SAVREMENO POSLOVANJE PODRŽANO INFORMACIONIM TEHNOLOGIJAMA I UPRAVLJANJE RIZIKOM

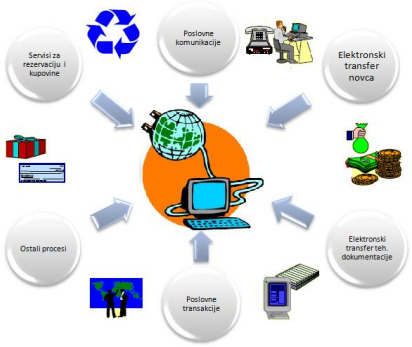
Gavrilović Darko[1)], Stojanović Marjan[2)], Milenković Ivan[3)]

Rezime: *Savremeni poslovni trendovi i opstanak na globalnom tržištu, u bilo kojoj sferi, podrazumevaju razmenu velikih količina informacija kao i njihov sve brži transfer. Neophodnost verifikacije i zaštite naučno istraživačkog rada, novih tehnoloških rešenja i intelektualne svojine nameću potrebu neprekidnog nadgledanja i kontrole sistema u svakom pogledu. Rad daje prikaz kako se mogu primeniti metode upravljanja rizikom - sigurnosnih rizika kao deo modeliranja sistema bezbednošću informacija ISO 27000 (ISMS).*
Ključne reči: *Savremeno poslovanje, upravljanje rizikom, FMEA*

Abstract: *Modern business trends and survival in the global market, in any sphere, involve the exchange of large amounts of information as well as their faster transfer. The necessity of verification and the protection of scientific research, new technological solutions and intellectual property impose the need for continuous monitoring and control system in every respect. This paper reviews how to apply methods of risk management - security risks as part of the modeling system information security ISO 27000 (ISMS).*
Key words: *Modern business, risk management, FMEA*

1. UVOD

Svaka kompanija na svom razvojnom putu definiše svoju misiju i viziju. U savremenom digitalnom dobu, kompanije uveliko koriste automatizovane informacione tehnologije (IT) kako bi imale podršku najvišeg nivoa u ostvarivanju svoje misije. Upravljanje rizicima igra presudnu ulogu u zaštiti vitalnih informacija kompanije, a time određuje u potpunosti misiju i opstanak kako na lokalnom tako i globalnom tržištu.



Slika 1 - Informacione tehnologije i savremeno poslovanje

Efikasnost procesa upravljanja rizikom je važna komponenta uspešnosti informacionih tehnologija i bezbednosti programa. Osnovni cilj procesa upravljanja rizikom, bilo male ili velike kompanije, je da štiti organizaciju i njenu sposobnost da obavlja svoju misiju.
Upravljanje rizikom podrazumeva proces identifikacije rizika, odnosno procene rizika i preduzimanje koraka za smanjenje rizika na prihvatljiv nivo. Time se dobijaju smernice za razvoj programa upravljanja rizikom, koji sadrži i definicije i praktične smernice neophodne za procenu i ublažavanje rizika identifikovanih u IT sistemima. Krajnji cilj je da se pomogne organizacijama da bolje upravljaju IT, sa što manje rizika a sve sa ciljem ostvarenja zadate misije.

2. TRENDOVI SAVREMENOG POSLOVANJA

Rukovodeći menadžment kompanije najčešće koristi informacione tehnologije za obezbeđenje podataka o nabavci ulaznih materijala i sirovina, stanju zaliha, plasmanu i prodaji, naplati potraživanja, naručiocima roba i usluga, budžetu i drugim podacima neophodnim za brzo i kvalitetno odlučivanje. Sve veću primenu imaju i IT sistemi za podršku nadzoru, kontroli, dugoročnom i kratkoročnom odlučivanju i planiranju itd.

Svedoci smo da je danas gotovo uobičajena praksa da se mobilni telefoni, pejdžeri, elektronska pošta, video konferencije široko primenjuju u poslovnoj komunikaciji. U proteklih deset godina, čak i u našoj sredini, koje važi za nerazvijeno informatičko evropsko društvo, povećanjem broja personalnih računara po glavi stanovnika, upotrebom i širenjem javne mreže Interneta, kao posledica u praksi je zaživelo elektronsko trgovanje kao termin za sve transakcije ostvarene "elektronskim putem", odnosno putem računara.

Ovakav prodor informacionih tehnologija i elektronske trgovine prividno je umanjio ne mali jaz između visoko razvijenih i nerazvijenih društava. Ako ništa drugo za trenutak je pružena

1) Darko Gavrilović, Univerzitet u Nišu, Mašinski fakultet Niš, mail: gavrilo89@hotmail.com
2) Marjan Stojanović, Univerzitet u Nišu, Mašinski fakultet Niš, mail: maxa989@live.com
3) Ivan Milenković, Univerzitet u Nišu, Mašinski fakultet Niš, mail: ivca89@hotmail.com

šansa za ravnopravno poslovanje i velikim i malim zemljama odnosno kompanijama velikih i malih kapaciteta. Kao što to biva kroz istoriju, neko je to iskoristio u većoj ili manjoj meri, planski ili stihijno, uspešno ili neuspešno. Dobra rešenja vrlo brzo donose vidljiva poboljšanja i profit dok loša postaju opterećenja sama sebi i vrlo brzo nestaju. Sve je to direktno povezano sa savremenim trendovima i kretanjima kako na lokalnom tako i globalnom tržištu roba, usluga i informacija. Državne uprave prikupljaju i analiziraju ogromne količine podataka koristeći informacione tehnologije što dovodi do pružanja kvalitetnijeg servisa građanima. Primera radi, veoma efikasan način unapređenja usluga koje pruža država svojim građanima, gledano sa vrha, je uvođenje elektronske vlade. Pri tome, značajno je shvatiti da ova transformacija ne podrazumeva samo automatizaciju poslovanja vlade, već njeno potpuno reoblikovanje. Elektronska vlada omogućava suštinsku transformaciju ogromnog državnog aparata, organizovanog i ustoličenog tako da prvenstveno zadovolji zahteve i potrebe birokratskog aparata (a ne potrebe građana) u jednu modernu, efikasnu i jeftinu vladu informatičkog doba, po funkcijama usaglašenu sa potrebama građana. Elektronska vlada koristi računarske i telekomunikacione tehnologije sa ciljem radikalnih izmena u pružanju servisa građanima i javnosti, poslovnim subjektima, zaposlenima u upravi i drugim vladinim organizacijama i resorima.

Slika 2 - Savremeno zdravstvo podrazumeva najnovija dostignuća u IT

Jedna od ključnih društvenih aktivnosti je zdravstvena i socijalna zaštita. U ostvarivanju ciljeva uspešnog poslovanja u zdravstvu i farmaceutskoj industriji informacione tehnologije i softverski alati su od velike pomoći. U domenu upravljanja i praćenja najnovijih informacija, za prikupljanje, evidentiranje, skladištenje i obezbeđenje medicinskih resursa i podataka za podršku odlučivanju, planiranju pojedinačnih intervencija, predviđanju širih akcija i sl.

U visoko razvijenom zdravstvu lekarima su na raspolaganju ekspertni sistemi kao pomoć pri dijagnostici bolesti pacijenta i preporuci mogućeg tretmana. Elektronski zdravstveni zapisi, koji obuhvataju medicinske i nemedicinske istorije građana, pružaju dragocenu pomoć medicinskom osoblju u radu. Zahvaljujući ne malim medicinskim bazama podataka moguće je unaprediti procese u zdravstvu i olakšati mere kako opšte zdravstvene zaštite tako i pojedinačne usluge i intervencije. Umrežavanje i telemedicina – mrežni sistemi u obliku intraneta, ekstraneta i Interneta između ostalog omogućavaju i povezivanje sa lokalnim farmaceutskim kućama i apotekama, i na licu mesta pripremanje recepture za lekove koji su neophodni za pacijenta.

Ekonomsko finansijski sektor i bankarski sistemi doživeli su drastične promene s početkom primene plastičnog novca odnosno kartica, bankomata i elektronskog transfera novca sa mesta prodaje. Internet bankarstvo i plaćanje računa putem Interneta predstavlja takođe dobar primer primene novih informacionih tehnologija u savremenom poslovanju koji sa sobom nosi vrlo velike rizike.

Slika 3 - Bankarski sistem podrazumeva IT i visoku bezbednost

Savremena društva prati brzi razvoj svih oblika medija i komunikacija. Izdavačka delatnost i štampani mediji svoje poslovanje danas ne mogu da zamisle bez primene računara koristeći softversku podršku za brzu obradu teksta i slika. Turističke agencije i veliki turoperateri, autoprevoznici i aviokompanije, organizatori putovanja i veliki hotelski lanci sve više koriste informacione tehnologije u svom poslovanju. Informacione tehnologije se s jedne strane koriste za donošenje odluka u turističkim organizacijama radi pomoći u vođenju poslovne politike kako u dužem tako i kraćem periodu, a sa druge strane usmerene su ka pružanju brzih i kvalitetnih informacija potencijalnim korisnicima usluga. Takođe, turističke agencije koriste savremene

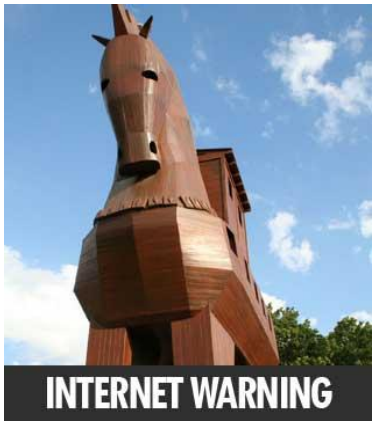
informacione tehnologije za rezervacije putnih karata i mesta u hotelu. Sve to podrazumeva rad sa velikim brojem podataka, gde se mora obezbediti sigurnost, pouzdanost i tačnost informacija.

Mnogi prodajni objekti, veliki trgovački lanci mogu da koriste POS (Point-of-sale) sistem za efikasnu obradu transakcija. Bar-kod čitač služi za unos podataka, pri čemu se naziv proizvoda, količina i cena prikazuje na displeju registar kase kao i na računu. Takav sistem predstavlja osnovu za uspešno praćenje i kontrolu zaliha koji ujedno pokreće druge vezane sisteme nabavke, transporta i sl.

3. OPASNOSTI KOJE PRETE NA INTERNETU

U samo nekoliko poslednjih godina Internet tehnologije postale su nezamenljive. Svesno ili nesvesno na njih se oslanjamo pri komuniciranju, zabavi, trgovini, razmeni informacija itd. Barem na prvi pogled, ovaj vid komunikacije učinio je naše živote zabavnim i produktivnim. Ali sve što je novo neminovono donosi sa sobom i neke loše trendove, naime Internet je postao izazov i predmet interesovanja lopovima, vandalima, stručnjacima za otkrivanje tajnih podataka, širenje industrijskog kriminala, narušavanje privatnosti, uništavanje računara, pa čak i za direktnu krađu novca.

Svaki put kada koristimo Internet, prihvatamo određene rizike: krađu identiteta, viruse, spam, spyware, itd. Postoje brojni alati i tehnike zaštite pa se današnji stvarni rizici mogu izbeći. Ne treba okrenuti leđa svemu što nam Internet pruža. Međutim, veliki je broj korisnika koji koriste Internet ne preduzimajući nikakve korake za ublažavanje rizika: nemaju antivirusni softver, firewall niti ikakve ideje o tome da prevaranti i lopovi aktivno ″kruže″ Internetom u potrazi za novim žrtvama.



Najbolji primer prevare je krađa identiteta. Tokom prevare otmičari pokušavaju preuzimanje kontrole nad računarom kako bi sproveli svoje nelegalne namere poput praćenja online aktivnosti, prikazivanja neželjenih oglasa, slabljenja performansi računara ili veze s Internetom. Jedna od danas najvećih i najbrže rastućih pretnji na Interneta je krađa identiteta – kopiranje informacija poput brojeva kreditnih kartica, lozinki i matičnih brojeva. Te se informacije mogu koristiti za online ili offline prevare.

Sprečavanje krađe identiteta

Trgovina putem Interneta zasniva se na sposobnosti korisnika da dokaže svoj identitet, odnosno njegovoj moći uveravanja da je zaista osoba kojom se predstavlja. Dokazi identiteta koriste se da bi potvrdili autentičnost korisnika organizacijama s kojima posluje ili da bi ovlastili isporuku usluga i transakcija. Na Internetu identitet korisnika se sastoji od niza elemenata poput korisničkih imena, lozinki, ličnih identifikacijskih brojeva (PIN-ova), jedinstvenih matičnih brojeva, raznih brojeva računa i drugih ličnih podataka. Ti digitalni identiteti rade pod pretpostavkom da smo jedina osoba koja zna svoje podatke. Kada poslujemo putem Interneta, niko ne traži sliku da bismo dokazali svoj identitet. Kradljivci identiteta češće koriste spam tehnike za slanje lažnih poruka.

Danas koristimo Internet za sve oblike finansijskih transakcija što bitno podiže verovatnoću za krađu identiteta. Kriminalci mogu upotrebiti naš digitalni identitet za otvaranje računa kreditnih kartica, menjanje adrese, podizanje nenamenskih i hipotekarnih kredita, za sprovođenje finansijskih transakcija. Oni te ukradene digitalne identitete mogu prodavati drugim kriminalcima na dobro organizovanom crnom tržištu Interneta. Prevara s kreditnim karticama najčešći je oblik krađe identiteta. Lopovi kradu lične informacije i koriste ih za otvaranje

računa u tuđe ime, troše sredstva s tog računa mesec ili dva i potom jednostavno odbace karticu kada je kompanija koja je izdala blokira. Postoji nekoliko načina za sprečavanje online krađe identiteta. Neki uključuju tehnologiju, ali se većina oslanja na zdrav razum koji je efikasniji i besplatan. Najbolja obrana od napada je nepoverenje i skepticizam prema svakoj poruci koja tvrdi da dolazi s neke lokacije za e-trgovinu ili iz finansijske institucije. Osim zdravog razuma i brojni alati pomažu u sprečavanju krađe identiteta.

Na vrhu popisa nalaze se antivirusni programi i anti-spyware programi. Budući da puno poruka e-pošte sadrži viruse i zlonamerni kod, svoj antivirusni softver moramo stalno ažurirati. Šta više moramo investirati u anti-spyware softver i redovno skenirati svoje računare. Anti-spyware softver može otkriti brojne vrste programa koje kradljivci identiteta koriste za dobijanje ličnih podataka. Trebamo preduzeti korake da svoj web pretraživač zaštitimo od programa s pokretanjem po učitavanju kojima zlonamerne ili kompromitovane web lokacije bez našeg znanja instaliraju malware na računare.

4. PROCENA I SMANJENJE RIZIKA

Procena rizika je prvi proces u metodologiji upravljanja rizicima. Organizacije koriste procenu rizika da bi se utvrdio obim potencijalnih pretnji i rizika u vezi sa IT sistema. Rezultat ovog procesa pomaže da se identifikuju odgovarajuće kontrole za smanjivanje ili eliminisanje rizika u toku procesa ublažavanja rizika.

Metodologija procene rizika obuhvata 9 osnovnih koraka:

1. karakterizacija sistema
2. identifikacija opasnosti
3. ranjivost identifikacije
4. analiza kontrole
5. utvrđivanje verovatnoće
6. analiza uticaja
7. određivanje rizika
8. kontrola
9. dokumentacija rezultata

U proceni rizika IT sistema, prvi korak je da se definiše obim napora. U ovom koraku, granice informacionog sistema su identifikovane, zajedno sa resursima i informacije koje čine sistem. On karakteriše IT sistem i uspostavlja obim rizika, ocrtava operativne dozvole (ili akreditacije), granice, i pruža informacije (na primer, hardver, softver, sistem veze, i odgovoran podele ili pomoćno osoblje) od suštinskog značaja za definisanje rizika.

U drugom koraku identifikacije, definiše se izvor pretnji za uspešno vršenje određene ugroženosti. Ranjivost je slabost koja se može slučajno ili namerno aktivirati ili eksploatisati. Cilj ovog koraka je da se identifikuju potencijalne pretnje - izvori i sastaviti spisak potencijalnih pretnji koji se mogu primeniti na IT sistema koji se ocenjuju.

Pretnje-izvori	Motivacija	Opasnosti
Haker	Izazov, ego, pobuna	Upad u sistem, neovlašćen pristup sistemu
Računarski kriminal	Uništavanje informacija, neovlašćeno menjanje podataka	Lažna dokumenta, lažna redstavljanja, presretanje, ...
Terorisanje	Ucena, iznuda, osveta	Bomba, informaciono ratovanje
Industrijska špijunaža	Konkurentska, ekonomska špijunaža	Krađa informacija
Insajderi (slabo obučeni, nezadovoljni, bivši zaposleni)	Radoznalost, monetarni dobitak, slučajna greška, osveta	Ucenjivanje, zloupotreba i kradje, sabotaža sistema

***Tabela 1 - Ljudske pretnje: Pretnje-izvori, motivacije, opasnos*ti**

Treći korak predstavlja analizu opasnosti, informacioni sistem mora da sadrži analizu ranjivosti u vezi sa sistemom životne sredine. Cilj ovog koraka je da se razvije lista ranjivosti sistema (nedostatke ili slabosti) koji mogu da budu iskorišćeni od strane potencijalnih pretnji - izvora.

Cilj sledećeg koraka je da se analiziraju kontrole koje su sprovedene, ili su u planu za implementaciju, od strane organizacije kako bi se smanjile ili eliminisale mogućnosti (ili verovatnoće) od opasnosti.

Nivo verovatnoće	Definicija verovatnoće
Visok	Pretnje – izvori su visoko motivisani i dovoljno sposobni, da spreče ranjivosti od neželjenih pojava.
Srednji	Pretnje - izvori su motivisani i sposobni, ali na snazi su kontrole koje mogu predstavljati prepreku uspešnom ostvarivanju ranjivosti.
Nizak	Pretnjama-izvorima nedostaju motivacije i sposobnosti, ili su kontrole tu da bi se sprečile, ili bar otežale ugroženosti koje se ostvaruju.

Tabela 2 – Ocena verovatnoće

U petom koraku određujemo ocenu verovatnoće po utvrđenom kriterijumu i usvojenoj gradaciji. Najčešće tri nivo, pet ili deset nivao.

Sledeći veliki korak u merenju nivoa rizika je da se utvrdi uticaj negativnih posledica uspešnog ostvarivanja ugroženosti (pretnje). Pre početka analize uticaja, neophodno je dobiti sledeće potrebne informacije:

• sistem misije (na primer, procese obavljaju informacioni sistemi)

• sistema i podataka kritičnosti (npr., sistema vrednosti)

• sistema i podataka osetljivosti.

Svrha sedmog koraka je da proceni stepen rizika u IT sistemima. Određivanje rizika za određenu opasnost:

Verovatnoća pretnje	**Uticaj**		
	Niski (10)	**Srednji** (50)	**Visoki** (100)
Visoka (1.0)	Niska 10 X 1.0 = 10	Srednja 50 X 1.0 = 50	Visoka 100 X 1.0 = 100
Srednja (0.5)	Niska 10 X 0.5 = 5	Srednja 50 X 0.5 = 25	Srednja 100 X 0.5 = 50
Niska (0.1)	Niska 10 X 0.1 = 1	Niska 50 X 0.1 = 5	Niska 100 X 0.1 = 10

Tabela 3 - Razmera rizika: Visoka (> 50 do 100), srednja (> 10 do 50); Niska (1 do 10)

Osmi korak je kontrola koja bi mogla ublažiti ili eliminisati identifikovane rizike, na odgovarajući način poslovanja organizacije. Cilj kontrole je da se smanji nivo rizika u informacionim sistema i podacima na prihvatljiv nivo. Sledeće faktore treba uzeti u obzir:

- Efektivnost
- Zakonodavstvo i regulativa
- Organizaciona politika
- Operativni uticaj
- Sigurnost i pouzdanost.

Kad je procena rizika završena, rezultati treba da budu dokumentovani u službenom izveštaju.

Izveštaj procene rizika je izveštaj koji pomaže menadžmentu, misiji vlasnika, donose odluke o politici, budžetu i izmene u operativnim sistemima upravljanja. Za razliku od revizije ili istrage izveštaja, izveštaj procene rizika ne bi trebalo da bude predstavljen na optužujuć način, već kao sistematski i analitički pristup procene rizika, tako da će više rukovodstvo razumeti rizike i rasporediti sredstva da se umanji i ispravi potencijalan gubitak.

Sve kompanije neophodno je da imaju osnovnu liniju sigurnosti koja će im pružiti minimalni nivo zaštite. Na primer, napadi kompjuterskih virusa mogu zapretiti bilo kojoj lokalnoj mreži kao i pojedinim računarima. Oni trebaju imati backup sisteme koji će ih zaštititi od gubitka ili uništavanja informacija i koji će osigurati fizičku zaštitu ličnih podataka i opreme.

ISO/IEC 27002:2005 daje kodeks dobre prakse koji opisuje neophodne elemente za osnovnu zaštitu, uključujući i:

- Politiku za upravljanje sigurnošću informacija visokoga nivoa;
- Značaj korisnika
- Antivirusni softver
- Backup
- Kontrolu pristupa
- Fizičku zaštitu objekata i komercijalno osetljivih akata i dokumenata u papirnoj formi
- Zaštitu ličnih i podataka i dokumenata kompanije

Informacija je dobro koje, kao i materijalna dobra, ima vrednost za kompaniju, te stoga traži da bude adekvatno zaštićena. Sigurnost informacionog sistema štiti informacije od širokog spektra pretnji u cilju osiguranja kontinuiteta poslovanja, minimiziranja poslovnih šteta, a maksimiziranja povraćaja investicija i profita. Informacija može egzistirati u mnogo formi. Može biti napisana ili odštampana na papir, elektronski skladištena, transmitovana telefaksom ili telefonom, prikazana na filmu ili izrečena tokom razgovora. Bez obzira na to u kojoj se formi javlja ili na koji način se prenosi i skladišti, informacija u svakom trenutku mora biti adekavtno zaštićena.

5. ZAKLJUČAK

Procesuiranje rizika, njegovo smanjenje i eliminisanje pri svakodnevnom protoku informacija danas je postao nezaobilazni element sigurnosti u datom poslovnom okruženju. FMEA metod pruža sistematski pregled informacija i pomaže administratorima da otkriju potencijalne

propuste, tako da se akcije protiv nelegalnih korisnika mogu pripremiti unapred. Za kompanije akumulirano znanje i praktično iskustvo je najvrednija imovina koja u neuređenim informatičkim odnosima može biti predmet interesovanja mnogim neovlašćenim korisnicima.
Za informacioni sistem je bitno da bude fleksibilan, tako da može brzo da se prilagodi promenama vezanim za promenu delatnosti ili cilja poslovne politike, da se može uvesti za relativno kratko vreme, da se iz baze podataka može dobiti bilo koja željena informacija koja ima smisla za sve nivoe odlučivanja i da omogućava racionalno poslovanje koje je u funkciji dobiti.

Funkcija	Greška	Uzrok greške	Efekat greške	S	O	Detekcija greške	D	Risk Priority Number (RPN)
Skeniranje sumnjivih datoteka ručno	Neki nepoznati virusi se ne mogu otkriti	Zlonamerni virusi mogu imati novi format	Virusi se ne mogu otkriti, prodor virusa	10	3	Ažuriranje baze podataka, i ponovno skeniranje	8	240
	Neki virusi se ne mogu obrisati u potpunosti	Virus može da se klonira i da automatski promeni ime	Virusi se ne mogu ukloniti, što šteti sistemu	10	5	Ova vrsta virusa će biti izolovana i korisnik će dobiti obaveštenje	5	250
Skeniranje virusa automatski sa stalnom zaštitom	Stalna zaštita ne može da radi zbog virusa	Inteligentni virus može da pronadje anti-virusne procese i da ih blokira	Automatsko skeniranje ne radi i ne štiti sistem	8	4	Daje visoku zaštitu i sprečava neovlašćen pristup promenama	4	128
	Skeniranje stalnom zaštitom povlači mnogo resursa	Anti-virus program zahteva adekvatnu konfiguraciju sistema	Efikasan rad i performanse biće ugrožene	3	4	Optimizacija softvera i ažuriranje drajvera	2	24
Ažuriranje baze virusa	Korisnici ne mogu da povrate poslednju bazu podataka sa servera	Mreža ne radi	Potrošači ne mogu da ažuriraju bazu podataka	7	2	Održavanje baze podataka sa velikom pouzdnošću	1	14
	Baza podataka ne može biti instalirana	Konflikt softvera ili hardvera	Baza podataka se ne može ažurirati	7	1	Omogućava smernice i efektivnu tehničku podršku klijentu	1	7
Potvrda licence	Licenca je ilegalna	Hakeri ili pojedinci "krekuju" softver	Ekonomski gubitak za anti-virusnu kompaniju	9	7	Poboljšavanje anti-piratskih tehnologija i traženje pomoći od zakona	7	441

Tabela 4 - Obrada i procena greške u IT

LITERATURA

[1] Stoiljković V, Integrisani sistemi menadžmenta ISO 9001 2000, ISO 14001 2004 ISO 18001 1999 – Mašinski fakultet Niš

[2] Stoiljković V, Mlosavljević P, Ranđelović S, Industrijski menadžment Praktikum, Mašinski fakultet u Nišu, Niš 2010.

[3] NIST Special Publication 800-12. An Introduction to Computer Security: The NIST Handbook. October 1995.

[4] NIST Special Publication 800-14. Generally Accepted Principles and Practices for Securing Information Technology Systems. September 1996. Co-authored with Barbara Guttman.

[5] NIST Special Publication 800-18. Guide For Developing Security Plans for Information Technology Systems. December 1998. Co-authored with Federal Computer Security Managers' Forum Working Group.

[6] NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems. August 2001.