čitateľov, ktorí majú dostatočné vedomosti informačnej bezpečnosti a/alebo štandardizácie v tejto oblasti. Nakoľko sa však predpokladá, že k práci sa dostanú aj iní čitatelia, považovali sme za nevyhnutné do jej úvodu (kapitola *2 Základy informačnej bezpečnosti*) zahrnúť aj základné poznatky z oblasti informačnej bezpečnosti.

V kapitole *3 Štandardizácia v oblasti informačnej bezpečnosti* sa práca venuje objasneniu významu informačnej bezpečnosti a štandardizácie v tejto oblasti.

Kapitola *4 Štandardizácia informačnej bezpečnosti vo svete* má za úlohu uviesť čitateľa do problematiky štandardizácie v oblasti informačnej bezpečnosti tým, že uvádza prehľad významných štandardizačných organizácií vo svete a popisuje činnosť troch z nich, ktoré považujeme za najvýznamnejšie.

V rámci kapitoly *5 Štandardizácia v oblasti informačnej bezpečnosti na Slovensku* je analyzovaný stav štandardizácie na Slovensku, sú identifikované jej slabé miesta a navrhnuté riešenia umožňujúce zlepšenie jej stavu.

Jedným z nástrojov použiteľným pri zlepšení stavu štandardizácie v oblasti informačnej bezpečnosti na Slovensku je kategorizácia štandardov (najmä medzinárodných). V kapitole *6 Kategorizácia štandardov v oblasti informačnej bezpečnosti* je definovaná schéma pre kategorizáciu štandardov. Súčasťou diplomovej práce však nie je zaradenie jednotlivých štandardov do kategórií.

Práca vychádza z pomerne veľkého počtu materiálov. Prevažná väčšina z nich bola získaná prostredníctvom verejnej siete Internet. V súčasnosti však neexistujú jednoznačné pravidlá na citovanie online zdrojov. Aby sa pri prípadnom zrušení alebo premiestnení citovanej webovej stránky nestratili nejaké informácie, sú všetky online zdroje uložené v prehľadnej adresárovej štruktúre na CD priloženom k tejto práci.

Na citovanie zdrojov bol použitý nástroj, ktorý je súčasťou aplikácie Microsoft Office Word 2007. Citácie sú vo formáte ISO 690, odkazy na citácie neštandardne používajú okrúhle zátvorky.

Pri písaní práce sme sa stretli s problémom, ktorý navonok pôsobí nenápadne. Je ním rozdiel v chápaní slova štandard (standard) v slovenskom a anglickom jazyku. Zatiaľ čo slovenčina rozlišuje pojmy norma a štandard, v angličtine je pre tieto dva pojmy

používaný výraz standard. V tejto práci sme sa priklonili k terminológii anglického jazyka a tam, kde by to nespôsobilo nejednoznačnosť, sme pre zjednodušenie na označenie noriem použili pojem štandardy.

Špecifickým prípadom v oblasti informačnej bezpečnosti je ochrana utajovaných skutočností (klasifikovaných informácií). Základný rámec pre ochranu utajovaných skutočností v SR tvorí zákon č. 215/2004 Z.z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov a na neho nadväzujúce predpisy (napr. vyhlášky Národného bezpečnostného úradu). Štandardy vyplývajúce z týchto predpisov sú často nedostupné (štandardy NATO), a preto sa nimi v tejto práci nezaoberáme.

Výsledky tejto diplomovej práce boli prezentované na konferencii *Informačná bezpečnosť '08* a sú publikované v zborníku (1).

2 Základy informačnej bezpečnosti

Táto práca je určená najmä pre čitateľov, ktorí majú aspoň základné znalosti v oblasti informačnej bezpečnosti.

Vzhľadom na to, že čitateľom práce však môže byť aj osoba bez potrebných znalostí, v tejto kapitole je uvedené vysvetlenie základných pojmov v tejto oblasti, vychádzajúce z (2) a (3). V prílohe *Príloha A – Slovník pojmov* je následne uvedený stručný výkladový slovník pojmov v oblasti informačnej bezpečnosti, vychádzajúci z (2).

Čitateľom, ktorí majú potrebné vedomosti z informačnej bezpečnosti odporúčame pokračovať v čítaní kapitolou *3 Štandardizácia v oblasti informačnej bezpečnosti*.

2.1 Základné pojmy informačnej bezpečnosti

Informačným a komunikačným systémom (IKT systémom) sa rozumie súhrn technických a programových prostriedkov, ktoré sa využívajú na prenos, spracovanie alebo ukladanie informácií. Časti IKT systému (subsystémy, technické komponenty, programové vybavenie, údaje,...) ako aj ďalšie „netechnické“ entity (ľudia, peniaze, dobré meno, know-how), ktoré je potrebné z bezpečnostného hľadiska uvažovať, sa nazývajú aktívami (assets) IKT systému. V IKT systéme okrem technologických komponentov spravidla pôsobia aj osoby a pre IKT systém sú stanovené pravidlá (písané a nepísané), ktoré upravujú jeho činnosť.

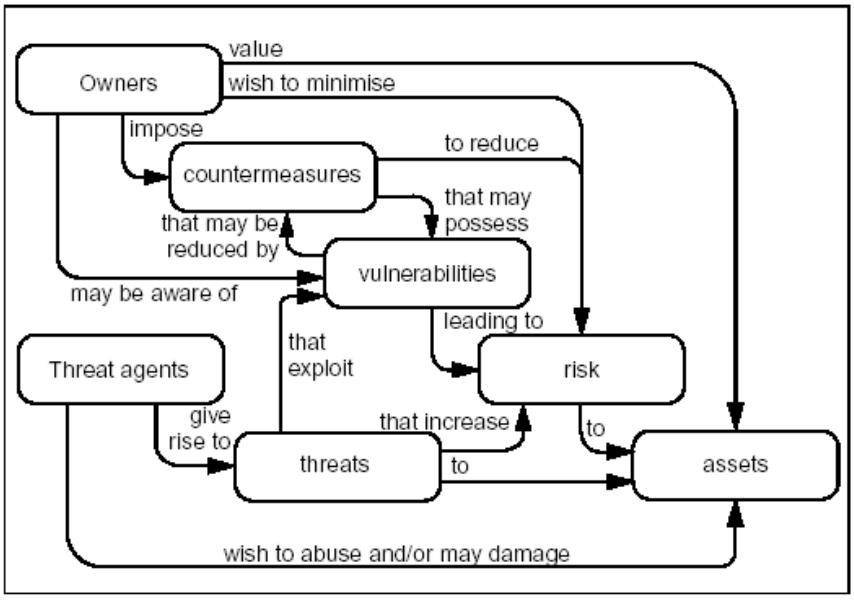
Aj činnosť osôb, pôsobiacich v systéme, je upravená pravidlami. Osoby, konajúce v súlade s pravidlami, sa nazývajú oprávnenými osobami. Oprávnenia osôb na výkon nejakých činností v systéme môžu byť stanovené individuálne. Častejšie, najmä v prípade väčšieho počtu osôb pôsobiacich v systéme, sú však ľudia podľa toho, aké činností potrebujú vykonávať v systéme, rozdelení do kategórií, ktoré sa nazývajú *roly* (napríklad používateľ, správca systému, operátor, audítor). Oprávnenia na činnosť v systéme sa udeľujú na základe rolí a v prípade potreby môžu byť ešte individuálne upravené.

Čokoľvek, čo môže viesť k odchýlke od pravidiel stanovených pre systém, sa nazýva hrozbou. Hrozba je potenciálna možnosť, ktorá existuje nezávisle od IKT systému. Ak nastane situácia, v ktorej sa hrozba uskutoční, hovoríme o naplnení hrozby. Hrozby bývajú orientované na jednotlivé aktíva systému. Hrozbou je napríklad možná krádež počítača, alebo možný prienik do databázy citlivých údajov. Hrozba má svojho nositeľa, t.j. entitu, ktorá je schopná hrozbu uskutočniť. Nositeľmi hrozby môžu byť technické prostriedky, ľudia, ale aj prírodné vplyvy (napr. blesk, záplava a pod.). Hrozby sa môžu realizovať

v dôsledku úmyselnej činnosti ľudí (aj pomocou technických alebo logických prostriedkov), alebo neúmyselne (ľudský omyl, technická chyba, porucha, prírodný vplyv).

Naplnenie hrozby sa nazýva bezpečnostný incident. Pokus o vedomé uskutočnenie hrozby sa nazýva útok. Ten, kto útok uskutočňuje, sa nazýva útočníkom. Na uskutočnenie hrozby je potrebné splnenie nejakých podmienok (napr. získanie prístupu k systému, vedomosti o systéme, čas, motivácia). Vlastnosť, technické riešenie, slabé miesto systému alebo jeho aktíva, ktoré umožňujú realizáciu hrozby, sa nazývajú zraniteľnosťami alebo slabinami systému (vulnerabilities). Podmienky potrebné na úspešný útok na systém sa nazývajú útočným potenciálom. Uskutočnenie hrozby má spravidla nejaké dôsledky pre systém (strata alebo obmedzenie funkčnosti, finančná ujma).

Druhým dôležitým kvantitatívnym parametrom hrozby je pravdepodobnosť toho, že hrozba nastane[1] (že sa naplnia podmienky jej uskutočnenia). Riziko vyplývajúce z hrozby je odvodené od pravdepodobnosti naplnenia hrozby a dôsledkov hrozby. Aktivity alebo prostriedky smerujúce k eliminácii rizík v IKT systéme, alebo aspoň ich zníženiu na únosnú mieru sa nazývajú bezpečnostné opatrenia. Vzťahy medzi základnými pojmami informačnej bezpečnosti sú uvedené na nasledujúcom obrázku, ktorý pochádza zo štandardu Common Criteria verzie 2.3. (4).



Obrázok 1: Vzťahy medzi základnými pojmami informačnej bezpečnosti

Cieľom ochrany IKT systému je zabezpečiť jeho bezproblémové fungovanie, t.j. vylúčiť výskyt bezpečnostných incidentov alebo aspoň znížiť bezpečnostné riziká voči systému. To znamená, že pri popise systému je potrebné identifikovať hrozby voči jeho jednotlivým

[1] Pád lietadla na budovu, v ktorej je umiestnený systém môže znamenať úplné zničenie systému. Pravdepodobnosť takejto udalosti je však veľmi malá.

položkám, vyčísliť ich závažnosť (ohodnotenie, resp. analýza rizík), navrhnúť a zaviesť bezpečnostné opatrenia.

Bezpečnostná politika (systému/produktu/funkcie) je súbor pravidiel, ktoré určujú, ako sú položky spravované a chránené. Model bezpečnostnej politiky je štruktúrovaná reprezentácia bezpečnostnej politiky. Bezpečnostná funkcia systému/produktu je časť systému/produktu, ktorá zabezpečuje dodržiavanie niektorej časti bezpečnostnej politiky. Bezpečnostný mechanizmus je konkrétny prostriedok (algoritmus, technické zariadenie) realizujúci bezpečnostnú funkciu.

2.2 Základné aspekty ochrany informácií

Aj keď sme doteraz hovorili o bezpečnosti IKT systémov, treba zdôrazniť, že podstatná je ochrana ich informačného obsahu, t.j. informácie, ktorá sa v nich spracováva, uchováva, alebo prenáša. Pre rôzne typy informácií existujú rôzne požiadavky na ich ochranu. Niektoré informácie je potrebné chrániť pred ich získaním neoprávneným subjektom, iné môžu byť verejné, ale je potrebné chrániť ich pred neoprávnenou modifikáciou. Nedostupnosť informácií pre oprávnený subjekt vtedy, keď ich potrebuje, môže tiež predstavovať vážnu hrozbu. Jednotlivé aspekty ochrany informácií sa navzájom ovplyvňujú a predstavujú určité obmedzenia na prostriedky ochrany. Napríklad ak je určité informácie potrebné chrániť pred prístupom neoprávneného subjektu, ale nie je dôležitá dostupnosť týchto informácií, tak ich môžeme uložiť napríklad v izolovanom počítači uloženom v dobre fyzicky chránenom trezore, resp. na inom bezpečnom mieste. Riziko úniku informácií v takomto prípade je určite menšie, ako keď sú informácie uložené v počítači, ktorý je priamo dostupný z Internetu, poskytuje rôzne sieťové služby a umožňuje aj vzdialený prístup k chráneným informáciám. Na druhej strane je dostupnosť informácií komplikovaná potrebou fyzického prístupu. V praxi sa zvyčajne stretávame s kombinovanými požiadavkami na ochranu informácií, preto pri hľadaní vhodného riešenia je potrebné nájsť rozumný kompromis medzi rôznymi požiadavkami.

Základné aspekty ochrany informácií môžeme rozdeliť do niekoľkých kategórií:

- dôvernosť (confidentiality),
- integrita (integrity),
- dostupnosť (availability),
- autentickosť (authenticity),
- sledovateľnosť (accountability),
- ochrana súkromnosti informácie (privacy).

V nasledujúcich častiach práce podrobnejšie popíšeme jednotlivé aspekty ochrany informácií.

2.2.1 Dôvernosť

V informačných systémoch sa často uchovávajú a spracúvajú informácie, ktoré sú dôverného charakteru, t.j. informácie, ktoré majú byť z informačného systému schopné získať len oprávnené subjekty. Cieľom ochrany dôvernosti je zabezpečiť, aby dôverné informácie nemohol získať neoprávnený subjekt.

Ochrana dôvernosti zahŕňa ochranu dôvernosti uložených informácií, ako aj informácií počas prenosu (napr. počítačovou sieťou). Dôvernosť uložených informácií sa dá chrániť dvoma základnými spôsobmi – riadením prístupu a šifrovaním. Riadenie prístupu môže ochrániť dôvernosť informácií len proti neoprávnenému prístupu prostriedkami systému, ktorý riadenie prístupu implementuje, šifrovanie môže ochrániť dôvernosť uložených alebo prenášaných informácií aj proti prístupu inými prostriedkami (napr. priamym prístupom k pamäťovému médiu, na ktorom sú uložené dôverné informácie, odpočúvaním komunikačných liniek).

2.2.2 Integrita

Následkom technických chýb, rušivých vplyvov prostredia, ale napr. aj úmyselnej činnosti útočníkov môže dôjsť k neoprávnenej alebo neúmyselnej zmene uložených alebo prenášaných informácií. Cieľom ochrany integrity je zamedziť takejto zmene alebo umožniť dostatočne spoľahlivo zistiť, že k nežiaducej zmene došlo.

Jedným z prostriedkov ochrany integrity je riadenie prístupu, ktoré môže brániť neoprávneným zmenám informácií prostriedkami systému, ktorý riadenie prístupu implementuje. Vo všeobecnosti však nie je možné zabrániť nežiaducej modifikácii informácií následkom technických chýb alebo vplyvu prostredia.

Taktiež často potrebujeme chrániť integritu informácií aj proti manipulácii obchádzajúcej prostriedky systému alebo integritu informácií prenášaných komunikačnými kanálmi mimo systému. V týchto prípadoch je možné použiť známe techniky umožňujúce zistiť, že informácia bola zmenená. Sú to predovšetkým hašovacie funkcie, hašovacie funkcie s tajným kľúčom a digitálne podpisy. Pomocou hašovacej funkcie sa z informácie vypočíta hašovacia hodnota, ktorá sa pripojí k informácii alebo sa uloží, resp. prenesie nezávisle na nej. Pri kontrole integrity sa opäť vypočíta hašovacia hodnota a porovná sa s uloženou alebo prenesenou hašovacou hodnotou. Ak sa informácia (alebo hašovacia hodnota) nezmenila, musia sa obe hašovacie hodnoty rovnať, ak sa zmenila, s veľkou pravdepodobnosťou sa rovnať nebudú.

Ak má byť takáto ochrana integrity účinná proti úmyselnej modifikácii útočníkom, musí byť pôvodná hašovacia hodnota uložená alebo prenesená tak, aby ju útočník nemohol nahradiť hašovacou hodnotou zmenenej informácie. Vhodným riešením účinným aj proti úmyselnej modifikácii je použitie hašovacej funkcie s tajným kľúčom alebo digitálneho podpisu. V súvislosti s ochranou integrity je potrebné spomenúť ešte samoopravné kódy, ktoré umožňujú detekovať a opraviť určitý (malý) počet chybných bitov v prenesenej alebo uloženej informácii. Tiež predstavujú spôsob ochrany integrity pred neúmyselnou modifikáciou informácie následkom technických chýb alebo vplyvu prostredia. Ich výhodou je schopnosť opravovať malé (a časté) chyby, no pri chybe väčšieho rozsahu svoju účinnosť strácajú. Nie sú použiteľné na ochranu správ proti úmyselnej modifikácii, pretože kontrolujú syntaktickú správnosť správ a pri úmyselnej modifikácii nie je problém zmeniť sémantiku tak, aby zostala syntax správy správna.

2.2.3 Dostupnosť

Častou a dôležitou požiadavkou na ochranu informácií je požiadavka na dostupnosť. IKT systém musí byť schopný poskytnúť oprávneným subjektom informácie vtedy, keď ich potrebujú. Informácie sa môžu stať nedostupnými napr. následkom úmyselnej činnosti útočníka, následkom technického zlyhania (napr. nefunkčný pevný disk, výpadok komunikačnej infraštruktúry, výpadok napájania) alebo aj následkom živelnej pohromy. Niektoré výpadky dostupnosti môžu byť dočasné (napr. výpadok komunikácie), iné môžu byť trvalé (zničenie médií, kde boli informácie uložené). Súčasťou požiadaviek na dostupnosť môže byť určenie maximálneho času, dokedy musia byť informácie poskytnuté, alebo určenie rozsahu výpadku, ktorý musí byť systém schopný tolerovať bez obmedzenia dostupnosti.

Dostupnosť sa zvyčajne zabezpečuje redundanciou zdrojov (alternatívne komunikačné kanály, redundantné diskové polia, záložné prostriedky na spracovanie informácií, ...), zálohovaním a archiváciou údajov.

2.2.4 Autentickosť

Aby bolo možné informácie považovať za záväzné (a na ich základe konať), je potrebné popri ochrane integrity zabezpečiť možnosť spoľahlivého určenia ich pôvodu. Informácia je autentická práve vtedy, ak je nezmenená a pochádza od toho, o kom to predpokladáme.

V prípade, že potrebujeme chrániť autentickosť informácie len proti narušeniu prostriedkami informačného systému, ktorý ju spracováva, je možné využiť mechanizmy riadenia prístupu. Systém musí spolu s informáciou uložiť a prezentovať aj spoľahlivo overenú identifikáciu subjektu, ktorý informáciu zadal alebo potvrdil (ďalej pôvodca). Ak

má byť subjekt, ktorý na základe takejto informácie koná, schopný preukázať, že konal na základe autentickej informácie, musí navyše systém zabrániť zmene uloženej informácie akýmkoľvek subjektom vrátane jej pôvodcu.

Univerzálnym prostriedkom ochrany autentickosti, ktorý navyše umožňuje overenie autentickosti nezávisle na informačnom systéme, ktorý ju spracováva, je digitálny podpis založený na princípoch asymetrickej kryptografie – pomocou súkromného kľúča pôvodcu (známeho len pôvodcovi) sa pri podpisovaní informáciu vypočíta digitálny podpis, ktorý sa dá následne overiť pomocou verejného kľúča pôvodcu (známeho overovateľovi). Ak sa zabezpečí väzba medzi identifikáciou pôvodcu a jeho verejným kľúčom, digitálny podpis umožňuje dokázať, že informácia je autentická, pretože digitálny podpis závisí na obsahu informácie a na jeho výpočet je potrebný súkromný kľuč pôvodcu.

2.2.5 Sledovateľnosť

Dôležitou požiadavkou na ochranu informácií je možnosť zistiť, ktorý subjekt vykonal bezpečnostne relevantné činnosti – napr. vložil, zmenil, zmazal alebo čítal určitú informáciu. Ak existuje viac subjektov, ktoré sú oprávnené určité činnosti vykonať, je sledovateľnosť potrebná na určenie zodpovednosti v prípade, že bola vykonaná činnosť v rozpore s pravidlami, ktorých dodržiavanie IKT systém nemôže kontrolovať.

2.2.6 Ochrana súkromnosti informácie

V IKT systémoch sa spracovávajú aj informácie, ktorých podstata nie je dôverná, ale v súvislosti s osobou, ktorej sa týkajú, dôverné sú. Príkladom sú zdravotné záznamy. Pokiaľ nie je možné zdravotné záznamy spojiť s osobou, ktorej sa týkajú, predstavujú len informáciu typu „Existuje osoba, ktorá mala takéto zdravotné problémy, použila sa takáto liečba s takýmito výsledkami.“. Takáto informácia nemusí byť považovaná za dôvernú. Ak sa k nej pridá informácia o identite pacienta, už sa dôvernou stane, ak sa ju nerozhodne spraviť verejnou pacient, ktorého sa týka.

Takáto informácia preto musí byť chránená spôsobom, ktorý umožní prístup k informácii bez častí predstavujúcich spojenie s konkrétnou osobou širšiemu okruhu subjektov a umožní prístup ku kompletnej informácii len užšiemu okruhu oprávnených subjektov.

3 Štandardizácia v oblasti informačnej bezpečnosti

Cieľom tejto kapitoly je pomôcť čitateľovi pochopiť význam štandardizácie v oblasti informačnej bezpečnosti, a poskytnúť stručný prehľad o histórii štandardizácie vo svete. Tieto informácie môžu byť neskôr užitočné pri analýze stavu štandardizácie v oblasti informačnej bezpečnosti na Slovensku a návrhu odporúčaní na jeho zlepšenie.

V časti *3.1 História a význam informačnej bezpečnosti* si v historickom kontexte uvedieme dôvody, ktoré podnietili jednotlivé organizácie k štandardizácii informačnej bezpečnosti. Časť *3.2 Možné prístupy k riešeniu informačnej bezpečnosti* analyzuje možné prístupy k riešeniu informačnej bezpečnosti v organizáciách a zdôvodňuje potrebu štandardizovaného prístupu. V časti *3.3 História štandardizácie v informačnej bezpečnosti* sú popísané najvýznamnejšie míľniky histórie štandardizácie v kľúčových oblastiach informačnej bezpečnosti.

3.1 História a význam informačnej bezpečnosti

História informačnej bezpečnosti siaha ďaleko do minulosti. Keď ľudia navzájom komunikovali o závažných otázkach, často potrebovali, aby sa k informáciám nedostali nepovolané osoby; keď sa rozhodovali, potrebovali aktuálne a spoľahlivé informácie o probléme, ktorý mali riešiť a keď prijímali nejaké záväzky, snažili sa zdokumentovať ich obsah tak, aby sa nedal zmeniť. Hoci si to explicitne možno neuvedomovali, usilovali sa zaistiť dôvernosť, dostupnosť, integritu a autentickosť informácie. Najprv boli explicitne formulované požiadavky na ochranu dôvernosti. Podľa Davida Kahna (5) sa história vedy o šifrovaní, kryptológie, začala písať približne pred 4000 rokmi v Starom Egypte. Hoci si význam ochrany informácií panovníci, vojaci, diplomati aj obchodníci v priebehu ďalších tisícročí dobre uvedomovali, kryptológia sa začala významnejšie rozvíjať až počas 2. svetovej vojny (5).

S rozvojom elektronických informačných a komunikačných technológií (IKT) sa do popredia dostávajú aj ďalšie bezpečnostné atribúty informácie a pod bezpečnosťou informácií sa rozumie najmä zaistenie ich dôvernosti, dostupnosti a integrity. Súčasné definície informačnej bezpečnosti (napr. v (6)) túto trojicu dopĺňajú o ďalšie bezpečnostné atribúty informácie, ako napr. autentickosť (authenticity), sledovateľnosť (accountability), vylúčenie popretia zodpovednosti (non-repudiation), spoľahlivosť (reliability), ochrana súkromnosti informácie (privacy) a ďalšie. Okrem chápania informačnej bezpečnosti ako stavu nejakého informačného a komunikačného systému, v ktorom je zaistená primeraná ochrana technických zariadení, jeho programového vybavenia a informačného obsahu, sa

informačná bezpečnosť chápe ako medziodborová disciplína, ktorej úlohou je skúmanie hrozieb voči IKT a vývoj prostriedkov na ich ochranu. Vývoj informačnej bezpečnosti ako disciplíny bol do značnej miery ovplyvnený vývojom IKT. Je potrebné uvedomiť si tento historický kontext, pretože až do súčasnosti sa zachovali niektoré princípy a riešenia, ktoré sa viažu na dávno prekonané technológie. V tejto časti dokumentu je uvedený stručný prehľad vývoja informačnej bezpečnosti v kontexte technologického vývoja počítačov, sietí a neskôr IKT.

Prvé počítače (obdobie 1950-1975) boli umiestnené v špeciálne vybudovaných sálach s klimatizáciou a dvojitou podlahou. Ich obsluhu zabezpečoval kvalifikovaný personál a používatelia k nim nemali priamy prístup. Údaje a programy boli zväčša uložené na diernych štítkoch alebo magnetických páskach. Na zaistenie ochrany postačovalo zavedenie fyzických, personálnych a organizačných opatrení. Využívali sa pri tom aj skúsenosti z vojenského prostredia. V takýchto podmienkach bolo úmyselných útokov na bezpečnosť systémov relatívne málo, prevažovali narušenia bezpečnosti spôsobené chybou techniky alebo ľudského faktora.

S cieľom zefektívnenia využitia relatívne nákladných zariadení sa zaviedlo do praxe používanie vzdialeného prístupu. Spočiatku bol vzdialený prístup realizovaný prostredníctvom terminálov, neskôr pomocou lokálnych počítačových sietí. Zefektívnenie využitia počítačov však prinieslo nové hrozby voči bezpečnosti informácií, súvisiace najmä s prístupom neoprávnených osôb k systémom. Dovtedy používané prostriedky ochrany (fyzická bezpečnosť) na riešenie týchto problémov nepostačovali.

Rozvoj telekomunikácií umožnil prepojenie počítačov na veľké vzdialenosti prostredníctvom modemov. Jednými z prvých typov verejných služieb boli tzv. bulletin board service (BBS), umožňujúce výmenu súborov prostredníctvom modemu a tým aj vytvorenie prvých diskusných fór, medzi ktorými, paradoxne, boli aj fóra zamerané na slabiny vtedajších IKT systémov.

Na rozhraní 80. a 90. rokov významne zmenil situáciu príchod Internetu, ktorý umožnil rozvoj hackerstva. Spočiatku si hackeri napádaním systémov dokazovali svoju odbornú zdatnosť. Neskôr, s rozvojom významnejšieho využitia informačných technológií, boli tieto motívy nahradené ekonomickými cieľmi. Významnou hrozbou do budúcnosti je tiež svetový terorizmus.

Zložitosť zariadení a ich programového vybavenia zvyšuje pravdepodobnosť neúmyselnej chyby, ktorú je možné využiť na úspešný útok na systém. V správe BSI o stave informačnej bezpečnosti v Nemecku (7) v roku 2007 sa uvádza, že v roku 2006 bolo objavených vyše

7000 bezpečnostných slabín v IKT systémoch a vyše polovica z nich umožňovala získanie prístupu s používateľskými alebo administrátorskými oprávneniami. Čas od odhalenia bezpečnostnej slabiny po jej zverejnenie sa v priebehu 2 rokov skrátil v priemere zo 6,5 dňa na 3 dni a 44% odhalených slabín bolo zverejnených spolu s návodom ako ich využiť.

S nástupom nových technológií, ako sú VoIP (telefonovanie cez Internet), bezdrôtové siete, mobilná komunikácia, aktívny obsah webových stránok, RFID (rádiofrekvenčná identifikácia), SCADA (riadenie technologických systémov), sa objavujú aj nové bezpečnostné hrozby, ktoré treba zavčasu riešiť.

Dnes sa prostredníctvom IKT riadia aj fyzické objekty ako sú vlaky, výrobné linky, reaktory alebo radary. Z dôvodu nárastu množstva spracúvaných informácií nie je možný návrat k manuálnemu spracúvaniu informácií. Narušenie informačnej bezpečnosti, či už v dôsledku technickej chyby, ľudského omylu alebo úmyselného útoku na systémy, môže mať rozsiahle dopady, počnúc ekonomickými stratami (narušenie výroby, poskytnutie konkurenčnej výhody, poškodenie zariadení), končiac ohrozením zdravia a života osôb. Preto je nutným predpokladom fungovania spoločnosti, ktorá dosiahla vysokú úroveň informatizácie, zaistenie informačnej bezpečnosti (8)(9).

3.2 Možné prístupy k riešeniu informačnej bezpečnosti

Zaistenie informačnej bezpečnosti nejakého IKT systému, alebo celej organizácie je možné principiálne riešiť dvojako: ad-hoc (nesystematicky) a systematicky. Nesystematický prístup, zaužívaný ešte aj v súčasnosti v mnohých organizáciách, sa zameriava na ad-hoc riešenie bezpečnostných problémov, ktoré sa v rámci organizácie vyskytli. „Výhodou“ tohto prístupu je, že sa riešia naozajstné problémy a tak netreba nikoho presviedčať o potrebe prijímania bezpečnostných opatrení. Očividnou nevýhodou je, že sa opakovane riešia tie isté problémy a nič nezaručuje, že sa tieto alebo iné bezpečnostné problémy neobjavia v budúcnosti a ich dopad neprekročí náklady na systematické riešenie informačnej bezpečnosti. Napriek nákladnosti, zložitosti, technickej a organizačnej náročnosti je informačnú bezpečnosť v praxi vhodnejšie riešiť systematicky a štandardizovane. Oproti ad-hoc riešeniam majú štandardizované riešenia mnohé výhody, medzi ktoré nesporne patri opakovateľnosť, kompatibilita, väčšia miera úplnosti a nižšie riziko chýb pri implementácii, čo v konečnom dôsledku znamená úsporu nákladov.

Pre základné bezpečnostné problémy dnes existujú cenovo dostupné technologické riešenia. Istým rizikom masového nasadenia niektorého z bezpečnostných riešení je možnosť prehliadnutia chyby pri jeho tvorbe a následného zneužitia tejto chyby útočníkmi.

Okrem konkrétnych bezpečnostných riešení existujú aj všeobecnejšie riešenia obsiahnuté v bezpečnostných štandardoch. Tieto štandardy predstavujú koncentrované poznanie v danej oblasti a sú významným nástrojom na dosiahnutie medzinárodnej kompatibility riešení a potrebnej úrovne informačnej bezpečnosti.

3.3 História štandardizácie v informačnej bezpečnosti

Za prvé bezpečnostné štandardy možno považovať štandardy upravujúce napr. formáty údajov, komunikačné protokoly a ďalšie náležitosti, bez ktorých by nebola možná kompatibilita a interoperabilita rozličných IKT systémov a teda ani dostupnosť údajov a služieb, ktoré tieto IKT systémy poskytovali. Dostupnosť sa však v minulosti nevnímala (a v praxi sa často nevníma ani dnes) ako bezpečnostná požiadavka, ale skôr ako základná požiadavka funkčnosti systému. Prvou skutočne bezpečnostnou požiadavkou, ktorej riešenia sa stali predmetom štandardizácie, je dôvernosť. Stručný prehľad histórie štandardizácie pre túto oblasť sa nachádza v časti *3.3.1 Kryptografické štandardy*.

Kryptológia tvorí jadro informačnej bezpečnosti, pretože mnohé bezpečnostné riešenia sa opierajú o kryptografické funkcie (šifrovanie, hašovacie funkcie, digitálny podpis a i.). Napriek tomu ale samotná kryptológia na zaistenie informačnej bezpečnosti nepostačuje, keďže mnohé hrozby voči IKT systémom sú spojené s implementáciou bezpečnostných riešení a prevádzkou IKT systémov. To viedlo k nutnosti posudzovania informačnej bezpečnosti IKT systému ako celku, v rámci čoho je zohľadnený aj vplyv prostredia, v ktorom je IKT systém prevádzkovaný. Napriek jedinečnosti IKT systémov sa aj tu uplatnila taká kategorizácia/klasifikácia systémov, ktorá umožnila štandardizáciu požiadaviek na ich ochranu a stanovenie potrebnej úrovne ich ochrany. História štandardizácie v oblasti ohodnotenia bezpečnosti IKT systémov je popísaná v časti *3.3.2 Ohodnocovanie bezpečnosti IKT systémov*.

V praxi sa však ukázalo, že samotné technologické zabezpečenie bezpečnosti informácií (ich spracúvaním v bezpečných systémoch a bezpečným ukladaním/prenosom) nie je postačujúce. Informačnú bezpečnosť (jej zavádzanie a aplikáciu v každodennej praxi) je potrebné systematicky riadiť. Pre túto oblasť v 90 rokoch vznikla samostatná vetva štandardov, ktorej história je popísaná v časti *3.3.3 Štandardy pre riadenie informačnej bezpečnosti*.

3.3.1 Kryptografické štandardy

Ako už bolo spomenuté v úvodných častiach, použitie kryptografie je nevyhnutné pre aplikáciu viacerých bezpečnostných funkcií. Je preto prirodzené, že štandardizácia neobišla ani kryptografiu, najmä ak uvážime, že algoritmy, protokoly a iné kryptografické

primitíva sa spravidla dajú popísať matematicky a vyznačujú sa parametrami, ktorých hodnoty sa dajú presne špecifikovať. Priekopníkom v oblasti štandardizácie kryptografických riešení je nepochybne americký National Institute of Standards and Technology (NIST). Vďaka zákonu *Brooks Act* z roku 1965 sa NIST (vtedy ešte pod názvom National Bureau of Standards) stal inštitúciou zodpovednou za vývoj federálnych noriem upravujúcich používanie výpočtovej techniky. NIST vydal rad noriem FIPS PUB (Federal Information Processing Standard Publications) pokrývajúcich všetky oblasti IKT, vrátane informačnej bezpečnosti. NIST sa vo svojej činnosti v oblasti informačnej bezpečnosti zameriaval na dva základné smery – normy pre počítačovú kryptografiu a normy pre vytváranie a hodnotenie IKT systémov. Viaceré z kryptografických noriem, ktoré NIST vydal, presiahli významom rámec Spojených štátov. Medzi také normy patria FIPS PUB 46 *Data Encryption Standard* a jeho nasledovník FIPS PUB 197 *Advanced Encryption Standard*, definujúce blokové šifrovacie algoritmy, FIPS PUB 180-3 S*ecure Hash Standard*, či FIPS 186-2 *Digital Signature Standard*. Medzinárodne známou normou je FIPS 140 (1,2,3) špecifikujúcou podrobné bezpečnostné požiadavky na kryptografické moduly. Štandardizácia v oblasti kryptografie predstavuje významnú oblasť činnosti ISO/IEC JTC 1 (činnosť štandardizačnej komisie ISO/IEC JTC 1 je popísaná v kapitole *4.1 Spoločná technická komisia ISO a IEC (ISO/IEC JTC 1)*). Štandardizačné úsilie ISO/IEC v oblasti kryptografie sa zameriava na kryptografické algoritmy (symetrické a asymetrické šifry, hašovacie funkcie, generátory náhodných čísel, generátory prvočísel), kryptografické primitíva založené na eliptických krivkách, ako aj na aplikačné otázky (digitálne podpisy, časové pečiatky, distribúciu kryptografických kľúčov a i.).

Popri šifrovaní je najvýznamnejšou bezpečnostnou funkciou, zabezpečujúcou autentickosť (a zároveň integritu) dokumentu založenou na kryptografických primitívach digitálny podpis. Jeho praktické využitie (napríklad v elektronickom obchode, alebo v systémoch e-Government-u) si vyžaduje vytvorenie tzv. infraštruktúry verejných kľúčov (public key infrastructure, PKI), ktorá umožňuje spoľahlivú distribúciu verejných kľúčov pomocou certifikátov verejných kľúčov, a overovanie elektronických podpisov, vydávanie časových pečiatok a ďalšie činnosti. Hoci národné (NIST) aj medzinárodné (ISO/IEC) štandardizačné organizácie vydali rad štandardov upravujúcich vytváranie a používanie digitálnych podpisov a časových pečiatok, najrozšírenejšími štandardami sú:

- X.509 vydané organizáciou ITU Telecommunication Standardization Sector (ITU-T),
- PKCS, ktoré spravuje súkromná organizácia RSA Laboratories (10).

Európska únia vydala Direktívu o elektronickom podpise (11) a vytvorila pracovnú skupinu EESSI (European Electronic signature standardization initiative), ktorá v období 1999-2004 spracovala niekoľko štandardizačných dokumentov o formátoch elektronických podpisov, vytváraní a overovaní elektronických podpisov, požiadavkách na zariadenia na vytváranie a overovanie elektronických podpisov, ktoré po ukončení činnosti EESSI prešli do správy ETSI (European Telecommunications Standards Institute).

Okrem štandardov vydaných oficiálnymi štandardizačnými organizáciami existujú aj de-facto štandardy spracované odbornými organizáciami. Medzi najvplyvnejšie patrí The Internet Engineering Task Force (IETF), zverejňujúca tzv. Request for comments (RFC) predstavujúce často predbežné verzie budúcich štandardov, predložené na verejnú diskusiu. Zoznam RFC, ako aj znenie jednotlivých dokumentov, je voľne dostupný prostredníctvom Internetu. (12)

3.3.2 Ohodnocovanie bezpečnosti IKT systémov

Ohodnocovanie bezpečnosti IKT systémov v USA

Za jeden z prvých dokumentov, ktorý začal éru štandardizácie v informačnej bezpečnosti sa považuje štandard *Trusted Computer System Evaluation Criteria (TCSEC)*. V roku 1983 ho vytvorila americká Národná bezpečnostná agentúra (National security agency, NSA), pričom bol zaradený medzi publikácie amerického ministerstva obrany (US Department of Defense, DOD). Štandard sa používal najmä na ohodnotenie a výber IKT systémov určených na spracúvanie citlivých informácií v prostredí ozbrojených síl USA.

TCSEC rozdeľuje systémy do kategórií a pre každú kategóriu určuje minimálnu množinu implementovaných bezpečnostných požiadaviek:

A – overená ochrana Zahŕňa systémy ktorých dizajn bol formálne verifikovaný. Definuje podtriedy A1 (funkčne zhodné s B3) a A1+.

B – povinná ochrana Zahŕňa systémy s pokročilými bezpečnostnými funkciami. Systémy v tejto triede musia používať bezpečnostné značky vo všetkých významných dátových štruktúrach. Definuje podtriedy B1, B2 a B3.

C – voliteľná ochrana Zahŕňa systémy umožňuje základné bezpečnostné nastavenia, najmä z hľadiska riadenia prístupu k zdrojom a vytvárania auditných záznamov. Definuje podtriedy C1 a C2.

D – minimálna ochrana Zahŕňa systémy, ktoré boli ohodnotené, ale nevyhoveli podmienkam pre zaradenie do vyššej skupiny

Štandard *Trusted Computer System Evaluation Criteria* vyšiel v knižnej forme, v oranžovej papierovej väzbe. Z toho dôvodu je často označovaný aj ako Oranžová kniha – Orange book. V priebehu rokov 1983 až 1993 postupne vychádzali ďalšie publikácie (štandardy, odporúčania, ...), ktoré súviseli s ohodnocovaním IKT systémov pre DOD a nadväzovali na TCSEC. Spolu bolo takto vydaných viac ako 30 publikácií. Takmer každá z nich mala kvôli rozlíšeniu obálku inej farby, z toho dôvodu sa táto séria publikácií často označuje aj ako dúhová séria – rainbow series. V priebehu 90. rokov 20. storočia začal postupný prechod na využívanie modernejšieho štandardu Common Criteria ktorý obsahovo vychádzal aj z Rainbow series. Štandardu Common Criteria sa budeme venovať v jednej z nasledujúcich častí.

Ohodnocovanie bezpečnosti IKT systémov v Európe a Kanade

V roku 1990 Francúzsko, Nemecko, Holandsko a Veľká Británia vydali na základe dovtedajších skúseností v oblasti ohodnocovania bezpečnosti IKT systémov vo svojich krajinách spoločný štandard *Information Technology Security Evaluation Criteria* (ITSEC) (13). Štandard sa dostal do praxe v 2. polovici roku 1991 po dôslednom medzinárodnom pripomienkovaní.

Podobne ako TCSEC, aj ITSEC definoval štruktúrovanú sadu bezpečnostných požiadaviek na jednotlivé produkty. Jednotlivé systémy boli podľa štandardu zaraďované do tried bezpečnosti E0 až E6, pričom tieto triedy boli navrhnuté tak, aby boli kompatibilné s triedami štandardu TCSEC. Na rozdiel od štandardu TCSEC, v ktorom je na certifikáciu pre nejakú kategóriu nevyhnutné splniť všetky požiadavky stanovené štandardom (vrátane tých neaplikovateľných alebo zbytočných), štandard ITSEC umožňuje istú mieru flexibility. Relevantné požiadavky na bezpečnosť sú dokumentované v rámci bezpečnostného zámeru (security target), ktorý je ohodnocovaný ešte pred ohodnotením samotného systému, pri ohodnocovaní systému sa overuje len splnenie bezpečnostných požiadaviek uvedených v bezpečnostnom zámere.

Certifikácie podľa štandardu ITSEC boli akceptované mnohými ďalšími európskymi krajinami.

Štandard s podobným zameraním bol zavedený taktiež v Kanade. V roku 1993 vydal Communications Security Establishment štandard *Canadian Trusted Computer Product Evaluation Criteria* (CTCPEC). V tomto štandarde boli skombinované prístupy použité v TCSEC a ITSEC.

Podobne ako TCSEC, aj ITSEC a CTCPEC boli/sú v praxi postupne nahrádzané štandardom Common Criteria.

Common Criteria

Aby výrobcovia produktov, ktorých klientmi boli aj vládne subjekty jednotlivých krajín nemuseli zabezpečovať certifikáciu podľa troch štandardov, štandardy TCSEC, ITSEC a CTCPEC boli zjednotené do jediného štandardu – Common Criteria. Prvá verzia spoločného štandardu bola vydaná v roku 1994. Štandard pozostáva z troch častí a je k dispozícii bezplatne prostredníctvom Internetu (14).

Common Criteria boli postupne dopĺňané a v roku 1999 boli prevzaté štandardizačnou organizáciou ISO v troch samostatných dokumentoch (ISO/IEC 15408-1:1999, ISO/IEC 15408-2:1999, ISO/IEC 15408-3:1999). Ďalšia aktualizácia noriem ISO/IEC 15408 prebehla v roku 2005, v súčasnosti príslušná štandardizačná komisia spracúva tretiu verziu štandardu.

Common Criteria definujú množinu bezpečnostných požiadaviek, z ktorých si tvorca produktu vyberá tie, ktoré sú primerané účelu použitia produktu. Požiadavky sú dvojakého charakteru: funkčné požiadavky (functional requirements) a požiadavky na bezpečnostné záruky (assurance requirements).

Bezpečnostné požiadavky sú delené do niekoľkých tried (funkčné požiadavky – 11 tried, požiadavky na záruky – 8 tried)[2]. V rámci každej triedy sú požiadavky ďalej delené do rodín (families)[3] zložených z komponentov (components)[4]. Pre každý komponent sú definované konkrétne požiadavky a/alebo závislosti na iných požiadavkách.

Štandard taktiež definuje 7 úrovní systémov podľa bezpečnostných záruk, ktoré poskytujú. Triedy sú označované EAL1 až EAL7 a zoznam požiadaviek na bezpečnostné záruky je určený výberom bezpečnostných komponentov.

Common Criteria umožňujú pred začatím implementácie systému stanoviť takmer ľubovoľnú kombináciu bezpečnostných požiadaviek. Niektoré schválené kombinácie bezpečnostných požiadaviek sú k dispozícii v podobe tzv. bezpečnostných profilov (protection profile) (15). V rámci tvorby produktu sú bezpečnostné požiadavky rozpracované do podoby bezpečnostného zámeru (security target) – bezpečnostných potrieb konkrétneho systému, prispôsobených jeho charakteristikám a spôsobu jeho implementácie.

[2] Napr. FMT Security management (Manažment bezpečnosti)

[3] Napr. FMT_MSA Management of security attributes (Manažment bezpečnostných atribútov)

[4] Napr. FMT_MSA.1 Management of security attributes allows authorised users (roles) to manage the specified security attributes. (Manažment bezpečnostných atribútov umožňuje oprávneným používateľom /roliam/ spravovať určené bezpečnostné atribúty.)

Aby sa zaistila spätná kompatibilita so štandardmi, ktoré Common Criteria v praxi nahrádzajú, boli vytvorené a schválené bezpečnostné profily, ktoré kladú na systém požiadavky ekvivalentné s požiadavkami niektorých z tried bezpečnosti podľa štandardu TCSEC. Príkladom je bezpečnostný profil Controlled Access Protection Profile, ktorý je ekvivalentom triedy TCSEC C2.

3.3.3 Štandardy pre riadenie informačnej bezpečnosti

Popri tvorbe štandardov pre ohodnotenie bezpečnosti systémov bolo druhou úlohou britského Commercial Computer Security Centre vytvorenie dokumentu, ktorý by zhŕňal odporúčané postupy pre zaistenie bezpečnej prevádzky IKT systémov. Táto snaha vyústila do dokumentu „Users Code of Practice" publikovaného v roku 1989. Jeho ďalšieho vývoja sa ujalo Národné výpočtové centrum (National Computing Centre) v spolupráci s konzorciom britských priemyselných organizácií. Výsledok ich práce bol po verejnej diskusii schválený ako štandard BS 7799:1995 *A code of practice for information security management* britskej štandardizačnej organizácie BSI.

Tento štandard bol ďalej neúspešne navrhnutý na zaradenie do sústavy medzinárodných štandardov ISO. Po aktualizácii v roku 1999 bol štandard ponúknutý opäť a po absolvovaní zrýchlenej schvaľovacej procedúry bol zaradený do sústavy medzinárodných noriem pod označením ISO/IEC 17799:2000.

Nedostatkom tohto štandardu však bol fakt, že podľa nej nebolo možné posudzovať bezpečnosť systémov a organizácií. Preto v roku 1999 vznikol druhý štandard, BS 7799-2:1999, ktorý zaviedol pojem „systém manažérstva informačnej bezpečnosti" (Information security management system, skrátene ISMS) a umožnil certifikáciu riadenia informačnej bezpečnosti pre celú organizáciu, vybrané činnosti, organizačné jednotky alebo jednotlivé informačné systémy. Štandard prešiel aktualizáciou v roku 2002 a následne bol prijatý organizáciou ISO pod označením ISO/IEC 27001:2005 *Information technology – Security techniques – Information security management systems – Requirements*.

V roku 2007 rodinu štandardov ISO/IEC 27000 rozšíril štandard ISO/IEC 27006:2007 *Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems* upravujúci podmienky pre organizácie certifikujúce zavedené systémy manažérstva informačnej bezpečnosti. V súčasnosti je v príprave ďalších 5 štandardov, pričom tieto štandardy sú v rozličných štádiách rozpracovanosti a mali by pokrývať všetky nevyhnutné aspekty zavádzania ISMS

v organizáciách, ako napr. odporúčania pri zavádzaní ISMS (27003), riadenie rizík (27005), alebo meranie efektívnosti implementovaných opatrení (27004).

Oblasť riadenia informačnej bezpečnosti v minulosti pokrývali viaceré štandardy, napr. štandardy z rodiny ISO/IEC 13335, niektoré zo štandardov triedy NIST SP. Predpokladá sa však, že koncept ISMS bude úspešný a postupne v praxi nahradí, alebo čiastočne pohltí spomínané bezpečnostné štandardy. Jeho hlavnou výhodou je relatívne jednoduchá koncepcia riadenia kompatibilná s inými všeobecne zaužívanými štandardmi, ako napr. ISO 9001 (systém manažérstva kvality), ISO 14001 (environmentálny manažérsky systém) alebo OHSAS (manažérsky systém BOZP), čo umožňuje jednoduché zavádzanie ISMS v rámci integrovaných manažérskych systémov.

4 Štandardizácia informačnej bezpečnosti vo svete

Podobne ako v iných oblastiach, aj v oblasti informačnej bezpečnosti existuje veľa organizácií, ktoré sa snažia riešiť štandardizáciu. Tieto organizácie sú často veľmi rôzneho charakteru:

- *Národné štandardizačné organizácie a odborné organizácie vydávajúce štandardy* – najvýznamnejšími národnými hráčmi sú britské BSI British Standards, americké National Institute of Standards and Technology (NIST) a American National Standards Institute (ANSI) a nemecké DIN Deutsches Institut für Normung e. V. a Bundesamt für Sicherheit in der Informationstechnik (BSI),
- *Medzinárodné štandardizačné organizácie* – inštitúcie, do ktorých činnosti sa spravidla zapájajú zástupcovia národných štandardizačných organizácií, ako aj zástupcovia súkromného sektora. Najvýznamnejšími medzinárodnými štandardizačnými organizáciami sú International Organization for Standardization (ISO), International Electrotechnical Commission (IEC)[5], European Committee for Standardization (CEN), European Committee for Electrotechnical Standardization (CENELEC) a European Telecommunications Standards Institute (ETSI),
- *Súkromné inštitúcie* – inštitúcie rôzneho charakteru spravujúce vlastné štandardy, alebo de-facto štandardy. Patria medzi ne najmä ISACA, The Internet Engineering Task Force (IETF), International Telecommunication Union – Telecommunication Standardization Sector (ITU-T) a RSA Security Inc[6].

V nasledujúcich častiach tejto kapitoly si uvedieme základné informácie a popísaná činnosť najvýznamnejších organizácií vydávajúcich štandardy pre oblasť informačnej bezpečnosti.

4.1 Spoločná technická komisia ISO a IEC (ISO/IEC JTC 1)

Pre oblasť IKT, v ktorej sa pôsobnosti medzinárodných štandardizačných organizácií ISO a IEC prekrývajú, bola vytvorená spoločná technická komisia ISO/IEC Joint Technical

[5] Informačnú bezpečnosť pokrýva spoločná technická komisia organizácií ISO a IEC JTC1, ktorého práca je podrobnejšie popísaná v kapitole *4.1 Spoločná technická komisia ISO a IEC (*ISO/IEC JTC 1).

[6] Štandardy Public Key Cryptography Standards (PKCS) vytvorené kvôli rozširovaniu asymetrického šifrovacieho algoritmu RSA, ktorého patent v tom čase vlastnila spoločnosť RSA Security Inc.

Commitee 1 (ISO/IEC JTC 1, ďalej aj JTC 1). Organizačne je táto komisia ďalej rozdelená na cca 20 subkomisií[7], z ktorých každá sa venuje štandardizácii v rámci pridelenej oblasti.

Informačnej bezpečnosti sa primárne venuje subkomisia SC 27 *IT Security techniques*. Do jej činnosti sa aktívne zapája 37 krajín (tzv. P-členstvo), ďalších 14 krajín má štatút pozorovateľa (tzv. O-členstvo). V súčasnosti do jej kompetencií spadá približne 80 platných štandardov a približne 60 rozpracovaných štandardov[8] (16).

V rámci subkomisie SC 27 je vytvorených 5 pracovných skupín, v rámci ktorých sa riešia jednotlivé oblasti informačnej bezpečnosti. Stručný prehľad pracovných skupín a ich najvýznamnejších oblastí pôsobnosti je uvedený v nasledujúcej tabuľke (tabuľka vychádza z informácií zverejnených na (17)).

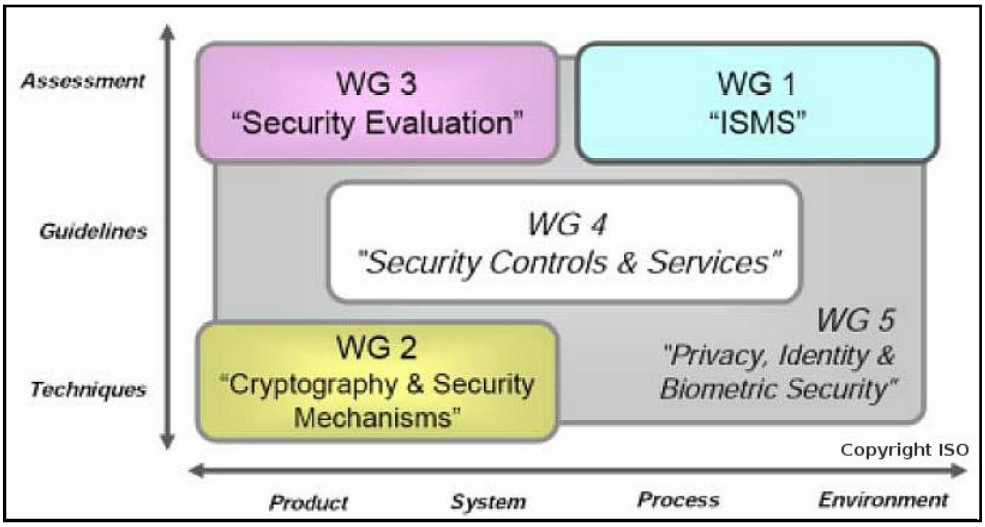
Pracovná skupina	Najvýznamnejšie oblasti pôsobnosti
Pracovná skupina 1 (WG 1) Systémy manažérstva informačnej bezpečnosti	• Vývoj štandardov a odporúčaní súvisiacich s ISMS (rodina štandardov ISO/IEC 27000), • udržiavanie doteraz schválených štandardov v kompetencii WG 1, • spolupráca s ostatnými pracovnými skupinami (najmä WG 4) pri tvorbe štandardov pre implementáciu riadiacich cieľov a opatrení z ISO/IEC 27001.
Pracovná skupina 2 (WG 2) Kryptografické a bezpečnostné mechanizmy	• Vývoj terminológie, všeobecných modelov a štandardov súvisiacich s technikami ochrany informácií v IT systémoch a aplikáciách, so zameraním na oblasť kryptografie.
Pracovná skupina 3 (WG 3) Kritéria pre hodnotenie bezpečnosti systémov	• Vývoj štandardov týkajúcich sa ohodnotenia a certifikácie IT systémov, komponentov a produktov, zohľadňujúc počítačové siete, distribuované systémy, služby aplikácií a pod.
Pracovná skupina 4 (WG 4) Bezpečnostné opatrenia a služby	• Vývoj štandardov a odporúčaní týkajúcich sa služieb a aplikácií podporujúcich implementáciu bezpečnostných cieľov a opatrení v rámci ISMS (ISO/IEC 27001), v oblastiach ako sú napr. sieťová bezpečnosť, riadenie bezpečnostných incidentov, plánovanie kontinuity činností a pod., • spolupráca s ostatnými pracovnými skupinami, najmä WG 1.
Pracovná skupina 5 (WG 5) Technológie pre správu identít a zaistenie súkromia	• Vývoj štandardov a odporúčaní týkajúcich sa bezpečnostných aspektov správy identít, biometrických údajov a ochrany osobných údajov, • spolupráca s ostatnými pracovnými skupinami, najmä WG 1, WG 2 a WG 3, • spolupráca so subkomisiou ISO/IEC JTC1 SC 37 – Biometria.

Tabuľka 1: Pracovné skupiny technickej komisie ISO/IEC JTC 1

[7] Presné informácie o subkomisiách nie je možné získať, nakoľko oficiálne informácie publikované na stránkach organizácií ISO (www.iso.ch) a IEC (www.iec.ch) nie sa nezhodujú napriek tomu, že obe organizácie uvádzajú 17 subkomisií.

[8] V čase finalizácie tohto dokumentu bolo v pôsobnosti JTC 1 SC 27 platných 79 a rozpracovaných 59 štandardov.

Oblasti pôsobnosti jednotlivých pracovných skupín jednoducho ilustruje nasledujúci obrázok (zdroj: (18)).



Obrázok 2: Charakteristika štandardov v gescii pracovných skupín ISO/IEC JTC 1 SC27.

Väčšina procesov v rámci technickej komisie JTC 1, vrátane tvorby nového štandardu, je popísaná v (19). Štandardizačný proces pozostáva z presne definovaných etáp, na záver každej etapy prebieha hlasovanie o postúpení do nasledujúcej etapy.

Bežne sa vývoj štandardu od jeho zaradenia do programu komisie plánuje na 3 roky, podľa rozhodnutia komisie je možné túto časovú lehotu skrátiť alebo predĺžiť o 1 rok. Spolu s voliteľnou etapou štúdia oblasti, ktorá prebieha ešte pred samotným zaradením do programu komisie nepočíta sa do harmonogramu teda štandardizačný proces môže trvať až 5 rokov, čo je pre niektoré oblasti príliš dlhá doba.

Vybraní členovia JTC 1 (najmä P-členovia) majú právo navrhnúť na prevzatie akýkoľvek platný štandard inej štandardizačnej organizácie prostredníctvom zrýchleného konania, tzv. Fast track procedure. V tomto prípade sa úvodné etapy (etapy tvorby štandardu) preskakujú a štandardizačný proces môže trvať menej ako rok.

4.2 Nemecký spolkový úrad pre bezpečnosť IKT systémov

Keďže skratka nemeckého *Bundesamt für Sicherheit in der Informationstechnik* je totožná so skratkou britského BSI British Standards, aby sa predišlo nejednoznačnosti textu, ďalej budeme túto organizáciu skrátene označovať BSI-DE.

Ako už napovedá názov, BSI-DE nie je typickou štandardizačnou organizáciou. Tento úrad plní funkcie najvyššieho štátneho (federálneho) úradu pre informačnú bezpečnosť.

Predmetom jeho činností sú najmä:

- zaistenie bezpečnosti aplikácií, kritickej infraštruktúry a Internetu,

- podpora zavádzania e-Governmentu,
- posudzovanie bezpečnosti kryptografických algoritmov, návrh a implementácia systémov primárne využívajúcich kryptografické algoritmy,
- zabezpečenie informácií proti neautorizovanému prístupu odpočúvaním, o.i. riešením problematiky elektromagnetického vyžarovania,
- analýza bezpečnosti a súladu s bezpečnostnými štandardami nových technológií, ako sú napr. biometrické techniky, elektronické pasy obsahujúce biometrické údaje držiteľov (tzv. biometrické pasy), technológia RFID,
- certifikáciou bezpečnosti IKT systémov (najmä podľa štandardu ISO/IEC 15408 / Common Criteria) a posudzovanie ich súladu s nemeckými právnymi predpismi, akreditáciou organizácií zabezpečujúcich certifikáciu v oblasti bezpečnosti IKT systémov,
- vykonávanie funkcie CERT (Computer Emergency Response Team) [9] pre štátne/federálne úrady.

V rámci uvedených činností BSI-DE vyvíja vlastné IKT systémy, resp. moduly systémov alebo zabezpečuje tvorbu metodických materiálov v uvedených oblastiach. Niektoré metodické materiály je v nemeckých podmienkach možné považovať za štandardy.

Za najvýznamnejší metodický materiál je možné považovať súbor dokumentov na zaistenie základnej úrovne bezpečnosti IKT systémov nazývanú „*IT-Grundschutz*“. Tento súbor pozostáva z:

- Štandardu BSI-Standard 100-1: *Information Security Management Systems*
- Štandardu BSI-Standard 100-2: *IT-Grundschutz Methodology*
- Štandardu BSI-Standard 100-3: *Risk Analysis based on IT-Grundschutz*
- Katalógy hrozieb a opatrení *IT-Grundschutz Catalogues*

Všetky dokumenty sú k dispozícii v nemeckom a anglickom jazyku na internetovej stránke BSI-DE.

Keďže Katalógy hrozieb a opatrení sú pomerne rozsiahle (majú takmer 3000 strán), BSI-DE vytvorilo pre svojich klientov aplikáciu GSTOOL, ktorá zjednodušuje aplikovanie metodiky (a použitie katalógov). Taktiež bolo vytvorených niekoľko dokumentov na podporu použitia metodiky IT-Grundschutz, najmä v prostredí menších organizácií.

[9] **CERT** – tím, ktorého úlohou je poskytovať pomoc pri riešení bezpečnostných incidentov. Niekedy označovaný aj ako CSIRT (Computer Security Incident Response Team).

4.3 BSI British Standards

Organizácia BSI British Standards (ďalej len BSI-UK) je národným štandardizačným orgánom Spojeného kráľovstva Veľkej Británie a Severného Írska. Jeho história siaha do roku 1901, BSI-UK bol vôbec prvým národným štandardizačným orgánom v Európe. Zastupuje záujmy Spojeného kráľovstva v rámci medzinárodných štandardizačných organizácií. Pri vývoji štandardov úzko spolupracuje s vládou Spojeného kráľovstva.

BSI-UK vyprodukuje vo všetkých oblastiach ročne približne 2000 štandardov. Z jeho „dielne" pochádzajú také významné štandardy, ako ISO 9001 (Systém manažérstva kvality), ISO 14001 (systém environmentálneho manažérstva), alebo BS 18001 (OHSAS – manažérsky systém BOZP).

BSI-UK je významnou organizáciou aj v oblasti štandardizácie informačnej bezpečnosti. Ako už bolo spomenuté v kapitole 3.3.3 Štandardy pre riadenie informačnej bezpečnosti, BSI-UK je tvorcom rodiny štandardov ISO/IEC 27000 (pôvodne BS 7799). K pôvodnej dokumentácii vyvinutej na podporu zavádzania SMIB patrí aj rodina dokumentov PD 3000[10].

Medzi ďalšie významné produkty súvisiace s informačnou bezpečnosťou vyvinuté BSI-UK patrí rodina štandardov ISO/IEC 20000 *Information technology -- Service management* (pôvodne BS 15000) týkajúca sa riadenia IT služieb a rodina štandardov BS 25999 *Business continuity management* týkajúca sa riadenia informačnej bezpečnosti.

V porovnaní s JTC 1 sú štandardy v BSI-UK vyvíjané podstatne rýchlejšie. Vývoj trvá spravidla menej ako 1,5 roka. BSI-UK taktiež vydáva iné štandardizačné dokumenty (napr. PAS – Publicly Available Specification), ktoré je možné vyvinúť v priebehu niekoľkých mesiacov. Často sú tieto dokumenty následne použité ako základ pre štandard (príkladom je dokument PAS 56, ktorý položil základy rodiny štandardov BS 25999).

[10] **PD** – Published Document – Publikovaný dokument

5 Štandardizácia v oblasti informačnej bezpečnosti na Slovensku

Táto kapitola sa zaoberá stavom štandardizácie v oblasti informačnej bezpečnosti na Slovensku. V časti *5.1 Súčasný stav štandardizácie v oblasti IB na Slovensku* je popísaný východiskový stav štandardizácie informačnej bezpečnosti na Slovensku. V časti *5.2 Návrh ďalšieho postupu pri štandardizácii v oblasti IB na Slovensku* sa budeme venovať možnostiam, ako zlepšiť stav štandardizácie informačnej bezpečnosti na Slovensku.

5.1 Súčasný stav štandardizácie v oblasti IB na Slovensku

Na Slovensku je zodpovednosť za informačnú bezpečnosť a vydávanie noriem pre túto oblasť rozdelená medzi viaceré inštitúcie. Slovenský ústav technickej normalizácie (SÚTN) je národným normalizačným orgánom, zodpovedá za tvorbu, schvaľovanie a vydávanie slovenských technických noriem a zastupuje Slovensko v medzinárodných a európskych normalizačných organizáciách (ISO, IEC, CEN, CENELEC a ETSI). SÚTN vydáva aj všeobecne platné normy z oblasti informačnej bezpečnosti. Na základe platnej právnej úpravy niektoré štátne orgány vydávajú vyhláškami alebo výnosmi štandardy pre špeciálne oblasti (pozri nižšie).

Štandardizáciu v oblastí informačných technológií na SÚTN pokrýva technická komisia TK 37, v rámci ktorej pôsobí subkomisia SK 02 pre informačnú bezpečnosť. Táto subkomisia zabezpečuje najmä správu noriem sústavy STN súvisiacich s informačnou bezpečnosťou (navrhovanie zaradenia nových noriem a vyradenia neaktuálnych noriem), sledovanie prípravy medzinárodných noriem v danej oblasti a spoluprácu so zahraničnými a medzinárodnými štandardizačnými organizáciami. Prioritne sa sústreďuje na preberanie noriem, ktorých gestorom je subkomisia SC 27 komisie ISO/IEC JTC 1 (činnosť technickej komisie je popísaná v kapitole *4.1 Spoločná technická komisia ISO a IEC (ISO/IEC JTC 1)*). Na zaradenie do sústavy STN môže navrhnúť normu ľubovoľnej organizácie, prípadne vypracovať vlastnú normu.

Pri výbere noriem určených na zaradenie do sústavy STN zohráva významnú úlohu skutočnosť, že niektoré normy (normy vydané organizáciami CEN, CENELEC a ETSI) má SÚTN povinnosť preberať. Táto povinnosť mu vyplýva priamo z členstva v uvedených organizáciách. Technická komisia v prípade povinného preberania noriem spolurozhoduje o spôsobe ich prebratia (20).

Zahraničnú normu možno prijať do sústavy STN prijať nasledovnými spôsobmi:

- prekladom do slovenského jazyka,

- prebratím pôvodného znenia normy v cudzom jazyku,
- prebratím normy v pôvodnom jazyku s doplnením národného komentára v slovenskom jazyku.

Vzhľadom na personálne kapacity členov komisie je pravdepodobné, že počet noriem prebratých prekladom do slovenského jazyka bude relatívne nízky. Pre kľúčové normy sa však dá očakávať, že bude zvolený aj táto možnosť.

Vzhľadom na cenovú politiku organizácie ISO (prebraté normy v pôvodnom znení sa musia predávať za ceny stanovené ISO) je pre SÚTN ekonomicky nevýhodné preberanie noriem v pôsobnosti ISO/IEC JTC 1 v pôvodnom znení. Z uvedených dôvodov sa javia ako relevantné nasledujúce možnosti preberania noriem:

- preberanie medzinárodných noriem v českom jazyku zo sústavy ČSN (českých technických noriem) v spolupráci s ČNI (Český normalizační institut),
- preberanie noriem v pôvodnom znení s doplnením komentára v slovenskom jazyku[11]; vypracovanie komentára by zabezpečovali členovia TK 37 SK 02.

V sústave noriem STN po vyradení zastaraných[12] noriem, ktoré prebehlo v roku 2006, zostalo cca 10 noriem týkajúcich sa informačnej bezpečnosti. Z tohto počtu bolo menej ako polovica spracovaných prekladom do slovenského jazyka. Subkomisia ISO/IEC JTC 1 SC 27 v súčasnosti spravuje 138 noriem (79 platných a 59 pripravovaných), všetky úzko súvisiace s informačnou bezpečnosťou (16).

Okrem SÚTN v podmienkach Slovenskej republiky vydáva, resp. má právo vydávať štandardy súvisiace s informačnou bezpečnosťou viacero štátnych orgánov:

- Národný bezpečnostný úrad (oblasti ochrany utajovaných skutočností a elektronického podpisu),
- Úrad na ochranu osobných údajov (oblasť ochrany osobných údajov),
- Ministerstvo financií SR (štandardy pre informačné systémy verejnej správy),
- Ministerstvo zdravotníctva SR (záväzné štandardy pre zdravotnícku informatiku).

Štandardy sú spravidla vydávané formou vyhlášky alebo výnosu príslušného úradu. Ako príklad môžeme uviesť zákon č. 275/2006 Z.z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov, pre ktorý boli štandardy vydané výnosom Ministerstva dopravy, pôšt a telekomunikácií Slovenskej republiky č. 1706/M-2006

[11] Doplnenie slovenského komentára umožní SÚTN predávať normy iné ceny, ako sú ceny stanovené ISO.

[12] Medzinárodná norma, ktorá bola prebratá do systému STN, bola medzičasom zrušená alebo nahradená inou normou

o štandardoch pre informačné systémy verejnej správy. V súčasnosti je už táto oblasť zastrešená Ministerstvom financií Slovenskej republiky, MF SR v súčasnosti pripravuje aktualizáciu štandardov.

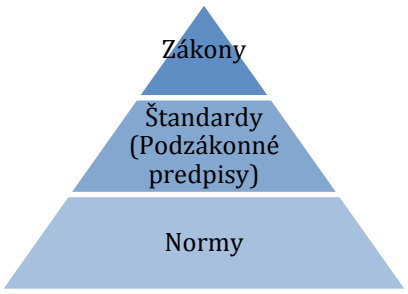
Vydávanie štandardov v oblasti informačnej bezpečnosti nie je centrálne koordinované. Existuje nanajvýš personálne prepojenie niektorých štandardizačných aktivít prostredníctvom zástupcov štátnych orgánov a súkromnej sféry v subkomisii TK 37 SK 02, pracovných skupinách na NBÚ SR a v Komisii pre informačnú bezpečnosť MF SR.

Koordinácia štandardizačnej činnosti bola označená ako jedna z najvýznamnejších priorít pri riešení informačnej bezpečnosti na Slovensku v rámci návrhu dokumentu *Národná stratégia pre informačnú bezpečnosť v Slovenskej republike*(21). Dokument bol vytvorený na Sekcii informatizácie MF SR a v súčasnosti je v etape medzirezortného pripomienkového konania. Predpokladá sa, že stratégia po nevyhnutných úpravách nadobudne účinnosť ešte v priebehu 2. kvartálu roku 2008.

5.2 Návrh ďalšieho postupu pri štandardizácii v oblasti IB na Slovensku

V kontexte rozvoja informatizácie verejnej správy podporeného prijatím Operačného programu Informatizácia spoločnosti (OPIS) sa dá predpokladať, že na Slovensku vznikne niekoľko zákonov súvisiacich s informačnou bezpečnosťou, resp. ktoré budú definovať bezpečnostné požiadavky na nejaký komponent (napr. IKS). Z toho dôvodu je nevyhnutné zabezpečiť, aby tieto bezpečnostné požiadavky boli konzistentné, úplné a kvalitné.

Toto je možné zabezpečiť použitím vhodného prístupu k tvorbe dokumentov. Za optimálne považujeme doterajší prístup, popísaný v predchádzajúcej časti (zákony sa odkazujú na podzákonné predpisy obsahujúce štandardy), o ďalšiu vrstvu obsahujúcu všeobecne akceptované štandardy. Za všeobecne akceptované štandardy sa v prostredí Slovenskej republiky považujú najmä normy zo sústavy STN.



Obrázok 3: Návrh postavenia štandardov pri tvorbe legislatívy

Proces tvorby zákonov by aj pri navrhovanom prístupe zostal nezmenený. Pri tvorbe akýchkoľvek dokumentov týkajúcich sa informačnej bezpečnosti (zákonov, podzákonných predpisov, štandardov, noriem, ...) je však potrebné dodržiavať jednotnú terminológiu. Jedným zo spôsob, ako je možné zabezpečiť túto požiadavku, je vypracovanie metodického materiálu obsahujúceho výkladový slovník pojmov z oblasti informačnej bezpečnosti a jeho dôsledné využívanie pri tvorbe dokumentov.

Na ostatných úrovniach by aplikovanie navrhovaného prístupu vyžadovalo splnenie nasledujúcich predpokladov:

- zabezpečiť zmenu prístupu k tvorbe štandardov,
- zabezpečiť vhodnú komunikáciu medzi orgánmi spracúvajúcimi štandardy a technickou komisiou zabezpečujúcou prípravu noriem,
- zabezpečiť vhodné podmienky a dostatok zdrojov (personálnych, finančných) na tvorbu noriem.

V ideálnom prípade by štandardy mali obsahovať najmä odkazy na jednotlivé požiadavky noriem, spolu s informáciou o tom, za akých podmienok je splnenie referencovaných požiadaviek potrebné (napr. povinné, povinné za stanovených podmienok, odporúčané).

S tým súvisí aj požiadavka na dostupnosť vhodných noriem v sústave STN. Úlohou príslušnej technickej komisie (subkomisie SK 02 TK 37 SÚTN) by malo byť v relatívne krátkom čase zabezpečiť naplnenie sústavy STN aktuálnymi, neprotirečivými a kvalitnými normami. Predpokladá sa, že ako základ sa použijú vybrané normy vypracované v rámci ISO/IEC JTC 1 SC 27. V prípade potreby je možné ich doplniť akýmkoľvek iným štandardom spracovaným inou organizáciou alebo vytvoreným samotnou komisiou. Na naplnenie tohto cieľa boli v rámci subkomisie SK 02 technickej komisie TK 37 SÚTN na poslednom zasadnutí, ktoré sa konalo dňa 28.4.2008, podniknuté úvodné kroky.

Okrem naplnenia sústavy STN by bolo vhodné zabezpečiť komunikáciu medzi orgánmi zabezpečujúcimi spracovanie štandardov a technickou komisiou zabezpečujúcou prípravu noriem ohľadom prípadných požiadaviek na vytvorenie/prebratie štandardu pre oblasť, ktorá v danom čase nie je pokrytá platnými normami v sústave STN. Výber konkrétnych noriem a ich spracovanie/prevzatie by však za každých okolností malo byť výhradne v kompetencii odborníkov.

Pri aplikácii navrhovaného prístupu sa môže ako problematická javiť nedostatočná kapacita ľudských zdrojov. Nakoľko ľudí s odbornými predpokladmi je relatívne málo, je nevyhnutné, aby boli odbremenení od akýchkoľvek aktivít, ktoré nie sú nevyhnutné na prácu v technickej komisii. Toto sa týka najmä technického zabezpečenia a administratívnej podpory. Čiastočne by tento problém mohol byť vyriešený implementáciou systému podľa požiadaviek, ktoré sú uvedené v prílohe *Príloha B – Základné požiadavky na funkčnosť IS*.

Keď bude štandardizácia v oblasti informačnej bezpečnosti na Slovensku na dostatočnej úrovni, bude možné spraviť ďalší krok, ktorým je presadzovanie záujmov Slovenska v medzinárodných štandardizačných organizáciách. Tento cieľ je možné dosiahnuť iba

aktívnou participáciou na štandardizačných procesoch. Práca v medzinárodnej štandardizačnej komisii je časovo veľmi náročná a vyžaduje si aj nemalé ďalšie náklady (napr. náklady súvisiace s účasťou na zasadnutiach technických komisií). Preto považujeme za nevyhnutné v budúcnosti vyriešiť zdroj financovania týchto aktivít.

6 Kategorizácia štandardov v oblasti informačnej bezpečnosti

Štandardov týkajúcich sa informačnej bezpečnosti je nespočetne veľa. Aby bolo možné s nimi efektívne pracovať, je nevyhnutné zaviesť mechanizmy kategorizácie štandardov a relácií medzi štandardmi.

Prehľad o existujúcich štandardoch je pre niektoré osoby nevyhnutný. Týka sa to najmä členov štandardizačných komisií alebo iných obdobných orgánov. Pôvodným zámerom bolo aplikovanie navrhnutej kategorizácie štandardov v rámci TK 37 SK 02 SÚTN.

Individuálna kategorizácia štandardov bez použitia vhodného nástroja by však bola pomerne náročná a značne neefektívna. Preto vznikla myšlienka vytvoriť informačný systém, ktorý by umožňoval jednoduchú evidenciu štandardov, ich kategorizáciu a vytváranie vzťahov medzi nimi. Aby sa zjednodušil prístup používateľov IS k informáciám o štandardoch a obmedzilo viacnásobné vykonávanie tých istých činností, navrhli sme tento systém implementovať ako tenkého klienta (aplikáciu s webovým front-endom). Špecifikácia požiadaviek na systém je súčasťou tejto diplomovej práce a nachádza sa v prílohe *Príloha B – Základné požiadavky na funkčnosť IS*.

Uvedená špecifikácia je súčasťou zadania záverečnej práce študenta bakalárskeho študijného programu na FMFI UK. Bakalárska práca študentky Evy Porvazníkovej s pracovným názvom *Systém pre kategorizáciu štandardizačných materiálov v oblasti informačnej bezpečnosti* bola v čase tvorby odovzdania dokumentu v procese tvorby.

V tejto kapitole si uvedieme niektoré z možností kategorizácie a vytvárania vzťahov medzi štandardmi. Jednotlivé možnosti boli navrhované tak, aby boli jednoducho použiteľné v rámci informačného systému po jeho dokončení.

6.1 Kategorizácia štandardov

Vzhľadom na veľkú rôznorodosť štandardov môžeme štandardy kategorizovať podľa viacerých hľadísk – kritérií. V tejto kapitole sú popísané kritériá, ktoré považujeme za najvýznamnejšie. Patria medzi ne:

- obsahové zameranie štandardu,
- záväznosť štandardu,
- úroveň spracovania (cieľová skupina) štandardu,
- vydavateľ štandardu,
- stav procesu štandardizácie,
- jazyk štandardu.

V nasledujúcich častiach si zdôvodníme potrebu zavedenia týchto kritérií (najmä z hľadiska použitia v rámci technickej komisie TK 37 SK 02 SÚTN) a uvedieme kategórie, do ktorých je možné zaraďovať jednotlivé štandardy.

6.1.1 Kategorizácia podľa obsahového zamerania štandardu

Oblasť informačnej bezpečnosti zahŕňa veľké množstvo oblastí, pre ktoré sú vytvárané štandardy. Zaradenie štandardov do kategórií podľa obsahového zamerania je nevyhnutné pre orientáciu medzi veľkým množstvom štandardov, preto ho považujeme za základné a najvýznamnejšie kritérium pre kategorizáciu štandardov.

Na kategorizáciu štandardov podľa obsahu je možných niekoľko prístupov. Prvý prístup je inšpirovaný rozdelením pracovných skupín v rámci ISO/IEC JTC 1 SC 27. Druhý prístup vychádza z kategorizácie vlastných štandardov, ktorú vypracoval americký NIST. Ani jeden z uvedených prístupov však na naše účely nepovažujeme za optimálny, preto v závere tejto časti navrhneme vlastný prístup na kategorizáciu štandardov podľa obsahového zamerania

Prístup prvý – kategorizácia inšpirovaná rozdelením ISO/IEC JTC 1 SC 27

V predchádzajúcej kapitole (Tabuľka 1 uvedená v časti *4.1 Spoločná technická komisia ISO a IEC (ISO/IEC JTC 1)*) sme si uviedli základné rozdelenie kompetencií jednotlivých pracovných skupín JTC 1 SC 27. Keďže toto delenie definuje základné oblasti informačnej bezpečnosti, po menších úpravách by mohlo byť vhodné na kategorizáciu štandardov podľa obsahového zamerania. V takomto prípade by boli definované nasledujúce kategórie:

- systémy manažérstva informačnej bezpečnosti,
- kryptografické a bezpečnostné mechanizmy,
- kritéria pre hodnotenie bezpečnosti systémov,
- bezpečnostné opatrenia a služby,
- technológie pre správu identít a zaistenie súkromia.

S prihliadnutím na veľkú rozmanitosť štandardov však považujeme takéto rozdelenie za príliš „hrubé“.

Prístup druhý – kategorizácia podľa NIST

Otázkou kategorizácie štandardov sa už v minulosti zaoberal aj americký NIST. Výsledkom bola publikácia (22), v ktorej boli dokumenty produkované NIST zaradené do kategórií z hľadiska troch kritérií. Jedno z kritérií (*topic clusters*) by bolo možné použiť ako základ pre kategorizáciu štandardov z hľadiska obsahového zamerania štandardu. Originálne

názvy a popisy kategórii sú v prílohe Príloha *C – Prístup NIST ku kategorizácii* štandardov podľa zamerania uvedené spolu s voľným slovenským prekladom. Táto kategorizačná schéma je naopak príliš „jemná“, preto ju nepovažujeme za vhodnú.

Prístup tretí – kategorizácia podľa vlastného návrhu

Na základe uvedených skutočností sme sa rozhodli vytvoriť vlastný prístup ku kategorizácii na strednej úrovni granularity. Tento prístup obsahuje nasledujúce kategórie:

- Audit
- Certifikácia systémov
- Identifikácia a autentifikácia
- Kryptografia
- Manažment informačnej bezpečnosti
- PKI a digitálny podpis
- Riadenie kontinuity činností a bezpečnostných incidentov
- Technické aspekty informačnej bezpečnosti
- Vývoj a údržba systémov
- Iné

Vzťah medzi prístupmi na kategorizáciu podľa obsahového zamerania štandardov

Uvedené kategórie boli navrhované tak, aby bolo možné podľa možností čo najjednoduchšie vzájomné mapovanie všetkých troch prístupov ku kategorizácii podľa obsahového zamerania uvedených v tejto kapitole. Vzťahy medzi kategóriami pri kategorizácii podľa rôznych prístupov sú zrejmé z nasledujúcej tabuľky.

Prístup podľa ISO/IEC	**Navrhovaný prístup**	**Prístup podľa NIST**
Systémy manažérstva informačnej bezpečnosti	Manažment informačnej bezpečnosti	Plánovanie Ohodnotenie rizík
	Audit	Audit a sledovateľnosť Vyšetrovanie
Kryptografické a bezpečnostné mechanizmy	Kryptografia	Kryptografia
	PKI a digitálny podpis	Digitálny podpis Infraštruktúra verejných kľúčov (PKI)
Kritéria pre hodnotenie bezpečnosti systémov	Certifikácia systémov	Certifikácia a akreditácia IS

Prístup podľa ISO/IEC	Navrhovaný prístup	Prístup podľa NIST
Bezpečnostné opatrenia a služby	Vývoj a údržba systémov	Údržba Akvizícia systémov a súvisiacich služieb
	Technické aspekty informačnej bezpečnosti	Komunikácie a bezdrôtové siete Všeobecné aspekty bezpečnosti IT Vírusy a škodlivý softvér
	Riadenie kontinuity činností a bezpečnostných incidentov	Plánovanie kontinuity činností Reakcia na bezpečnostné incidenty
Technológie pre správu identít a zaistenie súkromia	Identifikácia a autentifikácia	Autentifikácia Biometria Overovanie identity osôb Smart karty
Iné	Iné	Povedomie a vzdelávanie v oblasti bezpečnosti

Tabuľka 2: Vzťah medzi kategóriami pri kategorizácii podľa rôznych prístupov

6.1.2 Kategorizácia podľa záväznosti štandardu

Záväznosť štandardu významne ovplyvňuje poradie preberania štandardov. Niektoré štandardy musia byť povinne prebraté v stanovenom čase. Iné štandardy je naopak vhodné prebrať do sústavy STN, nakoľko sú referencované niektorým z právne záväzných dokumentov. Toto kritérium však považujeme za užitočné aj pre ostatných používateľov štandardov.

Pre kategorizáciu podľa záväznosti navrhujeme zaviesť nasledujúce kategórie:

- EN – európska norma[13],
- aplikácia štandardu vyplýva z legislatívy SR alebo EÚ,
- podľa štandardu je možná certifikácia organizácie/produktu,
- nezáväzné štandardy.

6.1.3 Kategorizácia podľa úrovne spracovania (cieľovej skupina) štandardu

Toto kritérium veľa napovedá o obsahu štandardu. Úroveň spracovania je potrebné zohľadňovať aj pri tvorbe stratégie preberania štandardov (napr. vo väčšine prípadov nemá zmysel spracovať najprv metodický materiál na aplikáciu certifikačnej normy skôr, ako je vydaná samotná norma).

[13] Slovenská republika je povinná prevziať všetky EN do 6 mesiacov od ich vydania.

Z hľadiska úrovne spracovanie sme identifikovali nasledujúce kategórie:

- certifikačná/záväzná norma,
- odporúčania,
- metodický materiál,
- návod, *How-to* príručka.

6.1.4 Kategorizácia podľa vydavateľa štandardu

Viaceré medzinárodné štandardy vznikli prebratím národných štandardov, resp. existujú tematický rovnako zamerané štandardy rozličných štandardizačných organizácií. Na zisťovanie vzťahov medzi takýmito štandardami je užitočné aj kritérium vydavateľa štandardu.

Keďže vydavateľov štandardov je veľké množstvo, nie je možné (a ani efektívne) vytvoriť ich úplný zoznam. Predpokladá sa však, že väčšina evidovaných štandardov bude vydaných jednou zo štandardizačných organizácií spomenutých v úvode kapitoly *4 Štandardizácia informačnej bezpečnosti vo svete*, resp. v kapitole *5 Štandardizácia v oblasti informačnej bezpečnosti na Slovensku*.

6.1.5 Kategorizácia podľa etapy životného cyklu štandardu

Významným faktorom ovplyvňujúcim výber štandardov vhodných na prebratie do sústavy STN je aj informácia o tom, v ktorej etape životného cyklu sa štandard nachádza. Niektoré kategórie taktiež infikujú nutnosť/vhodnosť zapojenia sa do procesu prípravy alebo schvaľovania medzinárodného štandardu.

Väčšina štandardizačných organizácií využíva rozdielne životné cykly štandardov. Na základe spoločných čŕt boli identifikované nasledujúce etapy životného cyklu štandardov, ktoré by mali jednoznačne charakterizovať stav štandardizácie daného dokumentu:

- v príprave,
- čaká na schválenie,
- platný,
- čaká na revíziu/zrušenie,
- zrušený.

6.1.6 Kategorizácia podľa jazyka štandardu

Napriek tomu, že toto kritérium je pomerne priamočiare, jeho hodnota je pri rozhodovaní o použití, resp. prebratí štandardov pomerne významná. Napr. štandardy v českom a slovenskom jazyku sú použiteľné okamžite, štandardy v ostatných jazykoch na použitie vyžadujú príslušné jazykové znalosti.

Očakáva sa, že väčšina evidovaných štandardov bude pri kategorizácii podľa jazyka zaradená do nasledujúcich kategórií:

- anglický,
- nemecký,
- francúzsky,
- český,
- slovenský.

6.2 Vytváranie vzťahov medzi štandardmi

Samotné zaradenie štandardov do jednotlivých kategórií by používateľovi nemuselo poskytnúť úplné informácie o štandardoch – kategorizáciou je len veľmi ťažko možné poskytnúť informácie o vzájomných vzťahoch medzi štandardmi.

Počas analýzy problematiky boli identifikované dva hlavné typy vzájomných vzťahov medzi štandardmi:

- vzťahy medzi dvoma štandardmi (binárne vzťahy),
- vzťahy medzi viacerými štandardmi (N-árne vzťahy).

Binárne vzťahy ďalej môžeme deliť na neorientované a orientované. V prípade neorientovaných vzťahov nezáleží na poradí, v akom sú štandardy uvedené. V prípade orientovaných vzťahov naopak záleží na poradí, v ktorom sú štandardy vo vzťahu uvedené. Pri tvorbe tejto práce boli identifikované nasledujúce binárne vzťahy:

- „súvisí s“ (neorientovaný),
- „koliduje s“ (neorientovaný),
- „nahrádza“ (orientovaný),
- „je prekladom“ (orientovaný),
- „preberá“[14] (orientovaný).

Význam uvedených vzťahov považujeme za zrejmý, preto ho nebudeme podrobnejšie popisovať.

Binárne vzťahy je možné taktiež popísať pomocou orientovaného grafu[15], ktorého vrcholmi sú jednotlivé štandardy. Neorientovaná hrana v ňom reprezentuje neorientovaný binárny vzťah, orientovaná hrana reprezentuje orientovaný binárny vzťah.

[14] Napr. STN ISO/IEC 7064:2004 preberá ISO/IEC 7064:2003

[15] V prípade potreby objasnenia niektorého z pojmov teórie grafov odporúčame čitateľa napr. na (22).

Vzťahy medzi viacerými štandardmi (N-árne vzťahy) nám umožnia modelovať skupiny štandardov. Je ich možné využiť napr. na uchovávanie informácií o rodinách štandardov, ako sú PKCS, ISO/IEC 13335 alebo BS 25999.

Významovo sú rozšírením binárneho neorientovaného vzťahu a je možné ich s použitím tohto vzťahu modelovať. V takomto prípade by však údržba informácií o väčších skupinách štandardov bola značne náročná.

V grafovej teórii by N-árne vzťahy bolo možné reprezentovať pomocou hyperhrán v hypergrafe, ktorého vrcholmi sú jednotlivé štandardy.

7 Záver

S významom IKT systémov vzrastá aj potreba ich adekvátnej ochrany. Rozsah a zložitosť IKT systémov prakticky vylučuje možnosť individuálneho riešenia informačnej bezpečnosti jednotlivých IKT systémov. Štandardizácia v oblasti informačnej bezpečnosti predstavuje isté východiská – stanovuje bezpečnostné požiadavky na systémy, resp. komponenty systémov, spôsob komunikácie medzi nimi, bezpečnostné funkcie aj celkové riadenie informačnej bezpečnosti. To umožňuje prejsť od nesystematického riešenia bezpečnosti (ad-hoc) k systematickému prístupu, keď sa zložitejšie IKT systémy vytvárajú z komponentov so zaručenou bezpečnostnou úrovňou spôsobom, ktorý zachováva bezpečnostnú úroveň jednotlivých komponentov aj na úrovni celku. Bezpečnostné štandardy sa takto stávajú dôležitým nástrojom na dosiahnutie potrebnej úrovne informačnej bezpečnosti. To sa prejavuje aj v aktivite štandardizačných organizácií, narastajúcom počte štandardov, ktoré vydávajú a oblastiach, ktoré pokrývajú.

Aby bolo možné využívať poznanie, ktoré štandardy predstavujú a zaistiť porovnateľnú úroveň slovenských IKT systémov s medzinárodnými, je potrebné sprístupniť aspoň najdôležitejšie medzinárodné bezpečnostné štandardy slovenskej odbornej verejnosti. V súčasnosti sa javí ako najvhodnejšie vybrať niektoré štandardy prijaté komisiou ISO/IEC JTC 1 SC 27 a doplniť ich vhodnými dokumentmi vytvorenými inými štandardizačnými organizáciami. Taktiež je potrebné zohľadniť ich pri tvorbe akýchkoľvek právne záväzných dokumentov, najmä pri vydávaní zákonov a súvisiacich štandardov (prostredníctvom podzákonných noriem).

Štandardizačná činnosť v oblasti informačnej bezpečnosti na Slovensku popri roztrieštenosti kompetencií a nedostatočnej koordinácii vydávaných rezortných štandardov naráža na najmä nedostatok odborných kapacít, materiálnych a technických zdrojov. V dôsledku toho nie je zabezpečené dostatočné aktualizovanie noriem sústavy STN.

Uvedené problémy je možné riešiť koordináciou vydávania štandardov a zmenou prístupu k tvorbe štandardov využívaných zákonmi. Pri nedostatku odborných kapacít a vysokom množstve úloh je nevyhnutné zabezpečiť dostatočnú materiálno-technickú a organizačnú podporu odborníkom pri vykonávaní svojich úloh. Za významný nástroj na uľahčenie práce odborníkov považujeme kategorizáciu existujúcich štandardov podľa viacerých kritérií. V prípade, že kategorizácia štandardov bude podporená vhodným nástrojom (ktorý v ideálnom prípade môže integrovať aj ďalšiu funkcionalitu), môže jeho dostupnosť znamenať významnú úsporu času členov technickej komisie.

Iba preberanie štandardov vytvorených inými organizáciami nie je na plnenie záujmov Slovenska postačujúce. V budúcnosti je nevyhnutné zabezpečiť ich presadzovanie aj prostredníctvom aktívneho zapájania do procesu štandardizácie v rámci medzinárodných organizácií.

Národná stratégia pre informačnú bezpečnosť v Slovenskej republike a pripravované projekty informatizácie verejnej správy (e-Government), zdravotníctva, ako aj ďalšie veľké projekty založené na IKT zvyšujú pravdepodobnosť, že sa problémy štandardizácie v oblasti informačnej bezpečnosti načrtnuté v tejto práci budú riešiť. Realizácia riešení navrhovaných v diplomovej práci, ktoré vychádzajú zo skúseností v štandardizačnej komisii SÚTN, alebo iných riešení vyššie uvedených problémov môže významne napomôcť vyriešiť nielen najzávažnejšie problémy štandardizácie v oblasti informačnej bezpečnosti na Slovensku, ale prispieť aj k zvýšeniu úrovne informačnej bezpečnosti v SR.

8 Zoznam referencií

1. **Kralovič, Martin a Olejár, Daniel.** Štandardy v informačnej bezpečnosti. *Informačná bezpečnosť '08 - Zborník príspevkov.* Bratislava : SASIB, 2008.

2. **Olejár, Daniel a Janáček, Jaroslav.** Bezpečnostné aspekty systémov postavených na Open Source. *EEA - informačné a komunikačné riešenia.* [Online] http://www.eea.sk/osin/doc/Bezpecnost.pdf.

3. **Inštitút informatiky a štatistiky.** *Bezpečnostné aspekty systému integrovaných e-služieb verejnej správy - Príloha C správy k záverečnej oponentúre riešenia úlohy.* Bratislava : Inštitút informatiky a štatistiky, 2005.

4. Common Criteria for Information Technology Security Evaluation v. 2.3. *Common Criteria - The Common Criteria Portal.* [Online] http://www.commoncriteriaportal.org/files/ccfiles/ccpart1v2.3.pdf.

5. **David, Kahn.** *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet.* New York : Scribner, 1996.

6. *ISO/IEC 27002:2005 Information technology -- Security techniques -- Code of practice for information security management.*

7. **Bundesamt für Sicherheit in der Informationstechnik.** The IT Security Situation in Germany in 2007. [Online] apríl 2007. http://www.bsi.de/english/publications/securitysituation/Lagebericht_2007_englisch.pdf.

8. **Galler, Gerard.** A Strategy for a secure Information Society – "Dialogue, Partnership and empowerment and empowerment". [Online] 17. január 2007. http://www.etsi.org/WebSite/document/Workshop/Security2007/Security2007S4_0_Gerard_Galler.pdf.

9. **Rada Európy.** Uznesenie Rady o Stratégii pre bezpečnú informačnú spoločnosť v Európe. [Online] 22. March 2007. http://www.telecom.gov.sk/externe/legeu/telekom/070324i.htm.

10. **RSA Security Inc.** Public-Key Cryptography Standards (PKCS). [Online] http://www.rsa.com/rsalabs/node.asp?id=2124.

11. *Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.* 12. február 2000, Official Journal, Zv. L 013, 19/01/2000, s. 0012 - 0020.

12. **The Internet Engineering Task Force.** RFC Index. *IETF Home Page.* [Online] http://www.ietf.org/iesg/1rfc_index.txt.

13. Information technology security evaluation criteria v 1.2. [Online] 28. jún 1991. http://www.ssi.gouv.fr/site_documents/ITSEC/ITSEC-uk.pdf.

14. Official CC/CEM versions. *The Common Criteria Portal.* [Online] http://www.commoncriteriaportal.org/thecc.html.

15. Protection Profiles. *The Common Criteria Portal.* [Online] http://www.commoncriteriaportal.org/pp.html.

16. **International Organization for Standardization.** ISO Standards - JTC 1/SC 27 - IT Security techniques. *ISO - International Organization for Standardization.* [Online] http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=45306.

17. **Deutsches Institut für Normung e. V.** Deutsches Institut für Normung : Structure (ISO/IEC JTC 1 SC 27). *Deutsches Institut für Normung : Homepage.* [Online] http://www.jtc1sc27.din.de/cmd?level=tpl-bereich&menuid=63157&cmsareaid=63157&languageid=en.

18. **Steichen, Pascal.** Roadmap ISO/IEC 2700x. [Online] máj 2007. http://www.ansil.eu/files/pres-eurosec2007-23052007.pdf.

19. **ISO/IEC JTC 1.** ISO/IEC JTC 1 Directives, 5th Edition Version 3.0. [Online] 05. apríl 2007. http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/755080/1054033/2541871/JTC001-N-8557.pdf?nodeid=6319110&vernum=0.

20. **Slovenský ústav technickej normalizácie.** Štatút a rokovací poriadok technickej komisie. [Online] 1. február 2008. http://www.sutn.gov.sk/get_file.php?id=508&type=text.

21. **Ministerstvo financií Slovenskej republiky.** Národná stratégia pre informačnú bezpečnosť v Slovenskej republike (pracovná verzia). [Online] 2008. http://www.finance.gov.sk/Default.aspx?CatID=6768.

22. **National Institute of Standards and Technology.** Guide to NIST Information Security Documents. [Online] marec 2007. http://csrc.nist.gov/publications/CSD_DocsGuide.pdf.

23. **Diestel, Reinhard.** Graph Teory. [Online] 2005. http://www.math.uni-hamburg.de/home/diestel/books/graph.theory/GraphTheoryIII.counted.pdf.

Poznámka: Všetky online zdroje sú platné ku dňu odovzdania tejto práce (7.5.2008)

Príloha A – Slovník pojmov

Access (prístup)

(1) Špecifický typ interakcie medzi subjektom a objektom, ktorého výsledkom je tok informácií od jedného k druhému.

(2) Schopnosť a prostriedky potrebné na dosiahnutie, uloženie alebo získanie údajov, na komunikáciu s alebo použitie nejakého zdroja IKT systému.

Access control (riadenie prístupu)

(1) Ohraničenie práv alebo možností subjektu komunikovať s inými subjektmi alebo používať funkcie alebo služby IKT systému.

(2) Obmedzenia riadiace prístup subjektu k objektu.

Access right (prístupové právo)

Povolenie uskutočňovať nejaký typ prístupu (access type) udelené subjektu alebo objektu.

Access type (typ prístupu)

Špecifický typ interakcie, ktorý možno uplatniť na nejakom objekte.

Accountability (sledovateľnosť)

Vlastnosť alebo stav IKT systému umožňujúca priradiť činnosti uskutočňované v systéme jednotlivcom, ktorých potom možno za ne brať na zodpovednosť. Činnosti zahŕňajú porušenia a pokusy o porušenia bezpečnostnej politiky, ako aj povolené činnosti.

Administrator (administrátor)

Osoba, ktorá je v kontakte s IKT systémom a je zodpovedná za udržiavanie jeho operačných schopností.

Asset (aktívum)

Informácia alebo zdroj, ktorý má hodnotu, môže byť cieľom pôsobenia nejakej hrozby a má byť chránený.

Assurance (záruka)

Stupeň dôvery v to, že IKT systém adekvátne spĺňa bezpečnostné požiadavky. Dva hlavné aspekty záruk sú efektívnosť a korektnosť.

Assurance level (úroveň záruk)

Preddefinovaná množina komponentov záruk, ktorá priraďuje mieru vlastnej bezpečnostnej kvality IKT systému. Ak IKT systém dosahuje nejakú úroveň záruk, znamená to že sa na IKT systém použili všetky prostriedky záruk (assurace measures) prislúchajúce danej úrovni.

Attack (útok)

Pokus o obídenie bezpečnostných mechanizmov IK systému. Môže byť aktívny (narušenie údajov) alebo pasívny (získanie údajov).

Attack potential (útočný potenciál)

Predpoklady potrebné na uskutočnenie úspešného útoku. Vyjadrujú sa pomocou útočníkových znalostí, motivácie a zdrojov.

Audit (audit)

Nezávislé skúmanie a vyhodnotenie záznamov a aktivít za účelom určenia súladu s definovanými pravidlami a zistenia prípadných nedostatkov v bezpečnostnej politike IKT systému alebo jej uplatňovaní.

Authentication (autentifikácia)

(1) Overenie identity používateľa, zariadenia alebo inej entity.

(2) Overenie integrity uložených, prenášaných údajov, alebo údajov iným spôsobom vystavených možnosti neoprávnenej modifikácie v IK systéme.

Authentication data (autentifikačné údaje)

Informácia, ktorá sa používa na overenie deklarovanej identity používateľa.

Autorization (autorizácia)

Udelenie prístupových práv pre používateľa, program alebo proces.

Authorized user (oprávnený používateľ)

Používateľ, ktorý môže v súlade s bezpečnostnou politikou systému vykonať nejakú operáciu v systéme.

Availability (dostupnosť)

Požiadavka, aby informácia a iné zdroje systému boli prístupné oprávneným používateľom bez zbytočného zdržiavania vtedy, keď to je potrebné.

Channel (kanál)

Cesta v systéme slúžiaca na prenos údajov. Môže tiež predstavovať mechanizmus, prostredníctvom ktorého sa cesta realizuje.

Compromise (kompromitácia)

Narušenie bezpečnosti systému, ktoré môže viesť k odhaleniu citlivej informácie.

Confidentiality (dôvernosť)

Bezpečnostný atribút vyjadrujúci to, že obsah správy, údajov nie je odhalený nepovolanej osobe, procesu, entite alebo organizácii.

Configuration (konfigurácia)

Výber jednej z možných kombinácií parametrov systému.

Configuration control (riadenie konfigurácie)

Riadenie zmien hardvéru, softvéru, firmvéru a dokumentácie systému v priebehu jeho vývoja a celého životného cyklu.

Configuration management (manažment konfigurácie)

Manažment bezpečnostných charakteristík a záruk systému prostredníctvom zmien hardvéru, softvéru, firmvéru, dokumentácie, testov a ich dokumentácie v priebehu vývoja a životného cyklu systému.

Connectivity (prepojenosť)

Vlastnosť systému, ktorá mu umožňuje interakcie s externými IKT entitami. To zahŕňa výmenu údajov pomocou pevnej linky alebo bezdrôtového spojenia na ľubovoľnú vzdialenosť, v ľubovoľnom prostredí alebo konfigurácii.

Contingency plan (plán kontinuity činností)

Plán reakcií na mimoriadne situácie, operácie zálohovania a obnovy systému po havárii, ktorý je súčasťou bezpečnostného programu organizácie. Jeho cieľom je zaistiť dostupnosť kritických zdrojov a umožniť kontinuitu operácií systému v núdzových situáciách.

Cost-risk analysis (analýza rizík a nákladov)

Odhad nákladov na ochranu údajov v systéme v porovnaní s ujmou spôsobenou stratou alebo kompromitáciou údajov.

Countermeasure (protiopatrenie)

Činnosť, zariadenie, procedúra, technika alebo iný prostriedok, ktorý redukuje zraniteľnosť systému nejakou hrozbou.

Covert Channel (skrytý kanál)

Komunikačný kanál, ktorý umožňuje nejakému procesu prenášať informácie spôsobom, ktorá je v rozpore s bezpečnostnou politikou systému.

Data (údaje)

Informácia v špecifickej fyzickej reprezentácii.

Data confidentiality (dôvernosť údajov)

Bezpečnostný atribút údajov, ktorý vyjadruje, že údaje sú chránené pred neoprávneným odhalením.

Data integrity (integrita údajov)

Bezpečnostný atribút údajov, ktorý vyjadruje, že údaje sú chránené pred neoprávnenou modifikáciou alebo zničením.

Data security (bezpečnosť údajov)

Ochrana údajov pred neoprávnenou (neúmyselnou alebo zámernou) modifikáciou, zničením alebo odhalením.

Denial of service (odmietnutie služby)

Zabránenie autorizovanému prístupu k nejakej položke alebo službe IKT systému, alebo oneskorenie časovo kritickej operácie.

Evaluation (evaluácia)

Ohodnotenie systému, bezpečnostného profilu alebo bezpečnostného cieľa vzhľadom na stanovené kritériá.

Evaluation assurance level (EAL)

Súbor komponentov záruk zo štandardu Common Criteria, ktorý predstavuje bod na stupnici záruk definovanej štandardom Common Criteria.

Environment (prostredie)

Všetko (používatelia, procedúry, objekty, podmienky, iné systémy), čo nie je súčasťou IKT systému, ale má vplyv na systém.

Functional testing (funkčné testovanie)

Časť bezpečnostného testovania, pri ktorom sa deklarované rysy systému testujú na korektnosť operácií.

Functionality (funkcionalita)

Množina funkčných bezpečnostných požiadaviek, ktorá sa má implementovať v IKT systéme.

Granularity (granularita)

Rozlišovacia úroveň, na ktorú možno nejaký mechanizmus nastaviť.

Identification (identifikácia)

Proces ktorý umožňuje IKT systému rozpoznať nejakú entitu.

Implementation (implementácia)

Fáza vývojového procesu systému, v ktorej sa detailná špecifikácia systému realizuje pomocou hardvéru a softvéru.

Least privilege (najmenšie privilégium)

Princíp, ktorý vyžaduje, aby každý subjekt dostal najmenšie možné oprávnenia, ktoré postačujú pre výkon jeho úloh.

Need-to-know principle (princíp nutnosti vedieť)

Princíp ktorého uplatňovanie znamená, že subjekt má prístup, pozná alebo vlastní špecifické informácie potrebné pre výkon jeho oficiálnych povinností.

Object (objekt)

Pasívna entita, ktorá obsahuje alebo dostáva informáciu. Z prístupu k objektu vyplýva aj prístup k informácii, ktorú objekt obsahuje.

Object reuse (opätovné použitie objektu)

Priradenie a opätovné použitie pamäťového média (napr. rámca stránky, sektora disku, magnetickej pásky) ktoré už obsahovalo nejaké objekty. Aby sa pamäťové médiá dali bezpečne znova použiť, nesmú obsahovať zvyšky údajov predchádzajúcich objektov, ktoré boli na nich uložené.

Organizational Security Policy (bezpečnostná politika organizácie)

Súbor právnych noriem, pravidiel a praktík ktoré upravujú spôsob, ako organizácia manažuje, ochraňuje a distribuuje citlivú informáciu.

Password (heslo)

Chránený/súkromný reťazec znakov, ktorý slúži na overenie identity alebo na autorizovanie prístupu k údajom.

Permissions (oprávnenia)

Popis typov oprávnených interakcií subjektu s objektom. Príklady: čítanie, zápis, vykonávanie, pridávanie, modifikácia a odstraňovanie.

Personnel security (personálna bezpečnosť)

Procedúry prijaté na zabezpečenie toho, že personál, ktorý má prístup k citlivým informáciám má na to aj príslušné oprávnenia.

Physical security (fyzická bepečnosť)

Použitie fyzických prekážok a kontrolných procedúr ako preventívnych opatrení a protiopatrení proti hrozbám voči zdrojom a citlivej informácii.

Privacy (súkromie)

(1) Schopnosť jednotlivca alebo organizácie kontrolovať zberanie, uchovávanie, zdieľanie a šírenie informácie o svojej osobe alebo organizácii.

(2) Právo jednotlivca na ochranu informácie osobného charakteru a na definovanie oprávnených používateľov tejto informácie a spôsobu jej použitia

Privilege (privilégium)

Špeciálne oprávnenie, pridelené konkrétnemu používateľovi na vykonávanie bezpečnostne relevantných operácií.

Profile (profil)

Podrobný bezpečnostný popis fyzickej štruktúry, komponentov, umiestnenia, vzťahov, a všeobecného operačného prostredia systému.

Recovery procedures (procedúry obnovy)

Činnosti potrebné na obnovu výpočtových kapacít systému a dátových súborov po zlyhaní systému.

Reliability (spoľahlivosť)

Rozsah v ktorom sa dá očakávať že systém plní svoje funkcie s požadovanou presnosťou.

Resource (zdroj)

Čokoľvek, čo sa používa alebo spotrebováva pri plnení funkcie.

Risk (riziko)

Očakávaná strata následkom uskutočnenia hrozby zohľadňujúca zraniteľnosti systému a útočný potenciál nositeľa hrozby.

Risk management (manžment rizík)

Celkový proces identifikácie, riadenia, eliminácie alebo minimalizácie neurčitých udalostí, ktoré môžu mať vplyv na zdroje systému. Zahŕňa analýzu rizík, analýzu cost-benefit, výber, implementáciu a testovanie, evaluáciu bezpečnosti opatrení a celkové posúdenie bezpečnosti.

Role (rola)

Definovaný súbor funkčne príbuzných operácií a oprávnení potrebných na vykonávanie týchto operácií, ktoré môžu byť priradené používateľovi.

Secure state (bezpečný stav)

Podmienka, za ktorej žiaden subjekt nemôže pristúpiť k nejakému objektu neoprávneným spôsobom.

Security target (bezpečnostný zámer)

Produktovo špecifický popis, rozpracovávajúci všeobecnejšie požiadavky z protection profile zahŕňajňajúci informácie/svedectvá výrobcov o tom, ako systém/produkt spĺňa požiadavky protection profile.

Security testing (testovanie bezpečnosti)

Proces, ktorý sa používa na overenie toho, že bezpečnostné rysy systému sú implementované v súlade s návrhom a že sú adekvátne pre predpokladané aplikačné prostredie. Proces zahŕňa ručné testovanie, penetračné testovanie a verifikáciu.

Sensitive information (citlivá informácia)

Informácia, ktorú určila oprávnená autorita a ktorá má byť chránená pred neoprávneným zverejnením, zmenou, stratou alebo zničením, ktoré by prinajmenšom spôsobili znateľnú škodu niekomu alebo niečomu.

Subject (subjekt)

Aktívna entita (osoba, proces alebo zariadenie) ktorá spôsobuje tok informácie medzi objektmi alebo zmeny stavu systému.

Threat (hrozba)

Činnosť alebo udalosť ktorá môže ohroziť bezpečnosť systému.

TOE Security Functions (TSF, bezpečnostné funkcie systému, bezpečnostné jadro systému)

Súbor pozostávajúci z hardvérových, softvérových a firmvérových prostriedkov systému, na ktoré sa možno spoľahnúť pri korektnom presadzovaní bezpečnostnej politiky systému.

Verification (overovanie)

Proces porovnávania dvoch špecifikácií systému rozličnej úrovne za účelom zistenia, či navzájom správne korešpondujú.

Virus (vírus)

Samoreprodukujúci sa zlomyseľný segment programu, ktorý sa sám pripája k aplikácii, alebo inému vykonateľnému komponentu systému a nezanecháva vonkajšie stopy svojej prítomnosti.

Vulnerability (zraniteľnosť)

Bezpečnostná slabina systému, ktoré sa dá použiť na narušenie bezpečnostnej politiky systému.

Príloha B – Základné požiadavky na funkčnosť IS

B.1 Úvod

Aby bolo možné v dostatočnom rozsahu popísať účel aplikácie, je potrebné pochopiť dôvody vzniku jednotlivých požiadaviek. Požiadavky na funkčnosť tohto IS vznikli z dvoch nezávislých zámerov.

Prvým zámerom bolo vytvoriť aplikáciu, ktorá by umožňovala evidenciu informácií o veľkom počte dokumentov – štandardizačných materiálov (ďalej aj „ŠM“) vydaných rôznymi vydavateľmi, ich kategorizáciu a modelovanie vzťahov. V ideálnom prípade by aplikácia mala byť schopná v rámci informácie o ŠM uložiť aj jeden alebo viac súborov – znení ŠM.

Druhým zámerom, motivovaným skúsenosťami z pôsobenia v TK 37 SÚTN, bolo vytvorenie aplikácie na sledovanie štandardizačného procesu pre štandardy schvaľované v ISO/IEC JTC 1 (partnerskej komisii TK 37). Pracovné dokumenty JTC 1 sú členom TK 37 sprístupňované prostredníctvom pomerne neprehľadného systému, kde sú prezentované ako zoznam súborov (za posledný rok bolo týchto súborov len pre subkomisiu SK 02 takmer 700). Tento systém neumožňuje jednoduché vyhľadanie súborov súvisiacich s konkrétnym pripravovaným štandardom, a tým sťažuje sledovanie vývoja konkrétnych štandardov, resp. štandardov v určených oblastiach. Cieľom bolo teda vytvoriť systém, ktorý by za podmienky pravidelného dopĺňania informácií a súborov (zamestnancom SÚTN alebo členmi technickej komisie) umožňoval všetkým členom TK 37 jednoduché sledovanie procesu štandardizácie v oblastiach, za ktoré sú zodpovední.

Keďže systémy, ktoré by realizovali uvedené zámery, by sa do veľkej miery prelínali, bol navrhnutý systém integrujúci uvedenú funkcionalitu. Predpokladá sa, že systém bude implementovaný v rámci záverečných prác študenta FMFI (bakalárska a diplomová práca), preto je pri návrhu požiadaviek zohľadnený aj tento faktor (viď kapitolu *B.7 Možnosť vývoja aplikácie vo viacerých etapách*).

Aplikácia by mala umožňovať prístup k údajom prostredníctvom internetového prehliadača (tenký klient). Vzhľadom na určenie aplikácie nie je potrebné zhotovovať samostatnú aplikáciu na prístup k údajom (tučného klienta).

Aplikácia by mala byť vyvíjaná na platforme Microsoft .NET Framework 2.0 s použitím ASP.NET 2.0, ako databázový server by mal slúžiť Microsoft SQL Server 2005. V prípade potreby je možné použiť novšie verzie, resp. rozšírenia.

B.2 Aplikované štandardy a kompatibilita s prehliadačmi

Aplikácia by mala byť v súlade nasledujúcimi špecifikáciami:

- W3C XHTML 1.0 Strict
- W3C CSS 2.1

Aplikácia by taktiež mala vyhovovať požiadavkám W3C WCAG 1.0 priority 1 do takej miery, ako to umožňuje použitý framework.

Generované stránky by sa mali správne zobrazovať v najrozšírenejších webových prehliadačoch, t.j.:

- Microsoft Internet Explorer 6.0
- Windows Internet Explorer 7.0
- Mozilla Firefox 2.0

B.3 Štandardizačný materiál

Pod ŠM rozumieme akýkoľvek jednotlivý publikovaný štandardizačný dokument (napr. normu), prípadne štandardizačný dokument o ktorom sa predpokladá, že sa stane publikovaným[16] (napr. norma v procese tvorby). Každý ŠM má nejaké základné vlastnosti, napr.:

- Označenie (číslo)
- Názov
- Dátum vydania
- Počet strán
- Abstrakt

V čase tvorby tohto dokumentu nie sú identifikované ďalšie vlastnosti ŠM, avšak architektúra aplikácie by mala umožňovať v budúcnosti doplniť alebo zmeniť vlastnosti ŠM tak, aby boli zásahy do kódu boli vykonávané iba na minimálnom počte ucelených úsekov kódu.

Každý ŠM by mal byť zaradený v jednej alebo viacerých kategóriách, pričom kategorizácia by mala byť vykonávaná podľa viacerých kritérií. Podrobnejšie informácie o kategóriách ŠM sú uvedené v kapitole *B.4 Kategórie* štandardizačných materiálov.

[16] Nie je smerodajné, či je publikovaný verejne, alebo v rámci uzatvorenej skupiny používateľov.

Niektoré ŠM sú s inými ŠM prepojené. Aplikácia by mala umožňovať evidenciu vzájomných vzťahov ŠM. Podrobnejšie informácie sú uvedené v kapitole *B.5 Vzťahy medzi* štandardizačnými materiálmi.

V závislosti na autorovi ŠM prechádzajú ŠM rôznymi procesmi tvorby a pripomienkovania. Aplikácia by mala podporovať sledovanie tohto procesu. Podrobnejšie sú požiadavky uvedené v kapitole *B.6 Podpora procesu* vývoja .

Aplikácia by mala umožňovať vyhľadávanie v ŠM v rozsahu evidovaných atribútov.

B.4 Kategórie štandardizačných materiálov

Veľmi dôležitou funkciou, ktorú má plniť aplikácia na evidenciu ŠM je možnosť kategorizovať ŠM podľa zvolených kritérií. Príkladmi kritérií, podľa ktorých môžu byť ŠM kategorizované sú:

- Podľa vydavateľa:
    - ISO,
    - IEC,
    - ISO/IEC,
    - SÚTN,
    - BSI,
    - DIN,
    - …
- V prípade niektorých vydavateľov podľa komisie zodpovednej za vývoj normy
- Podľa záväznosti ŠM, napr.:
    - EN – európska norma – členské štáty sú povinné ŠM prevziať do 6 mesiacov od vydania,
    - aplikácia normy vyplýva z právnych predpisov SR alebo EÚ,
    - podľa normy je možná certifikácia organizácie/produktu (napr. ISO/IEC 27001),
    - súhrn odporúčaní „best practices“ (napr. ISO/IEC 17799),
- Podľa obsahového zamerania, napr.:
    - riadenie informačnej bezpečnosti,
    - kryptológia,
    - audit,
    - certifikácia systémov (Common Criteria),
    - vývoj systémov,
    - správa systémov,

    - ...,
- Podľa jazyka

Systém musí byť vyvinutý tak, aby umožňoval pridanie, zmenu alebo odobratie kritéria a kategórie v rámci jedného kritéria. Zmazanie nesmie spôsobiť inkonzistenciu v databáze. V prípade zmeny/vymazania používaného kritéria alebo kategórie musí používateľ na túto skutočnosť byť upozornený pred potvrdením zmazania. Upozornenie musí obsahovať počet ŠM, ktorých sa zmena/vymazanie dotkne.

B.5 Vzťahy medzi štandardizačnými materiálmi

Aplikácia by mala podporovať definíciu vzťahov medzi ŠM. Vzťah ŠM je popísaný nasledujúcimi atribútmi:

- Kategória vzťahu
- Štandardizačný materiál
- Štandardizačný materiál

Kategórie vzťahov by mali okrem mena, príp. krátkeho popisu definovať aj „orientáciu vzťahu“ so sémantikou ako v teórii grafov, t.j., vzťahy môžu byť dvoch druhov:

- „neorientované“, pri ktorých nezáleží na poradí, v ktorom sú ŠM uvedené (napr. vzťahy „súvisí s“, „koliduje s“),
- „orientované“, pri ktorých záleží na poradí, v ktorom sú ŠM uvedené (napr. vzťah „nahrádza“).

Aplikácia by mala umožňovať definovanie nových kategórií vzťahov, úpravu a zmazanie existujúcich kategórií vzťahov. Zmazanie nesmie spôsobiť inkonzistenciu v databáze, t.j. zmazanie kategórie spôsobí zmazanie všetkých vzťahov zmazanej kategórie. V prípade zmeny/vymazania používanej kategórie vzťahov musí používateľ na túto skutočnosť byť upozornený pred potvrdením zmazania. Upozornenie musí obsahovať počet vzťahov/ŠM, ktorých sa zmena/vymazanie dotkne.

B.6 Podpora procesu vývoja štandardizačných materiálov

Aplikácia by mala umožňovať zadefinovať rôzne typy ŠM odlišujúce sa rôznymi procesmi ich tvorby. Proces vývoja ŠM je definovaný:

- jednotlivými etapami označenými názvom a voliteľne kódom,
- definíciami možných prechodov medzi etapami,
- definíciou aspoň jednej možnej počiatočnej etapy procesu,

- definíciou aspoň jednej možnej konečnej etapy procesu; nie všetky konečné etapy znamenajú publikovaný štandard (tzn. štandard bol odmietnutý).

Jednotlivé etapy by mali mať okrem názvu mať možnosť doplnenia poznámky, napr. o štandardnej dĺžke trvania etapy. Pri zaradení ŠM do niektorej z etáp by malo byť možné určiť predpokladaný dátum ukončenia etapy, aby bolo možné sledovať ďalší vývoj štandardizačného procesu. V prípade potreby by malo byť možné dátum ukončenia etapy zmeniť. O každej etape v rámci konkrétneho ŠM by tiež malo byť možné doplniť poznámku o priebehu etapy, ako aj dátumy reálneho začatia a ukončenia.

Pre každú etapu je možné vložiť jeden alebo viac súborov, ktoré s ňou súvisia (napr. pracovné verzie ŠM, prílohy, súhrn pripomienok, vyjadrenia k pripomienkam). Aplikácia by preto mala umožňovať ukladanie ľubovoľných súborov. Pre každý súbor by mali byť evidované niektoré vlastnosti, ako napr.:

- Dátum vytvorenia súboru
- Názov súboru
- Autor
- Popis obsahu súboru
- ...

B.7 Možnosť vývoja aplikácie vo viacerých etapách

Nakoľko sa predpokladá postupný vývoj aplikácie, významnou požiadavkou je možnosť dekomponovať jednotlivé funkcie systému do takých celkov, aby bolo možné aplikáciu využívať aj bez dostupnosti ostatných funkcií. Pri tvorbe architektúry aplikácie je však nutné zohľadniť aj funkcie, ktoré budú implementované aj v budúcnosti.

V prvej etape je potrebné realizovať všetky funkcie uvedené v tomto dokumente s výnimkou kapitoly *B.6 Podpora procesu vývoja* .

Následne je možné doplniť funkcie popísané v kapitole *B.6 Podpora procesu vývoja* , prípadne niektoré z nasledujúcich doplnkových funkcií:

- fulltextové vyhľadávanie vo vlastnostiach ŠM a obsahu externých súborov;
- N-árne vzťahy, čím by sa umožnilo vytvárať aj akési skupiny ŠM tak, že bude zachovaná konzistencia z pohľadu každého ich člena (napr. rodiny štandardov, ako sú PKCS, ISO/IEC 13335 alebo BS 25999);
- vytváranie vzťahov aj na dokumenty externé vzhľadom k ŠM (napr. právne predpisy, medzinárodné zmluvy, …);

- e-mailová notifikácia udalostí (napr. zaslanie emailu vlastníkovi ŠM v čase predpokladaného ukončenia etapy).

B.8 Bezpečnostné požiadavky na systém

B.8.1 Prístupové práva používateľov

Aplikácia by mala umožňovať riadenie prístupu používateľov, na autentifikáciu je postačujúce použitie hesla.

Vzhľadom na predpokladaný rozsah využitia aplikácie (v rámci technickej komisie SÚTN) sa nepredpokladá využitie veľkým počtom používateľov. To umožňuje ponechať komplexnosť subsystému na riadenie prístupu na relatívne nízkej úrovni. Pri návrhu architektúry systému je však vhodné predpokladať, že v budúcnosti môžu byť požiadavky na riadenie prístupu rozšírené (napr. o vnáranie skupín).

O používateľoch by mali byť evidované základné informácie, ako sú:

- meno,
- organizácia,
- kontaktné údaje (e-mailová adresa, telefónne číslo).

Používatelia s rovnakými požiadavkami na prístupové oprávnenia môžu byť združení v skupine. Skupina je charakterizovaná názvom a popisom. Jeden používateľ nemusí byť zaradený do žiadnej skupiny a môže byť členom ľubovoľného počtu skupín. Skupina nesmie obsahovať inú skupinu.

Pre jednotlivé roly v systéme je možné prideľovať prístupové práva jednotlivým používateľom alebo skupinám, pokiaľ nie je v špecifikácii uvedené inak. V rámci systému by mali byť zadefinované nasledujúce roly:

- administrátor aplikácie (používateľ s oprávneniami na všetky činnosti, vrátane konfigurácie systému a prehliadanie auditných záznamov),
- správca používateľov (používateľ s oprávneniami na všetky činnosti súvisiace so správou používateľov, ako je ich vytváranie, zmena atribútov, uzamknutie, …),
- kontrolný používateľ (používateľ s oprávneniami na prehliadanie auditných záznamov)
- správca obsahu (používateľ s oprávneniami čítať, meniť a rušiť akýkoľvek ŠM, kategóriu, vzťah, …),
- tvorca obsahu (používateľ s oprávneniami vytvoriť nový ŠM).

Každý ŠM môže mať zadefinovaného jedného vlastníka – osobu zodpovednú za správnosť a aktuálnosť evidovaných informácií. V prípade štandardu v procese tvorby je vlastníka možné považovať aj za projektového manažéra. Vlastníkom ŠM sa pri vytvorení stáva používateľ, ktorý ŠM vytvoril. V prípade potreby môže vlastníctvo ŠM zmeniť aktuálny vlastník ŠM, administrátor aplikácie a správca obsahu.

Jednotlivé ŠM môžu taktiež mať definovaných niekoľkých členov projektového tímu (používateľov alebo skupiny používateľov). Členstvo v projektovom tíme môže určiť vlastník ŠM, administrátor aplikácie a správca obsahu.

Prístupové oprávnenia súvisiace s daným ŠM by malo byť možné nastaviť pre nasledujúce operácie:

- zobrazenie základných informácií o ŠM a vybraných informácií o etapách (dátumy začatia a predpokladaného skončenia prebiehajúcej etapy, dátumy začatia a ukončenia etapy),
- zobrazenie poznámok k etapám,
- zobrazenie súborov priložených ku konečnej etape,
- zobrazenie súborov priložených ku všetkým etapám,
- úprava základných informácií o ŠM,
- úprava informácií aktuálnej etape (dátumy, poznámky),
- vytvorenie novej etapy, úprava informácií o všetkých etapách (dátumy, poznámky),
- priloženie súboru k aktuálnej etape,
- správa súborov priložených ku všetkým etapám.

Prístupové práva na jednotlivé operácie so ŠM by malo byť možné prideľovať nasledujúcim typom používateľov:

1. Vlastník ŠM (VŠM),
2. Členovia projektového tímu (ČPT),
3. Autentifikovaní používatelia (AP),
4. Neautentifikovaní používatelia (NAP).

Každý z uvedených typov zahŕňa aj všetky typy používateľov uvedené s nižším poradovým číslom (napr. typ používateľov *Prihlásení používatelia* zahŕňa aj typy používateľov *Vlastník ŠM* a *Členovia projektového tímu*).

Prístupové práva k ŠM by mať možnosť mali upravovať iba vlastník ŠM, administrátor aplikácie a správca obsahu, a to pre každú operáciu jednotlivo. Aby bolo riadenie prístupu zjednodušené, aplikácia by mala umožňovať vytvorenie štandardných profilov pre prístup

k ŠM, z ktorých bude možné jednoducho zvoliť. Ako príklad možných prístupových profilom môže poslúžiť nasledujúca tabuľka.

	Prístupový profil		
Operácia so ŠM	**ŠM – vývoj 1**	**ŠM – vývoj 2**	**ŠM uzamknutý verejný**
Zobrazenie základných informácií o ŠM a vybraných informácií o etapách	NAP	AP	NAP
Zobrazenie poznámok k etapám	ČPT	ČPT	ČPT
Zobrazenie súborov priložených ku konečnej etape	ČPT	ČPT	NAP
Zobrazenie súborov priložených ku všetkým etapám	ČPT	ČPT	ČPT
Úprava základných informácií o ŠM	ČPT	VŠM	VŠM
Úprava informácií aktuálnej etape (dátumy, poznámky)	ČPT	VŠM	VŠM
Vytvorenie novej etapy, úprava informácií o všetkých etapách (dátumy, poznámky),	VŠM	VŠM	VŠM
Priloženie súboru k aktuálnej etape,	ČPT	ČPT	VŠM
Správa súborov priložených ku všetkým etapám.	VŠM	VŠM	VŠM

Rozhranie aplikácie by nemalo zobrazovať ovládacie prvky, na ktorých použitie používateľ nemá dostatočné oprávnenia. V prípade, že sa používateľ aj napriek tomu pokúsi vykonať nepovolenú operáciu (napr. zadaním URL), operácia nesmie byť vykonaná, systém by mal ponúknuť možnosť prihlásiť sa pod používateľským účtom.

B.8.2 Vytváranie auditných záznamov

Aplikácia by mala mať možnosť ukladať záznamy o jej využívaní. Jedná sa o nasledujúce udalosti:

- úspešné a neúspešné prihlásenie používateľa,
- vytvorenie, zmena alebo zmazanie objektu (ŠM, kategória, používateľ, ...),
- zmena vlastníka ŠM,
- zmena prístupových práv k ŠM,
- pokus o vykonanie nepovolenej operácie,
- zmena konfigurácie prostredníctvom rozhrania aplikácie.

Pri všetkých udalostiach by mali byť zaznamenané všetky relevantné údaje potrebné pre prípadnú rekonštrukciu udalostí, minimálne však:

- Poradové číslo udalosti

- Dátum a čas
- IP klienta
- ID používateľa (ak je k dispozícii)
- Typ udalosti, popis
- ID súvisiacich objektov (ŠM, používateľ, pôvodný a nový vlastník ŠM...)

Prostredie by malo umožňovať jednoduché vyhľadávanie v auditných záznamoch, a to podľa všetkých relevantných atribútov.

Zmena alebo zmazanie auditných záznamov by nemali byť povolené ani administrátorom systému.

B.8.3 Bezpečnostné požiadavky webovej aplikácie

Vzhľadom na známe hrozby pôsobiace na webové aplikácie je v systéme potrebné zabezpečiť implementáciu dodatočných bezpečnostných prvkov zaisťujúcich ochranu pred týmito hrozbami. Jedná sa najmä o ochranu pred útokmi cross-site scripting, session hijack a SQL injection.

Príloha C – Prístup NIST ku kategorizácii štandardov podľa zamerania

Audit & Accountability	**Audit a sledovateľnosť**
A collection of documents that relates to review and examination of records and activities in order to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to provide the supporting requirement for actions of an entity to be traced uniquely to that entity.	Súbor dokumentov súvisiacich s preskúmavaním záznamov a činnosťami vykonávanými za účelom ohodnotenia primeranosti systémových opatrení. Ich cieľom je zabezpečenie súladu so zavedenými politikami a prevádzkovými procedúrami a zabezpečenie možnosti sledovania činností jednotlivých entít.
Authentication	**Autentifikácia**
Awareness & Training	**Povedomie a vzdelávanie v oblasti bezpečnosti**
Biometrics	**Biometria**
A collection of documents that details security issues and potential controls using a measurable, physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of a person.	Súbor dokumentov popisujúcich bezpečnostné otázky a potenciálne opatrenia používajúce merateľné fyzické charakteristiky alebo zvláštne rysy správania používané na zistenie identity alebo overenie deklarovanej identity osoby.
Certification & Accreditation (C&A)	**Certifikácia a akreditácia IS**
Certification and Accreditation (C&A) is a collection of documents that can be used to conduct the C&A of an information system in accordance with OMB A130-III.	Je súbor dokumentov ktoré možno použiť na vykonanie certifikácie a akreditácie informačných systémov v súlade s pravidlami stanovenými OMB A130-III.

Communications & Wireless

A collection of documents that details security issues associated with the transmission of information over multiple media to include security considerations with the use of wireless.

Komunikácie a bezdrôtové siete

Súbor dokumentov popisujúcich bezpečnostné aspekty spojené s prenosom informácií prostredníctvom rôznych typov médií, zohľadňujúc bezpečnostné aspekty spojené s použitím bezdrôtových technológií.

Contingency Planning

A collection of documents that details management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster.

Plánovanie kontinuity činností

Súbor dokumentov popisujúcich politiku a procedúry vytvorené za účelom udržania alebo obnovy obchodných činností, vrátane počítačových operácií, potenciálne na alternatívnom mieste, v prípade poruchy systému, mimoriadnej udalosti alebo živelnej pohromy.

Cryptography

A collection of documents that discusses the multiple uses and security issues of encryption, decryption, key management, and the science and technologies used to assure the confidentiality of information by hiding semantic content, preventing unauthorized use, or preventing undetected modification.

Kryptografia

Súbor dokumentov, ktorý rozoberá rôzne použitie a bezpečnostné otázky šifrovania, dešifrovania, manažmentu kľúčov a vedu a technológie na zaistenie dôvernosti informácie skrytím sémantického kontextu a znemožnenie neautorizovaného použitia alebo neodhaliteľnej modifikácie informácie.

Digital Signatures

A collection of documents that discusses the multiple uses and security issues of digital signatures.

Digitálny podpis

Súbor dokumentov rozoberajúcich rôzne použitie a bezpečnostné otázky digitálnych podpisov.

Forensics

A collection of documents that discusses the practice of gathering, retaining, and analyzing computer-related data for investigative purposes in

a manner that maintains the integrity of the data.

Vyšetrovanie

Súbor dokumentov popisujúcich postupy zhromažďovania, uchovávania a analyzovania údajov z automatizovaných systémov za účelom vyšetrovania a to tak, aby bola zachovaná integrita informácií.

General IT Security

A collection of documents that spans multiple topic areas and covers a very broad range of security subjects. These documents are not typically listed in Topic Clusters because they are generally applicable to almost all of them.

Všeobecné aspekty bezpečnosti IT

Súbor dokumentov, ktoré zahŕňajú rôzne predmetné oblastí a pokrývajú veľmi široký rozsah bezpečnostných otázok. Tieto dokumenty nebývajú zaradené do tematických skupín, pretože sú spravidla aplikovateľné na väčšinu z nich.

Incident Response

A collection of documents to assist in the creation of a pre-determined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber attack against an organization's IT system(s).

Reakcia na bezpečnostné incidenty

Súbor dokumentov pomáhajúcich pri vytváraní preddefinovanej množiny inštrukcií alebo procedúr na zistenie, reakciu na a obmedzenie dopadov rôznych typov narušenia bezpečnosti IT systémov organizácií.

Maintenance

A collection of documents discussing security concerns with systems in the maintenance phase of the System Development Life Cycle.

Údržba

Súbor dokumentov rozoberajúcich bezpečnostné otázky týkajúce sa systémov, ktoré sú v rámci životného cyklu vo fáze údržby.

Personal Identity Verification (PIV)

Personal Identity Verification (PIV) is a suite of standards and guides that are developed in response to HSPD-12 for improving the identification and authentication of Federal employees and contractors for access to Federal facilities and information systems.

Overovanie identity osôb

Súbor štandardov a návodov, ktoré sú vyvinuté v súvislosti s HSPD-12 na zlepšenie identifikácie a autentifikácie štátnych zamestnancov a zamestnancov dodávateľov pri prístupe do priestorov a informačných systémov štátnych inštitúcií..

PKI

A collection of documents to assist with the understanding of Public Key cryptography.

Infraštruktúra verejných kľúčov (PKI)

Súbor dokumentov pomáhajúcich pri pochopení kryptografie verejných kľúčov.

Planning

A collection of documents dealing with security plans and for identifying, documenting, and preparing security for systems.

Plánovanie

Súbor dokumentov zaoberajúcich sa bezpečnostnými plánmi a identifikáciou, dokumentovaním a prípravou bezpečnostných opatrení pre systémy.

Risk Asessment

A collection of documents that assists in identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact.

Ohodnotenie rizík

Súbor dokumentov, pomáhajúcich pri identifikácii rizík vplývajúcich na činnosť organizácie (napr. ohrozenie poslania, funkcií, obrazu alebo dobrého mena), aktív organizácie alebo jednotlivcov. Ohodnotenie rizík pozostáva z určenia miery pravdepodobnosti výskytu, rozsahu dopadov rizika a možných opatrení na zníženie týchto dopadov.

Services & Acquisitions

A collection of documents to assist with understanding security issues concerning purchasing and obtaining items. Also covers considerations for acquiring services, including assistance with a system at any point in its life cycle, from external sources.

Akvizícia systémov a súvisiacich služieb

Súbor dokumentov pomáhajúcich pri chápaní bezpečnostných otázok spojených s akvizíciou nových systémov. Taktiež pokrývajú oblasť obstarávania služieb od tretích strán, vrátane služieb podpory pre systém v ktorejkoľvek fáze životného cyklu.

Smart Cards	**Smart karty**
A collection of documents that provides information on cards with built-in microprocessors and memory that can be used for identification purposes.	Súbor dokumentov poskytujúcich informácie o kartách so vstavaným mikroprocesorom a pamäťou (smart kariet), ktoré môžu byť použité za účelom identifikácie osôb.
Viruses & Malware	**Vírusy a škodlivý softvér**
A collection of documents that deals with viruses, malware, and how to handle them.	Súbor dokumentov zaoberajúcich sa vírusmi a škodlivým softvérom a spôsobmi, ako sa pred nimi chrániť.