Standardi in priporočila na področju informacijske varnosti

Alenka Brezavšček
Univerza v Mariboru, Fakulteta za organizacijske vede, Kidričeva cesta 55a, 4000 Kranj
alenka.brezavscek@fov.uni-mb.si
Lucija Zupan
HERMES SoftLab, d. d., Litijska 51, 1000 Ljubljana
lucija.zupan@hermes.si

Povzetek

V prispevku so opredeljeni standardi in priporočila s področja zagotavljanja informacijske varnosti, ki se v praksi najbolj pogosto uporabljajo. Podrobneje je predstavljen standard BS 7799, ki je po novem sestavljen iz treh delov. Zgoščeno so podane spremembe, ki jih prinašata zadnji izdaji prvih dveh delov tega standarda, in sicer BS ISO/IEC 17799:2005 ter BS ISO/IEC 27001:2005. Opredeljeni so tudi možni vplivi teh sprememb na organizacije, ki so svoje sisteme za upravljanje informacijske varnosti (SUIV) oblikovale na osnovi prejšnjih verzij standarda BS 7799. Opisano je tudi, katere standarde s področja zagotavljanja informacijske varnosti lahko organizacije pričakujejo v bližnji prihodnosti.

Ključne besede: informacijska varnost, standardi, priporočila, BS 7799, BS ISO/IEC 17799:2005, BS ISO/IEC 27001:2005, BS 7799-3:2006

Abstract

Information security standards and guidelines

In the paper, the information security standards and guidelines are quoted. The standard BS 7799 that currently consists of three parts is described in detail. Modifications in the latest versions of the first two parts of this standard (BS ISO/IEC 17799:2005 and BS ISO/IEC 27001:2005) are briefly presented. The authors also discuss possible impact of these modifications on the organizations that have developed their information security management systems (ISMS) on the basis of the previous versions of the standard BS 7799. Besides, the article describes what the organizations can expect in the field of the information security standardization in the near future.

Keywords: Information security, standards, guidelines, BS 7799, BS ISO/IEC 17799:2005, BS ISO/IEC 27001:2005, BS 7799-3:2006

1 Uvod

Področje zagotavljanja informacijske varnosti je eno najbolj perečih področij v zadnjem času. Primer SKB je v Sloveniji povzročil znatno spremembo v vedenju in razmišljanju tako med uporabniki storitev kakor tudi med vodstvenimi kadri. Iz dneva v dan se povečujejo tudi pritiski regulative, zato so organizacije prisiljene oblikovati učinkovit sistem varovanja informacij.

Varovanje informacij ni preprosta naloga, saj obsega številna področja, ki jih moramo skrbno spremljati, da bi preprečili morebitno škodo. Poznavanje ustreznih standardov in priporočil igra pri tem pomembno vlogo, saj nam uporaba takih dokumentov omogoča vpeljavo preizkušene prakse ter uvedbo celovitega in sistematičnega pristopa pri zagotavljanju informacijske varnosti v organizaciji. Ne nazadnje uporabo standardov s področja informacijske varnosti narekujejo tudi zahteve po poslovni odličnosti, ki so lahko predmet interne poslovne politike ali pa so postavljene s strani zunanjih poslovnih partnerjev.

Na področju zagotavljanja informacijske varnosti so se bolj ali manj uveljavili številni standardi in priporočila. Množica teh dokumentov se iz leta v leto še povečuje, kar med uporabniki pogosto povzroča zmedo. Slednje otežuje obvladovanje že vpeljanih standardov, zahteva njihovo neprestano vzdrževanje v skladu s spremembami procesov, kar posledično povzroča organizaciji stroške. Dobra praksa narekuje uvedbo komplementarnih standardov, ki se medsebojno dopolnjujejo in omogočajo celovito pokritje področij. Zato se organizacije pogosto znajdejo pred vprašanjem, ali je bolje uvesti najprej ITIL ali COBIT, ISO 9001 ali BS 7799, ali preprosto uporabljati stare načine dela, preizkušene prakse, ki

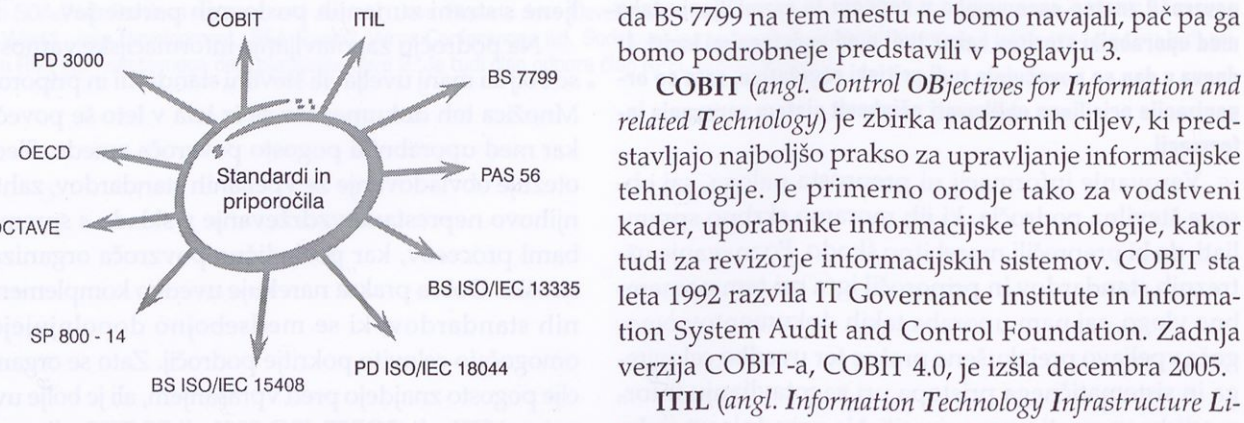
ne zahtevajo prilagoditve procesov in sprememb obstoječih načinov dela.

V pričujočem prispevku bomo na kratko predstavili standarde in priporočila s področja informacijske varnosti, ki se po našem mnenju v praksi najpogosteje uporabljajo. Podrobneje bomo opisali standard BS 7799, ki je eden izmed najbolj celovitih dokumentov na področju zagotavljanja informacijske varnosti. Po novem je standard BS 7799 sestavljen iz treh delov: BS ISO/IEC 17799:2005, BS ISO/IEC 27001:2005 in BS 7799-3:2006. Strukturirano bomo predstavili spremembe, ki jih prinašata najnovejši izdaji prvih dveh delov tega standarda. Preučili bomo vpliv teh sprememb na organizacije, ki so svoje sisteme za upravljanje informacijske varnosti zasnovale na prejšnjih verzijah standarda BS 7799. Navedli bomo tudi, katere standarde s področja zagotavljanja informacijske varnosti lahko organizacije pričakujejo v prihodnjih letih.

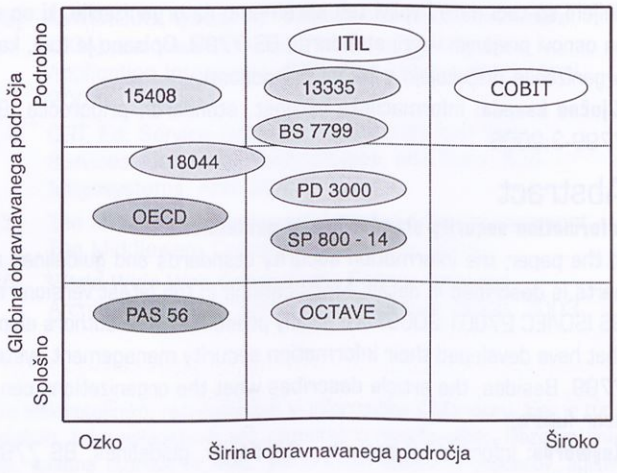
2 Standardi in priporočila na področju informacijske varnosti v praksi

Množica standardov, priporočil in drugih dokumentov, ki v širšem ali v ožjem smislu obravnavajo področje zagotavljanja informacijske varnosti, je precej obsežna. Na sliki 1 so navedeni tisti dokumenti, ki so se v praksi najbolj uveljavili in se po našem mnenju najpogosteje uporabljajo.

Dokumenti, navedeni na sliki 1, lahko služijo organizacijam kot pripomoček pri oblikovanju sistema za upravljanje informacijske varnosti (v nadaljevanju SUIV). Med seboj se razlikujejo glede na širino in globino področja, ki ga posamezen dokument obravnava. Nekateri od naštetih dokumentov so bolj splošne narave in pokrivajo širše področje zagotavljanja varnosti, medtem ko so drugi specializirani in podrobno obravnavajo določen, specifičen segment zagotavljanja varnosti. Razvrstitev dokumentov glede na širino in globino obravnavanega področja je shematično prikazana na sliki 2. Nekateri od dokumentov, ki so navedeni na sliki 2, so uveljavljeni mednarodni standardi, drugi predstavljajo izkušnje najboljše prakse, tretji pa so zgolj priporočila ali smernice, ki jih posamezne organizacije priporočajo. Različne statuse dokumentov smo v sliki 2 skušali ponazoriti z različnimi odtenki sivih barv.



Slika 1: **Standardi in priporočila na področju informacijske varnosti, ki se v praksi najpogosteje uporabljajo**



Slika 2: **Razvrstitev dokumentov na področju informacijske varnosti glede na status dokumenta ter glede na širino in globino obravnavanega področja**

V nadaljevanju bomo vsakega od dokumentov, navedenih na slikah 1 in 2, na kratko opisali. Standarda BS 7799 na tem mestu ne bomo navajali, pač pa ga bomo podrobneje predstavili v poglavju 3.

COBIT (*angl. Control OBjectives for Information and related Technology*) je zbirka nadzornih ciljev, ki predstavljajo najboljšo prakso za upravljanje informacijske tehnologije. Je primerno orodje tako za vodstveni kader, uporabnike informacijske tehnologije, kakor tudi za revizorje informacijskih sistemov. COBIT sta leta 1992 razvila IT Governance Institute in Information System Audit and Control Foundation. Zadnja verzija COBIT-a, COBIT 4.0, je izšla decembra 2005.

ITIL (*angl. Information Technology Infrastructure Library*) predstavlja zbirko najboljše prakse za upravljanje informacijskih storitev. Nastal je v osemdesetih

letih v Angliji pod okriljem Central Computer and Telecommunications Agency – CCTA. Danes skrbi za nadaljnji razvoj ITIL-a Office of Government Commerce – OCG. V drugi polovici leta 2006 se pričakuje izid prenovljene verzije ITIL-a – ITILv3.

BS ISO/IEC 13335 (*angl. Information Technology – Gudelines for the Management of IT Security*) je standard, v katerem so zbrane smernice za upravljanje varovanja informacijske tehnologije. Sestavljen je iz petih delov:

- BS ISO/IEC 13335-1:2004
  Koncepti in modeli za varovanje informacijske tehnologije
- BS ISO/IEC 13335-2:1997
  Upravljanje in načrtovanje varovanja informacijske tehnologije
- BS ISO/IEC 13335-3:1998
  Tehnike za upravljanje varovanja informacijske tehnologije
- BS ISO/IEC 13335-4:2000
  Izbira varovalnih ukrepov
- BS ISO/IEC 13335-5:2001
  Navodila za varovanje omrežij

PD ISO/IEC TR 18044:2004 (*angl. Information Technology, Security Techniques, Information Security Incident Management*) je standard, ki pokriva področje upravljanja incidentov[1] pri varovanju informacij. Namenjen je predvsem skrbnikom informacijskih sistemov in skrbnikom za informacijsko varnost.

ISO/IEC 15408 (*angl. Information Technology, Security Techniques, Evaluation Criteria for IT Security)* predpisuje kriterije za vrednotenje varnosti informacijske tehnologije. Standard je namenjen trem ciljnim skupinam: uporabnikom, načrtovalcem in presojevalcem informacijskih sistemov. Prenovljena različica standarda ISO/IEC 15408 je izšla leta 2005 v naslednjih treh delih:

- ISO/IEC 15408-1:2005
  Predstavitev in splošni model
- ISO/IEC 15408-2:2005
  Funkcionalne zahteve varnosti
- ISO/IEC 15408-3:2005
  Zahteve zagotavljanja varnosti

PAS 56 (*angl. Guide to Business Continuity Management*) je vodnik za upravljanje neprekinjenega poslovanja, ki ga je leta 2002 izdal The Busines Continuity Institute pod okriljem BSI (British Standards Institution). Kratica PAS pomeni, da gre za javno dostopne specifikacije (*angl. Public Available Specifications*).

PD 3000 je serija petih vodnikov, ki nudijo uporabnikom pomoč pri vzpostavitvi in vzdrževanju SUIV v organizaciji. Serija obsega naslednje vodnike:

- PD 3001
  Priprava na certificiranje po BS 7799-2
- PD 3002
  Vodnik za oceno tveganja po BS 7799
- PD 3003
  Ste pripravljeni na presojo po BS 7799-2?
- PD 3004
  Vodnik za vzpostavitev in presoje kontrol BS 7799
- PD 3005
  Vodnik za izbiro kontrol BS 7799-2

Serijo PD 3000 je leta 2002 izdal BSI – British Standards Institution.

SP 800-14 je dokument, ki zajema splošno sprejete koncepte in prakse za varovanje informacijskih sistemov. SP 800-14 je eden izmed številnih prosto dostopnih dokumentov s področja zagotavljanja informacijske varnosti, ki jih v seriji posebnih publikacij SP 800[2] izdaja ameriški inštitut NIST – National Institute of Standard and Tehnology.

OCTAVE (*angl. Operationally Critical Threat, Asset, and Vulnerability Evaluation*) je prosto dostopna metodologija za strateško planiranje zagotavljanja varnosti na podlagi ocenjevanja varnostnih tveganj.[3]

OECD (*angl. Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*) so prosto dostopne smernice za varovanje informacijskih sistemov in omrežij, ki jih je izdala organizacija OECD – Organisation for Economic Co-operation and Development.[4] Prvotno so bile namenjene vladnim institucijam, ki so pričele z uvajanjem e-uprave. Organizacije lahko smernice OECD koristno uporabijo predvsem v začetnih fazah vzpostavitve SUIV. Za organizacije, ki imajo glede zagotavljanja informacijske varnosti visoke zahteve, pa smernice OECD niso najbolj primerne.

Poleg naštetih dokumentov lahko v strokovni literaturi zasledimo tudi številne standarde, priporočila in smernice, ki obravnavajo ozka strokovna področja

---

[1] *Pod pojmom »incident« razumemo uresničitev kakršnegakoli dogodka, ki negativno vpliva na zaupnost, celovitost ali razpoložljivost informacij oziroma drugih dobrin informacijskega sistema. Takim dogodkom pravimo grožnje varnosti.*

[2] *Glej http://csrc.nist.gov/publications/nistpubs/index.html.*

[3] *Glej npr. http://www.cert.org/octave/pubs.html.*

[4] *Glej http://www.oecd.org/document/42/0,2340,en_2649_33703_15582250_1_1_1_1,00.html.*

kot npr. šifriranje podatkov, varovanje komunikacij, preverjanje istovetnosti uporabnikov ipd. Obsežen spisek dokumentov, ki obravnavajo področje zagotavljanja informacijske varnosti, lahko najdemo v spletnem viru [1].

3 Standard BS 7799

Standard BS 7799 je mednarodno uveljavljen standard za varovanje informacij. Predstavlja enega najbolj celovitih dokumentov na tem področju. Prva različica je izšla leta 1995 v Veliki Britaniji. V letih do danes je standard BS 7799 doživel več sprememb. Najnovejšo verzijo standarda BS 7799 sestavljajo trije deli:

- prvi del: BS ISO/IEC 17799:2005
- drugi del: BS ISO/IEC 27001:2005
- tretji del: BS 7799-3:2006

Prvi del standarda BS 7799 obsega priporočila in obsežen nabor nadzorstev,[5] ki predstavljajo najboljšo prakso na področju zagotavljanja informacijske varnosti. Ta del standarda lahko služi kot enotna referenčna točka za izbiro nadzorstev pri vzpostavitvi SUIV in oblikovanju krovne varnostne politike v organizaciji. Prenovljena različica prvega dela standarda je izšla junija 2005 (glej [2]).

Drugi del standarda BS 7799 predstavlja zbirko lastnosti, katerim mora SUIV v organizaciji ustrezati, da je s tem standardom skladen. Organizacije, ki dosegajo določila, navedena v drugem delu standarda BS 7799, lahko pridobijo certifikat skladnosti s standardom. Drugi del standarda BS 7799 temelji na principu PDCA (Plan – Načrtuj, Do – Izvedi, Check – Preveri, Act – Ukrepaj), podobno kot ga uvaja sistem vodenja kakovosti ISO 9001. Princip PDCA pokriva vse faze delovanja SUIV, od njegove vzpostavitve do zrele faze delovanja. Podrobnejši opis posameznih faz SUIV najdemo v članku [3]. Prenovljena različica drugega dela standarda je izšla oktobra 2005 (glej [4]).

Marca 2006 je izšel povsem nov, tretji del standarda BS 7799, ki obravnava področje upravljanja tveganj, povezanih z informacijsko varnostjo (glej [5]). Tretji del standarda BS 7799 predstavlja dopolnilo prvih dveh delov. Nekateri strokovnjaki trdijo, da je BS 7799-3 pravzaprav naslednik vodnika PD 3002.

3.1 Spremembe v novi izdaji prvih dveh delov standarda BS 7799

Z zadnjo prenovo se je standard BS 7799 prilagodil spremembam v poslovnih in drugih okoljih v zadnjih letih. Struktura standarda je preglednejša in razumljivejša, izrazoslovje pa je usklajeno z drugimi standardi in vodniki, ki obravnavajo informacijsko varnost.

Prvi del standarda BS 7799 je bil v prejšnji verziji poimenovan kot BS ISO/IEC 17799:2000 (glej [6]). Prejšnja in sedanja verzija prvega dela BS 7799 se razlikujeta v številu poglavij, njihovemu oštevilčenju in poimenovanju, kakor tudi v strukturi nekaterih podpoglavij. V novi izdaji so dodana tri poglavja, od tega sta dve poglavji uvodni. Preimenovala so se tudi nekatera podpoglavja in nadzorstva. Mnoga preimenovanja ne vplivajo bistveno na samo strukturo prvega dela standarda, saj je vsebina v številnih primerih ostala popolnoma nespremenjena. Nekatera podpoglavja oziroma nadzorstva pa so v novi verziji prvega dela BS 7799 samo prerazporejena v druga poglavja oziroma podpoglavja. Glavna področja sprememb v prvem delu standarda BS 7799 bi lahko strnjeno opredelili:

- spremenjena je struktura standarda,
- dodana so nova nadzorstva,
- nova je struktura in format zapisa posameznega nadzorstva,
- dodatna pozornost je posvečena analizi tveganja,
- poseben poudarek je zaslediti na opredelitvi odgovornosti, povezanih z zagotavljanjem informacijske varnosti.

Drugi del standarda BS 7799 je bil v prejšnji verziji poimenovan kot BS 7799-2:2002 (glej [7]), v novi izdaji pa je ta del izšel pod povsem novim imenom BS ISO/IEC 27001:2005. Oznaka ISO/IEC ponazarja, da gre za mednarodni standard. Zaradi večje prepoznavnosti je nova izdaja drugega dela BS 7799 dvojno poimenovana, in sicer BS 7799-2:2005 in BS ISO/IEC 27001:2005.

V novi izdaji drugega dela standarda BS 7799 je precej sprememb in dodatnih pojasnil, ki se nanašajo na posamezno fazo vzpostavitve SUIV. Več pozornosti je posvečene zagotavljanju dokazov o delovanju takega sistema v organizaciji ter doslednemu merjenju njegove učinkovitosti. Skozi ves prenovljen drugi del pa

[5] *V slovenskih prevodih standarda BS 7799 se v pomenu izraza »control« uporablja izraz » nadzorstvo«. V ta namen bi se lahko uporabil tudi izraz »kontrola«.*

je veliko pozornosti posvečene izvedbi analize tveganja, postopku obravnave tveganj kakor tudi dodeljevanju vlog in odgovornosti za doseganje ustreznega nivoja informacijske varnosti v organizaciji. Namen sprememb v drugem delu standarda BS 7799 je:

- uvedba manjkajočih definicij in uskladitev izrazoslovja z obstoječimi dokumenti, ki obravnavajo informacijsko varnost,
- razjasnitev in dopolnitev obstoječih zahtev, ki se nanašajo na posamezne faze uvedbe SUIV v organizacijo,
- razširitev obstoječih zahtev glede oblikovanja potrebne dokumentacije in ravnanja s to dokumentacijo,
- zagotovitev rednega izvajanja interne presoje obstoječega SUIV,
- razumevanje in vpeljava postopkov za merjenje učinkovitosti obstoječega SUIV,
- razumevanje procesa ocenjevanja in obravnavanja relevantnih tveganj in pravilne uporabe metodologije za ocenjevanje tveganj.

S prenovo prvih dveh delov standarda BS 7799 je dosežena boljša preglednost in razumljivost. Nekatera področja so obravnavana bolj podrobno kot do sedaj, poleg tega pa so posamezna nadzorstva natančneje obrazložena. Zaradi slednjega je pričakovati, da bo uporaba standarda BS 7799 kot referenčnega priročnika pri zasnovi SUIV v organizacijah še narasla. Spremembe v novi izdaji prvih dveh delov standarda BS 7799 so podrobneje opisane v članku [8].

3.2 Vpliv sprememb prvih dveh delov standarda BS 7799 na organizacije

Čeprav zadnje spremembe standarda BS 7799 niso tako obsežne kot so bile pri prehodu standarda iz BS7799:1995 na BS 7799-1:2000 in BS7799-2:2002, se morajo organizacije teh sprememb zavedati in jim posvetiti vso pozornost.

Organizacije bodo morale kritično oceniti svoj SUIV in obstoječe varnostne politike ter jih uskladiti z novim standardom tako v vsebinskem kot v oblikovnem smislu (npr. uskladiti oštevilčenje in imenovanje poglavij).

Organizacije, ki želijo v bližnji prihodnosti pridobiti certifikat skladnosti z novim standardom, morajo izvesti podrobno primerjavo med varovalnimi ukrepi, ki so v organizaciji že vpeljani, in nadzorstvi, ki jih predlagata novi izdaji standarda BS 7799. V primeru odstopanj je treba izvesti ustrezno analizo tveganja. Na podlagi rezultatov analize tveganja se v organizaciji odločijo, katero od dodatnih nadzorstev je treba še vpeljati v obstoječi SUIV.

Organizacije, ki bodo želele v svoje poslovanje vpeljati novo izdajo standarda BS 7799, bodo morale imeti jasno definirane vloge in odgovornosti, povezane z zagotavljanjem informacijske varnosti (npr. odgovornosti pri izvajanju delovnih nalog posameznika, odgovornosti glede nepooblaščenega razkritja občutljivih informacij ipd.) kakor tudi sankcije v primeru neizvajanja le-teh. V prihodnje bodo morale organizacije posvetiti večjo pozornost nadzorstvom, ki se nanašajo na zagotavljanje varnosti v procesu kadrovanja. Treba je vzpostaviti ustrezna nadzorstva za preverjanje osebja pred sklenitvijo zaposlitve, nadzorstva za zagotavljanje varnosti med trajanjem zaposlitve ter ob prekinitvi le-te.

Organizacije, ki so že pridobile certifikat skladnosti z BS 7799-2:2002, bodo morale izvesti prehod na nov standard, saj je ob izdaji standarda BS ISO/IEC 27001:2005 veljavnost standarda BS 7799-2:2002 potekla. Določeno naj bi bilo prehodno obdobje za izvedbo tega postopka, ki pa zaenkrat še ni znano (glej tudi [9]). Ker se po BS 7799 zahteva vsakoletna obnovitev certifikata, bodo morale organizacije, ki že imajo certifikat skladnosti z BS 7799-2:2002, uskladiti obstoječi SUIV z zahtevami ISO/IEC 27001 pred izvedbo redne letne presoje skladnosti s standardom.

4 Pričakovane novosti v bližnji prihodnosti

Podobno kot družina standardov ISO 9000 pokriva področje zagotavljanja kakovosti, je mednarodna organizacija za standardizacijo ISO rezervirala družino standardov ISO/IEC 27000 za področje zagotavljanja informacijske varnosti. Prvega člana te družine predstavlja sedanja različica drugega dela standarda BS 7799, BS ISO/IEC 27001:2005. V prihodnjih nekaj letih pa lahko znotraj družine ISO/IEC 27000 pričakujemo izid še naslednjih dokumentov (glej npr. [10]):

- ISO 27000 – temeljni principi in pojmovnik (*angl. Principles and Vocabulary*); ta standard naj bi usklajeval strokovno izrazoslovje za vso družino standardov ISO/IEC 27000,
- ISO 27002 – pod to številko naj bi v letu 2007 izšla sedanja različica prvega dela standarda BS 7799, BS ISO/IEC 17799:2005,
- ISO 27003 – Napotki za vzpostavitev sistema za upravljanje informacijske varnosti (*angl. Information Security Management System Implementation*

Gudelines); izid tega standarda pričakujemo oktobra 2008,

- ISO 27004 Merila sistema za upravljanje informacijske varnosti (*angl. Information Security Management System Metrics and Measurement*),
- ISO 27005 – pod to številko naj bi v bližnji prihodnosti izšel obstoječi tretji del standarda BS 7799, BS 7799-3:2006, ki obravnava področje upravljanja informacijskih tveganj,
- ISO 27006 – Smernice za ponovno vzpostavitev informacijskega sistema po katastrofi (*angl. Guidelines for Information and Communications Disaster Recovery Services*); ta standard naj bi temeljil na singapurskem standardu SS507 (*angl. Singapore Standards for Business Continuity/Disaster Recovery (BC/DR) Service Providers*), izšel pa naj bi novembra 2007.

Na področju neprekinjenega poslovanja se v bližnji prihodnosti pričakuje še ena novost. V kratkem naj bi obstoječi dokument PAS 56 izšel kot britanski standard pod številko BS 25999, obsegal pa naj bi naslednja dva dela:[6]

- BS 25999-1:2006 Kodeks za upravljanje neprekinjenega poslovanja (predviden izid ob koncu leta 2006),
- BS 25999-2:2006 Specifikacije za upravljanje neprekinjenega poslovanja (predviden izid v začetku leta 2007).

5 Sklep

Pri vzpostavitvi sistema varovanja in zaščite informacij se je smiselno in koristno opreti na uveljavljene standarde in priporočila. Množica dokumentov, ki pokrivajo področje varovanja informacij, je precej obsežna. Slednje pogosto povzroča med uporabniki zmedo, saj ne vedo, katere standarde oziroma priporočila naj bi vpeljali v poslovanje svoje organizacije in v kakšnem vrstnem redu.

V prispevku smo na kratko predstavili tiste standarde in priporočila s področja zagotavljanja informacijske varnosti, ki so se v praksi najbolj uveljavili. Navedli smo tudi, katere standarde na tem področju lahko pričakujemo v prihodnjih letih.

Podrobneje smo opisali standard BS 7799, ki je eden najpomembnejših in najbolj razširjenih standardov na področju zagotavljanja informacijske varnosti. Opredelili smo glavne spremembe v novi izdaji prvih dveh delov tega standarda, in sicer BS ISO/IEC 17799:2005 ter BS ISO/IEC 27001:2005. Preučili smo možne vplive teh sprememb na organizacije, ki so svoje sisteme za upravljanje informacijske varnosti oblikovale na osnovi prejšnjih verzij standarda BS 7799. Čeprav se na prvi pogled zdi, da zadnje spremembe standarda BS 7799 niso velike, menimo, da se jih morajo v organizacijah zavedati ter skladno z njimi ustrezno ukrepati. Ugotavljamo, da je s prenovo dosežena boljša preglednost in razumljivost standarda BS 7799, zaradi česar ocenjujemo, da bo uporaba tega dokumenta v organizacijah v svetu in pri nas še narasla.

Naj prispevek sklenemo z ugotovitvijo, da enega perečih problemov v slovenskem prostoru predstavlja neusklajenost izrazoslovja na področju informacijske varnosti. Izkazalo se je, da izrazoslovje, uporabljeno v slovenskih prevodih dokumentov, ki obravnavajo informacijsko varnost, variira glede na institucijo, ki je prevajanje izvedla. Slednje povzroča zmedo pri uporabnikih teh dokumentov, pri presojevalcih informacijskih sistemov, kakor tudi v drugi strokovni javnosti. Oblikovanje ustreznega izrazoslovja je nedvomno področje, ki zahteva pozornost strokovne javnosti. Le tako lahko dosežemo enotno poimenovanje v strokovni literaturi ter razumevanje med uporabniki. Z oblikovanjem spletnega terminološkega slovarja Islovar[7] na tem področju veliko prispeva jezikovna sekcija, ki deluje v okviru Slovenskega društva Informatika.

6 Viri in literatura

[1] PUTNAM, H. Adam: Information Security References, Corporate Information Security Working Group, 2004, http://reform.house.gov/UploadedFiles/Best%20Practices%20Bibliography.pdf.

[2] BS ISO/IEC 17799:2005 Information technology – Security techniques – Code of practice for information security management, British Standards Institution, 2005.

[3] ZUPAN, Lucija: Zahteve za uspešno vpeljavo standarda BS7799-2 za področje informacijske varnosti, Uporabna informatika, 2005, let. 13, št.1, str. 37–50.

[4] BS ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements, British Standards Institution, 2005.

[6] *Glej npr. http://www.bsi-global.com/Business_Information/PressReleases/pas56.xalter.*

[7] *Glej www.islovar.org.*

[5] BS 7799-3:2006 Information security management systems – Guidelines for information security risk management, British Standards Institution, 2006.

[6] BS ISO/IEC 17799:2000 Information technology – Code of practice for information security management. British Standards Institution, 2000.

[7] BS 7799-2:2002 Information security management systems-Specifications with guidance for use. British Standards Institution, 2002.

[8] ZUPAN, Lucija, BREZAVŠČEK, Alenka: Novosti, ki jih prinašajo spremembe standarda BS 7799, Organizacija, 2006, let. 39, št. 1, str. 58–66.

[9] Frequently Asked Questions for BS ISO/IEC 27001:2005, http://www.bsi-global.com /ICT/Security/27001faq.xalter, november 2005.

[10] About the ISO 27000 series, http://www.iso27001security.com/html/iso27000.html, januar 2006.

Alenka Brezavšček je leta 2000 doktorirala na Fakulteti za organizacijske vede Univerze v Mariboru, kjer je od leta 1994 tudi redno zaposlena. Habilitirana je v naziv docentka in je nosilka treh različnih predmetov na univerzitetnem programu in enega predmeta na visokošolskem strokovnem programu. Njeno raziskovalno delo obsega predvsem študij stohastičnih modelov zanesljivosti in razpoložljivosti kompleksnih sistemov ter zagotavljanja varnosti informacijskih sistemov. Je avtorica oziroma soavtorica več izvirnih znanstvenih člankov in referatov, objavljenih v domači in tuji strokovni literaturi. Poleg tega je članica urednikov spletnega slovarja Islovar, kjer deluje na področju informacijske varnosti.

Lucija Zupan je leta 2000 diplomirala na Fakulteti za organizacijske vede Univerze v Mariboru s področja informacijske varnosti. Leta 2004 je na isti fakulteti magistrirala s področja analize in načrtovanja informacijskih sistemov. Zaposlena je v Hermes SoftLab, d. d., kot svetovalka za informacijsko varnost in snovalka rešitev na področju upravljanja identitete in dostopov. Opravljen ima izpit za vodilnega presojevalca za informacijsko varnost po standardu ISO/IEC 17799/BS 7799-2:2002 in mednarodno priznan certifikat za vodjo informacijske varnosti - CISM (Certified Information Security Manager) ter ITIL (Foundation Certificate in IT Service Management). Je članica presojevalske ter izvedenske skupine s področja BS 7799. Je aktivna članica urednikov spletnega slovarja Islovar, kjer vsebinsko pokriva področje informacijske varnosti. Je avtorica oziroma soavtorica več prispevkov na domačih in mednarodnih konferencah ter v strokovnih publikacijah.