Synthesis
International Scientific Conference of IT and Business-Related Research

ORGANIZACIONA KULTURA KAO NETEHNIČKI ASPEKT BEZBEDNOSTI INFORMACIJA

ORGANIZATIONAL CULTURE AS NON-TECHNICAL ASPECT OF INFORMATION SECURITY

Bogdan Mirković
Fakultet za informacione tehnologije, Slobomir P Univerzitet, PF 70, Slobomir, Bijeljina, Bosna i Hercegovina

Apstrakt:
Jedno od najznačajnijih područja upravljanja informacijama svakako je upravljanje bezbednosti informacija. Pored tehničkih mera zaštite informacija, organizacije bi trebalo da obrate posebnu pažnju i na ne tehničke faktore bezbednosti informacija. U radu je stavljen poseban naglasak na ne tehničke faktore bezbednosti informacija, prvenstveno na organizacionu i bezbedonosno-informacionu kulturu. Rad predstavlja sublimaciju stručne literature iz ove oblasti i predstavlja osnov za dalje bavljenje ovom problematikom. Rad ujedno omogućava upravnim organima u organizacijama da steknu uvid u potrebu za poboljšanjem stepena i stanja organizacione kulture zaposlenih radi unapređenja sveukupne informaciono-bezbednosne kulture, a samim tim i informacione bezbednosti unutar organizacije.

Ključne reči:
organizaciona kultura, informaciono-bezbednosna kultura, organizacija, informaciona imovina.

Abstract:
Information security management is undoubtedly one of the most important areas of information management. Besides technical measures of information security, organizations should pay special attention to non-technical factors of information security. This paper places an emphasis on non-technical factors of information security, primarly on the organizational and information security culture. It represents the sublimation of technical literature in this field and a solid basis for future related research. Additionally, it should enable the administrative bodies and management within organizations to get an insight into the need to enhance the organizational culture of employees in order to improve the overall quality of information security culture, and thus, information-security in the organization.

Key words:
organizational culture, information - security culture, organization, information assets.

1. UVOD

Informaciona i komunikaciona tehnologija (IKT) je sveprisutna u današnjem društvu i prožima gotovo sve oblike antropološke interakcije. Današnja IKT pruža ogromne količine podataka organizacijama i njihovim zaposlenima. Kako sve više organizacija posluje i razmjenjuje osjetljive materijale preko interneta, izloženost napadima na informacionu bezbjednost takođe je u porastu. U uslovima savremenog tržišta, poslovni uspjeh i ekonomska bezbjednost nezamislivi su bez informacione bezbjednosti. Informacije i informacioni resursi predstavljaju nematerijalna dobra i zbog toga je zaštita informacija neodvojivi dio poslovanja.

Stručna lica koja se bave pitanjima informacione bezbjednosti su prepoznala da rješavanje sigurnosnih problema zahtijeva korišćenje tehnologije, procesa i ljudi (Chang & Ho, 2006). I pored ove činjenice, mnogi od njih se u svom stalnom radu bave samo pitanjima u vezi sa tehničkim mjerama, postupcima i procesima mjerenja nivoa zaštite informacija i njihove moguće zlouputrebe (Knapp *et al*., 2009). Tehnološki faktori nisu jedini koji su ključni za efektivno upravljanje bezbjednošću informacija (Carroll, 2006). Ulogama netehničkih faktora, uključujući organizacionu kulturu, bezbjedonosnu politiku i ljudsko djelovanje i ponašanje posvećuje se mala ili nikakva pažnja. Greška koja se čini nerazmatranjem i neuključivanjem netehničkih faktora u proces i politike informacione bezbjednosti mogu imati dalekosežne posljedice na informacionu bezbjednost organizacije. Informaciona bezbjednost je široka i multi-dimenzionalna tema. Neki od poznatih izraza koji se koriste kao sinonimi su računarska sigurnost (bezbjednost), sigurnost mreže, bezbjednost informacione tehnologije, bezbjednost informacionih sistema, kao i osiguranje informacija. U ovom radu pod pojmom „bezbjednost informacija" podrazumijevaćemo sveukupnost komponenti koje se tiču zaštite povjerljivosti, integriteta i dostupnosti informacija.

Povjerljivost informacija znači da niko ne bi trebao imati pristup informacijama organizacije koja su njeno vlasništvo osim ovlaštenih osoba ili entiteta. Ovakve informacije se smatraju informacionom imovinom. Integritet se odnosi na pouzdanost informacija koja može biti narušena kada se dešavaju nepravilne izmjene ili uništenja podataka koje se odvijaju u tranzitu informacija, što dovodi do različitih rezultata ili tumačenja informacija (Chang & Ho, 2006). Dostupnost se definiše pravovremenim pristupom podacima u smislu funkcionalnog značaja. Integritet i dostupnosti omogućavaju izbjegavanje slučajnih ili zlonamjernih promjena informacija, kao i osiguravanje da ovlaštene osobe imaju pristup podacima kada je to potrebno (Dhillon & Torkzadeh, 2006).

2. INFORMACIONA BEZBJEDNOST

Domen informacione bezbjednosti uglavnom je usmjeren na tehnologiju. Međutim, činjenica je da je profil kompetentnosti specijaliste za informacionu bezbjednost ne samo tehnički kao kod IT menadžera, već on mora posjedovati i upravljačka (menadžment, ekonomija, privredno pravo) i specijalistička znanja (organizacija sistema informacione bezbednosti, zaštita poslovnih tajni, specijalna psihologija, osnovi kriminalistike i

E-mail: bogdanmirkovic@yahoo.com
DOI: 10.15308/Synthesis-2015-321-326

industrijska špijunaža). Cilj informacione bezbjednosti je da se informacije koje se smatraju imovinom organizacije čuvaju od nedozvoljenog pristupa ili uništenja. Objavljivanje, mijenjanje ili negiranje su tri primarna mehanizma koje zlonamjerni pojedinci ili grupe koriste.

Organizacije se suočavaju s prijetnjama njihovoj informacionoj imovini bilo iz eksternih bilo iz internih izvora, bez obzira na vrstu ili veličinu organizacije (Colwill, 2010). Interne prijetnje uključuju nenamjerne i namjerne prijetnje po informacionu bezbjednost, a njihova opasnost leži u činjenici da mogu proći neopaženo dugo vremena i predstavljaju veći rizik od eksternih napada na informacionu imovinu (Carroll, 2006).

Namjerna prijetnja proizlazi iz slučajeva kada zaposleni ili partner u organizaciji svojim namjernim postupcima nastoji da uzrokuje štetu ili gubitak podataka (Kros *et al*., 2004/2005). Nenamjerne prijetnje nastaju kada pojedinac unutar organizacije nehotice oštećuje informacionu imovinu ili usluge (Colwill, 2010). U mnogim ranijim radova iz ove oblasti zaključeno je da su namjerne prijetnje ozbiljnije za informacionu bezbjednost (Caroll, 2006; Colwill, 2010; Blyth & Kovacich, 2006).

Zbog svega navedenog, organizacijama se predlaže da moraju njegovati sveobuhvatan pristup informacionoj bezbjednosti, koji obuhvaća i ljudske i tehničke dimenzije prilikom upravljanja informacionom bezbjednosti u svojim organizacijama (Barlas *et al.*, 2007). Aspekte kao što su organizaciona kultura, bezbjednosne politike, te ljudsko djelovanje i ponašanje mogu se posmatrati netehničkim aspektima, dok se specifične tehnologije (*firewall*, enkripcija i kontrola pristupa) mogu opisati kao tehničke osobine bezbjednosti informacija. Ovo se posebno odnosi na zaposlene u organizaciji, njihovu bezbjedonosnu kulturu i potrebu povećanja njihove svjesnosti o važnosti informacija koje organizacija posjeduje. Nadalje će u radu biti izloženi koncepti organizacione kulture kao i njen odnos sa bezbjedonosno-informacionom kulturom kao važnim netehničkim faktorima ukupne bezbjednosti informacija u organizaciji.

3. ORGANIZACIONA KULTURA

Termin organizaciona kultura (OK) nastao je u Americi i veoma brzo se proširio na ostatak poslovnog sveta. Napisano je mnogo članaka i knjiga o kulturi u organizacijama, koju obično nazivaju i „korporativna kultura" ili „organizaciona kultura". Često se kaže da kultura predstavlja moralne, socijalne i ponašajne norme jedne organizacije zasnovane na vjerovanjima, stavovima i prioritetima njenih članova (Duffy, 1999).

Kulturu možemo definisati kao karakteristična vjerovanja i ponašanja koja postoje u organizaciji. OK je skup formanih i neformalnih ponašanja koja je organizacija prihvatila kao svoj način obavljanja posla. Formalna strana obuhvata pisane izjave i šemu organizacione strukture. Neformalna strana bavi se time kako se posao obavlja - da li preko pisanih procedura ili putem direktne komunikacije, kako se zaposleni ponašaju jedni prema drugima, koliko su spremni da razmjenjuju ideje i informacije i kako hijerarhija dozvoljava zaposlenima da pređu granice „staze" da bi obavili posao (Guptara, 1994).

Šta je OK? U osnovi, ona je opisana kao osobenost, odnosno karakteristika jedne organizacije, ili jednostavno kao „način na koji su stvari uređene u organizaciji" (Wright & Boswell, 2002). Ona utiče na način na koji zaposleni misle, ponašaju se i osećaju. OK je širok termin koji se koristi za definisanje osobenosti ili karaktera posebne organizacije i uključuje elemente kao što su osnovne vrednosti i verovanja menadžmenta i ostalih zaposlenih, korporativna etika i pravila ponašanja. OK može biti izražena u misiji organizacije, u arhitektonskom stilu ili unutrašnjem dekoru kancelarija, zatim može biti iskazana načinom oblačenja zaposlenih na poslu, načinom na koji zaposleni oslovljavaju jedni druge i titulama koje su im date.

"Način na koji obavljamo stvari" je često navođena definicija kulture (Jakovljević & Grujić, 1998). Međutim, ovo je suviše opšta definicija koja propušta da naglasi sljedeće:

- kulture su kolektivna vjerovanja koja oblikuju ponašanje;
- kulture su djelimično zasnovane na emocijama, koje su posebno uočijive kada se prijeti promjenom;
- kulture su zasnovane na istorijskom kontinuitetu; potencijalni gubitak kontinuiteta djelimično objašnjava otpor promjeni;
- iako se kulture protive promjeni, one se konstantno mijenjaju, itd.

Zapravo, gotovo svako ko govori ili piše na ovu temu ima sopstvenu definiciju. Neke od njih ukazuju na to da je OK:

- predispozicija da se ponašamo na određene načine (Jakovljević & Grujić, 1998);
- grupa ponašanja i kodova koje ljudi koriste za usmjeravanje interakcije ka drugima; ona uključuje formalne, pisane politike organizacije i neformalna pravila nastala sa iskustvom;
- način na koji preduzeće vidi sebe i svoje okruženje (Guptara, 1994), itd.

Svaka organizacija ima svoju sopstvenu kulturu ili set vrijednosti. Najveći broj organizacija ne pokušava svjesno da kreira određenu kulturu, već se kultura organizacije uglavnom kreira nesvjesno i bazirana je na vrijednostima top menadžmenta ili osnivača organizacije. Ono čemu organizacija teži i koje vrijednosti se nada da će dostići, može se razlikovati od vrijednosti, vjerovanja i normi izraženih u tekućoj praksi i ponašanju.

Procjena kulture može da obezbedi realne podatke o stvarnim vrijednostima i normama organizacije. Kultura je "kolektivno programiranje uma koje pravi različitosti ljudi iz različitih zemalja, u skladu s socijalno-antropološkom teorijom" (Hofstede, 2001, str. 25). Na osnovu navedenog, OK se definiše kao niz osobina na koje utiče to kako zaposleni vidi organizaciju (Schein, 1992).

Schein (1992, str. 6) je definisao OK kao: "Kolektivni fenomen koji raste i mijenja se s vremenom i, u određenoj mjeri, na njega se može uticati ili čak i kreirati od strane upravnih organa organizacije". Osnovne pretpostavke koje određena grupa zaposlenih otkrije ili razvije u procesu učenja i nošenja sa svojim problemima eksterne adaptacije i interne integracije (ukoliko zaposleni to rade dovoljno dobro da se smatra ispravnim), mogu poslužiti i sa kao osnov za definisanje OK novih zaposlenih da i oni na isti način misle i osjećaju u vezi sa istim ili sličnim problemima. Ovo se posebno može odnositi na informaciono-bezbjedonosnu kulturu (IBK). Za neke autore, kultura je najvažniji faktor u objašnjavanju uspjeha ili neuspjeha u organizaciji (Deal & Kennedy, 1982). Međutim, ranijim studijama utvrđeno je da je samo 5% organizacija ima definisanu kulturu, gdje viši menadžment uzima aktivnu ulogu u oblikovanju OK (Atkinson, 1997). Ako menadžment ne razumije kulturu organizacije, to bi se moglo pokazati kao fatalno (Hagberg Consulting Group, 2009). Ipak, OK svake organizacije određuje ponašanje svojih zaposlenih i utiče na formiranje prihvatljivog ponašanja unutar organizacije (Beach, 1993).

4. INFORMACIONO-BEZBEDONOSNA KULTURA

Informaciona bezbjednost, kao jedan od novijih pravaca istraživanja u sferi bezbjednosti posljedinca, odraz je je tehno-

DOI: 10.15308/Synthesis-2015-321-326

loškog razvoja i novog pogleda na svijet. Ona se javlja ne samo kao jedan od vidova (oblika) bezbjednosti, već i kao presjek svih drugih vidova bezbjednosti u kojima informacione tehnologije zauzimaju važno mesto. O značaju informacione bezbednosti govori i činjenica da je ona postala jedna od osnovnih komponenata nacionalne bezbednosti.

IBK, koja je sastavni dio OK i ima veze s ponašanjem zaposlenih (Schlienger & Teufel, 2003). Načini na koji zaposleni obavljaju svoje poslove temelje se na kolektivnim vrijednostima, normama i znanjima i imaju presudan uticaj na uspjeh cijele organizacije. Veoma je mali broj istraživanja o IBK koja bi dala jasniju sliku o definiciji IBK, niti postoje jasni stavovi o tome kako stvoriti OK za podršku IBK (Chia *et al.*, 2002). Takođe, u istom radu (Chia *et al.*, 2002) tvrdi se da je veoma važno razumjeti OK koja će dovesti do odgovarajućeg načina upravljanja IBK-om.

OK ima značajan uticaj na sigurnost podataka, a to može biti negativno ili pozitivno (Chang & Lin, 2007). Važno je da OK odražava pozitivan stav prema informacionoj bezbjednosti kroz cijelu organizaciju, a to je važno za obavljanje poslova organizacije i treba biti u skladu s dobrom praksom IBK. Bezbjedonosna kultura se temelji na unapređenju svesti zaposlenih o važnosti podataka i ophođenja prema istim, kao i na usvajanju poželjnih modela ponašanja u kontekstu organizacione kulture (Da Veiga & Eloff, 2010, str. 198).

Da bi se razumio uticaj OK na bezbjedonosnu kulturu, predložen je organizacioni model kulture, baziran na modelu koji se koristi u literaturi o bezbjedonosnoj kulturi, koji je primjenjiv na sve dimenzije bezbjednosti u organizaciji (Detert *et al.*, 2000). Nakon toga, razvijen je istraživački model za vrednovanje IBK. Međutim, Helokunnas i Kuusisto su utvrdili da samo posvećivanje pažnje OK nije dovoljno za razumijevanje svih faktora koji utiču na IBK (Helokunnas & Kuusisto, 2003). Svaki pojedinac u svakoj organizaciji je pod uticajem nekoliko etičkih, nacionalnih i organizacionih kultura koje utiču na način na koje taj pojedinac tumači značenje i važnost informacione bezbjednosti. Kao rezultat toga, važno je razumjeti složenost OK koja ima uticaja na bezbjedonosnu kulturu.

5. ODNOS ORGANIZACIONE I INFORMACIONO-BEZBEDONOSNE KULTURE

Kultura je set shvatanja i pretpostavki u određenoj grupi, npr. etničkoj grupi ili zemlji. OK sastoji se iz glavnih shvatanja i pretpostavki o poslovanju, korporaciji ili organizaciji. Shvatanja uključuju zajednička vjerovanja i ubjeđenja, vrijednosti, pristup odlučivanju i najčešće nisu dokumentovani kao ciljevi u formalnim politikama organizacija. Na primer, od zaposlenih se može očekivati da budu uredno podšišani, da nose konzervativna odijela i da budu ljubazni s korisnicima. OK se formira u toku dužeg vremenskog perioda, koji može da traje i nekoliko godina. Kao i organizaciona struktura, tako i OK može uticati na razvoj i korišćenje informacionih sistema u organizacijama. Tako npr. procedura povezana s novim informacionim sistemom može biti u koliziji s nekim neformalnim proceduralnim pravilima koja su dio organizacione kulture.

Odnos između OK i ponašanja zaposlenih treba uzeti u obzir pri provođenju bezbjedonosne prakse, jer to utiče na način na koji se zaposleni ponašaju u organizacijama (Thomson *et al.*, 2006).

U radu Dhillon-a dodatno je naglašeno da ako sigurnosna kultura ne prevladava u organizacijama, te će organizacije biti u problemima za održavanje integriteta i zaštitite tehničkih sistema organizacije (Dhillon, 1997). Od 1996. godine, mnogi autori su predlagali da IBK mora biti integrisana sa OK kao uputstvo o ponašanju zaposlenih u održavanju informacione bezbjednosti (Dhillon, 1997; James, 1996; Andress & Fonseca, 2000; Breidenbach, 2000; Von Solms, 2000). U istraživanju grupe autora, IBK je prepoznata kao skup uvjerenja i poštovanja određenih vrijednosti, koje se manifestuju u postupcima i ponašanju zaposlenih kao i u zaštiti podataka organizacije (Ramachandran *et al.*, 2008).

Kroz ispitivanje definicija OK i IBK, ustanovljeno je da postoje argumenti koji ove pojmove povezuju. Godinama unazad, IBK ostaje kao jedan od najviše rangiranih oblasti rada akademskih istraživača i praktičara. Na primjer, Vijeće Organizacije za ekonomsku saradnju i razvoj (OECD) posebno je definisalo smjernice za postizanje željenog stepena IBK u organizacijama (OECD, 2002, 2003, 2005). Nakon toga, mnogi naučni radnici predložili se da IBK treba biti dio OK i podržavati sve aktivnosti koje se bave informacijama u organizacijama (Schlienger & Teufel, 2003; Von Solms, 2000). Drugi autori tvrde da bi se slučajevi gdje zaposleni u organizaciji dobrovoljno poštuju pravila organizacije, kao dio OK, mogli smatrati utopijom (Thomson *et al.*, 2006; Von Solms, 2000).

U literaturi su definisane tri vrste (tipa) odnosa između OK i IBK:

- Tip 1: IBK je odvojena od OK;
- Tip 2: IBK je subkultura OK;
- Tip 3: IBK je ugrađena u OK.

Tip 1 odnosi se na situacije u kojima informaciona bezbjednost nije sastavni dio većine OK (Chia *et al.*, 2002). Članovi organizacije često ne učestvuju, ili učestvuju vrlo malo, u provođenju bezbjednosti u organizacijama (Chia *et al.*, 2002). Oni imaju vrlo malo znanja i ne osjećaju da je njihova odgovornost u bezbjedonosnim problemima. Organizacije često imaju tendenciju da troškove u vezi sa bezbjednošću vide kao nepotrebne, a često se bore da smanje sredstva koja se izdvajaju za bezbjedonosne inicijative (Shedden *et al.*, 2006). Takođe, česta je situacija u kojoj je IBK organizacije potpuno odvojena od OK, a svijest o organizacionoj sigurnosti je niska. To je situacija u kojoj se aktivnosti koje se tiču informacione bezbjednosti odnose samo na zaposlene u IT sektoru organizacije.

Organizacije u tipu 2 - veza između IBK i OK predstavlja situaciju u kojoj su članovi organizacija unutar svog odjeljenja ili drugog nižeg oblika organizavanja poslova u organizaciji svjesniji sigurnosnih zahtjeva; povremena obuka za sigurnost se provodi kao poštovanje zahtjeva za upravljanje. Uprava više pažnje posvećuje primjeni informaciono-bezbjedonosne prakse.

U ovakvom tipu organizacija još uvijek je u manjem stepenu zastupljena međuresorna koordinacija u rukovanju informacionom bezbjednošću organizacije. Samo mala grupa ljudi učestvuje ili se uključuje u razvijanje i sprodođenje mjera iz oblasti bezbjednosti informacija i njihovo sprovođenje u organizacijama ovog tipa (Chia *et al.*, 2002). IBK organizacija ovog tipa je mješavina bezbjedonosnih subkultura, u kojoj svaka subkultura svoje potrebe povezuje s odgovornostima i radnim zadacima pojedinih profesionalnih grupa (Ramachandran *et al.*, 2008). IBK je subkultura OK. Ovakva situacija je prisutna, kada su određene vrijednosti prihvaćene od strane određene grupe, kao što je računovodstveni sektor ili sektor upravljanja ljudskim resursima.

Organizacije u tipu 3 odnosa IBK i OK ukazuju na situaciju u kojoj je organizaciona bezbjedonosna praksa odgovornost svih članova organizacije. Sprovođenje mjera bezbjednosti je uvedeno na holistički način i ima relativno visok nivo uključenosti članova.

Osim toga, u organizacijama ovog tipa se vodi računa i o ažuriranju bezbjedonosne politike. Članovi organizacije osjećaju

DOI: 10.15308/Synthesis-2015-321-326

određeni tip vlasništva nad informacijama i oni su motivisani da se pridržavaju bezbjedonosne politike. IBK je ugrađena u OK. Ovakva priroda odnosa je situacija u kojoj postoji razvijena svijest o važnosti zaštite podataka i ona nesvjesno postaje dio dnevnih poslova zaposlenih kao dio njihove rutine (Thomson *et al*., 2006; Von Solms, 2000). Svi članovi organizacije prihvataju važnost IBK koja omogućuje organizacijama donošenje boljih odluka u vezi sa bezbjednosti informacija.

Ovakva klasifikacija organizacija na osnovu tipa odnosa IBK i OK odgovara klasifikaciji organizacija na osnovu kulturoloških stavova prema informacionoj bezbjednosti koju je predložio Fitzgerald (2007). On je istakao da organizacioni kulturološki stavovi prema informacionoj bezbjednosti mogu biti, pojednostavljeno rečeno, visoki, umjereni i niski. Oni su ukratko opisani u nastavku:

- Visoki. Viši nivoi mendžmenta stalno vode računa o informacionoj bezbjednosti u svakom novom projektu koji se implementira u organizaciji. Periodično se vrši ažuriranje akata iz oblasti informacione bezbjednosti na visokom nivou odlučivanja. Zaposleni su svjesni važnosti informacione bezbjednosti i oni znaju kako i kome se trebaju prijaviti bezbjedonosni incidenti, kada

Priroda veze / Kulturni stavovi	Organizaciona kultura	Uvjerenja zaposlenih, akcije i ponašanje (IBK)	Moguće posljedice po bezbjednost
Tip 3 veze: IBK je obuhvaćena OK. (Schlienger & Teufel, 2003; Thomson *et al*., 2006; Von Solms, 2000) Visoki stavovi (Fitzgerald, 2007)	**Uključenost menadžmenta:** Menadžment se bavi bezbjedonosnim pitanjima i strategijama na visokom nivou. **Odgovornost:** upravljanje bezbjednosti uključuje svakog člana organizacije. **Informaciono-bezbjedonosna politika:** Objavljene na holistički načine. Osim toga, tu su i redovne obavijesti o bezbjedonosnoj politici. **Obrazovanje / Obuka:** Menadžment redovno pravi programe i treninge koji su obvezni za sve zaposlene. **Finansiranje:** Menadžment obezbjeđuje finansijska sredstava za pitanja bezbjednosti.	**Odgovornost:** Uvijek se pridržavaju sigurnosnih procedura i uputstava. **Učestvovanje:** Zaposleni prolaze periodično organizovane trening programe za podizanje nivoa bezbjednosti. **Predanost:** Zaposleni osjećaju odgovornost i vlasništvo nad podacima. **Motivacija:** Motivisani i angaživani prema sigurnosnim pitanjima. **Svijest / Znanje:** Znaj kako i kome se obratiti u vezi sa bezbjedonosnim pitanjima i problemima.	**Rizik:** mali. **Svijest:** Zaposlenici su vrlo svjesni i vode računa o bezbjedonosnim pitanjima u organizaciji. **Odgovornost:** Bezbjednost je obaveza svakog zaposlenog. **Bezbjedonosna praksa:** Holistički način. Nesvjesno postaje svakodnevna rutina. **Investiranje u bezbjedonosnu praksu:** Visoki troškovi u sprovođenju bezbjedonosnih aktivnosti.
Tip 2 veze: IBK je subkultura OK (Ramachandran *et al*., 2008) Umjereni stavovi (Fitzgerald, 2007)	**Uključenost menadžmenta:** Menadžment obično delegira pitanja bezbjednosti na IT sektor. **Odgovornost:** Menadžment preusmjerava bezbjedonosna pitanja na rukovodioce sektora. **Informaciono-bezbjedonosna politika:** Stvorena u IT sektoru i nema široku podršku. **Obrazovanje / Obuka:** Menadžment obraća pažnju na svijest. Zaposleni dobijaju neku obuku o informacionoj bezbjednosti. **Finansiranje:** Menadžment djeluje promptno prema troškovima koji se odnose na bezbjedonosne aktivnosti.	**Odgovornost:** Pridržavaju se bezbjedonosnih pitanja kao uslov za upravljanje. **Učestvovanje:** Zaposleni su uključeni oko bezbjedonosnim pitanjima u njihovom sektoru. Manje je izražena međuresorna koordinacija. **Predanost:** Odgovoran i počinio u sigurnosnim pitanjima za vlastite odjelu. **Motivacija:** Zaposlenici su motivisani u vezi sa bezbjedonosnim pitanjima u njihovom sketoru. **Svijest:** Znaju kako i ko se bavi bezbjedonosnim pitanjima kada se suočavaju sa ovom vrstom problema u sektoru.	**Rizik:** Srednji. **Svijest:** Zaposleni su svjesni bezbjedonosnih pitanjaa u njihovom sektoru. **Odgovornost:** Zaposleni su odgovorni za pitanja bezbjednosti u njihovom sektoru. **Bezbjedonosna praksa:** Bezbjednost je rutinska aktivnosti zaposlenog u njegovom sektoru. **Investiranje u bezbjedonosnu praksu:** Srednja veličina troškova u sprovođenju bezbjedonosnih aktivnosti.
Tip 1 veza: IBK odvojena od OK (Chia *et al*., 2002; Shedden *et al*., 2006) Niski stavovi (Fitzgerald, 2007)	**Uključenost menadžmenta:** Menadžment zna važnost informacione bezbjednosti, ali joj dodjeljuje niži nivo važnosti. **Odgovornosti:** Menadžment dodjeljuje svu bezbjedonosnu odgovornost IT sektoru. **Informaciono-bezbjedonosna politika:** Postoji deifinisana politika ali se ne sprovodi. **Obrazovanje / obuka:** Niska svijest. Menadžment ne obraća pažnju na obuku i treninge. **Finansiranje:** Obično dio sredstava za IT podršku.	**Odgovornost:** Ne brinu, i neodgovorne se ponašaju prema bezbjedonosnim pitanjima. **Učestvovanje:** Zaposleni nisu uključeni u aktivnosti vezane za bezbjedonosna pitanja. **Obaveze:** Bezbjedonosna pitanja se prepuštaju IT sektoru. Uvijek se nastoje zaobići bezbjedonosne procedure. **Motivacija:** Zaposlenici nisu motivisani za rad sa bezbjedonosnim pitanjima. **Svijest:** Ne znaju šta učiniti kada se suočavaju sa bezbjedonosnim problemima.	**Rizik:** Visok. **Svijest:** Bez svijesti oko bezbjedonosnih pitanja. **Odgovornost:** Samo IT sektor je odgovoran za pitanja bezbjednosti. **Bezbjedonosna praksa:** Nerutinska aktivnost zaposlenih. **Investiranje u bezbjedonosnu praksu:** Nisko investiranje u sprovođenje bezbjedonosnih aktivnosti.

Tabela 1. Odnos OK, IBK i mogućih posljedica po bezbjednost organizacije
Izvor: Lin *et al. (*2009)

DOI: 10.15308/Synthesis-2015-321-326

god do incidenata dođe. Godišnji budžet se postavlja na takav nivo da je obezbijeđeno finansiranje programa bezbjednosti. Viši menadžment tretira bezbjednost kao reduktor poslovnog rizika i traži od ostalih zaposlenih stalne napore na povećanju informacione bezbjednosti kroz učestovanje u aktivnostima za povećanje bezbjednosti i njihovo finansiranje.

- Umjereni. Zaposleni imaju određeni nivo obuke o informacionoj bezbjednosti. Uloga nadzornika informacione bezbjednosti je dodijeljena određenoj osobi kao regulatoru ili revizoru. Bezbjedonosna pravila su kreirana od strane IT odjeljenja ili sektora, ali to ne znači da se za sprovođenje ovakvih mjera ima snažna podrška. Zaposleni ne znaju gdje se pravila nalaze. Viši menadžment je obično dodijelio poslove vezane za informacionu bezbjednost zaposlenom u IT odjeljenju ili sektoru. Pojedincu su dodjeljena prava za operativne aktivnosti vezane za bezbjednost (lozinke i kreiranje novih naloga za novozaposlene).
- Niski. Informaciono-bezbjedonosna politika u organizaciji može biti izrađena (najčešće samo prekopirana od slične organizacije), ali je organizacija ne sprovodi ili nema ozbiljne namjere za njeno sprovođenje. Obično se mjere predviđene informaciono-bezbjedonosnom politikom upotrebljavaju u slučajevima kada je došlo do incidenata koji utiču na bezbjednost, kao što je razmjena lozinki za pristup podacima. Iako viši menadžment zna da je pitanje informacione bezbjednosti važno, ipak se ovakvim pitanjima dodjeljuje niži nivo važnosti u praksi. Nema posebnog fonda za informacionu bezbjednost i obično se ovaj dio aktivnosti finansira iz predviđenih troškova za IT podršku.

Važnost IBK i dalje raste, sve više i više organizacija se oslanja na podatke koji omogućavaju prednost u odnosu na konkurenciju u dinamičnom okruženju. Dakle, organizaciji je potrebna IBK, koja će voditi postupke i ponašanje zaposlenih u zaštiti podataka organizacije. Veza između klasifikacija organizacija koje su do sada predstavljene data je u tabeli 1.

U prvoj koloni tabele prikazani su tipovi veza i kultoroloških stavova, a njihv odnos može se smatrati kontinuitetom u rasponu od IBK nije dio OK, do IBK je ugrađena u potpunosti u OK. Druga kolona tabele prikazuje odnos organizacione kulture prema informaciono-bezbjedonosnoj praksi u organizacijama. Nivo učestvovanja menadžmenta i njehovo podržavanje u smislu uspostave bezbjedonosne strategije, raspored odgovornosti, učestvovanje, pružanje mogućnosti obuke, obrazovanja i treninga, kao i obezbjeđivanje finansijskih sredstava za njegovo sprovođenje može biti u rasponu od niskog do visokog. Treća kolona pokazuje djelovanje i ponašanje zaposlenih u odnosu na informaciono-bezbjedonsnu praksu. Na nivou gdje je IBK odvojena od OK, zaposleni ne brinu o odgovornosti prema bezbjedonosnim pitanjima. Zaposleni ne učestvuju u bezbjedonosnim pitanjima, a ta pitanja su ostavljena za IT sektor. Oni ne znaju kako i šta učiniti kada se suoče sa bezbjedonosnim pitanjima. Na suprotnoj strani odnosa, gdje je IBK u potpunosti ugrađen u OK, ponašanje i rad zaposlenih su uvijek u skladu sa informaciono-bezbjednosnom politikom i definisanim procedurama. Zaposleni periodično prolaze programe o bezbjednosti, osjećaju odgovornost i vlasništvo nad informacijama i prema bezbjedonosnim pitanjima. Oni znaju šta treba učiniti i koga treba obavestiti, kada se suoče sa bezbjedonosnim problemima. Četvrta kolona pokazuje moguće posljedice koje organizacija može imati sa bezbjedonosnim pitanjima, zavisno o njihovom trenutnom položaju u tabeli. Organizacije u kojima je IBK odvojena od OK mogu imati najniže troškove u sprovođenju mjera bezbjednosti, ali u isto vrijeme one se suočavaju s najviše ranjivost. S druge strane, organizacije u kojima je IBK u potpunosti ugrađen u OK mogu imati najniži rizik, ali to uključuje visoke troškove u sprovođenju mjera bezbjednosti.

6. REZIME

Teorijski posmatrano, da bi IBK uključili u OK, svi članovi organizacije moraju prihvatiti važnost IBK. Sa pravim fokusom, organizacije mogu brže promeniti nivo informacione bezbjednosti od niskog do visokog.

Ostaje pitanje zašto IBK još uvijek nije u potpunosti primenjen u organizacijama. U ovom radu je predstavljen okvir za bolje razumijevanje uticaja OK na bezbjednost informacija u organizaciji, kao i veza između IBK u organizaciji kao cjelini, pojedinaca koji čine tu organizaciju (menadžment, ostali zaposleni) i OK. Takođe, predstavljeni okvir daje određene smjernice menadžmentu ka boljem organizovanju obuke i treninga za poboljšanje stanja informacione bezbjednosti u organizaciji. Osnovni nedostatak predloženog okvira je njegov izvor koji se nalazi u pregledanoj literaturi iz ove oblasti, a koji još nije ispitan u praktičnom djelovanju. Okvirom nisu obuhvaćene konkretne mjere koje se mogu realizovati u svakoj specifičnoj organizaciji. Svaka organizacija svoje poslovanje i aktivnosti usmjerava ka poboljšanjima svog poslovanja, povećanju profita (profitno orjentisane organizacije), ili poboljšanju pružanja usluga (neprofitne organizacije uključujući i organizacije državne uprave i lokalne samouprave). IT sektori u organizacijama svih tipova posebnu pažnju posvećuju fizičkim i tehničkim mjerama bezbjednosti, dok se socijalnim i posebno kulturološkim faktorima koji utiču na informacionu bezbjednost organizacije posvećuje mala ili nikakva pažnja. Značajne aktivnosti u poboljšanju stanja OK i IBK, kao dijela bezbjednosti informacionh sistema organizacije, potrebno je preduzeti od najvišeg nivoa rukovođenja organizacijama, pa do hijerarhijski najnižeg nivoa rada u organizacijama, kako bi se poboljšala bezbjednost informacija u organizaciji. Naravno, ovo iziskuje povećanje, prije svega finansijskih troškova što je i osnovna barijera u preduzimanju mjera poboljšanja nivoa OK u organizacijama koje se trenutno, po mišljenju autora, na prostorima bivše SFRJ nalaze na vrlo niskom nivou, uz pojedinačne izuzetke.

LITERATURA

Andress, M., & Fonseca, N. (2000). Manage People to Protect Data. Infoworld, 22(46), 48.

Atkinson, P. (1997). Creating culture change: Strategies for success. Bedfordshire, England: Rushmere Wynne.

Barlas, S., Queen, R., Radowitz, R., Shillam, P., & Williams, K. (2007) Top 10 technology concerns (streetwise). *Strategic Finance*

Beach, L.R. (1993). *Making the right decision. Organizational culture, vision and planning.* Eaglewood Cliffs, New Jersey: Prentice Hall.

Blyth, A. & Kovacich, G. (2006). *Information assurance: Security in the information IT security risks*. Woburn, MA: Butterworth-Heinemann.

Breidenbach, S. (2000). How Secure Are You? *Information Week* 2000; 800:71-8

Carroll, M.D. (2006). Information security: Examining and managing the insider threat. *Computer and Information Science*, 156-158. DOI: 10.1145/1231047.1231082

Chang, S.H., & Ho, C.B. (2006). Organizational factors to the effectiveness of implementing information security management.

DOI: 10.15308/Synthesis-2015-321-326

Industrial Management & Data Systems, 106(3), 345-361. DOI: 10.1108/02635570610653498

Chang, S. E. & Lin, C. (2007). Exploring organisational culture for information security management. *Industrial Management & Data Systems*, 107(3), 438-458.

Chia, P., Maynard, S. & Ruighaver, A. B. (2002). Exploring Organizational Security Culture: developing a comprehensive research model, IS ONE World Conference, Las Vegas, Nevada USA

Colwill, C. (2010.) Human factors in information security: The insider threat - Who can you trust these days? *Information Security Tech*nical Report, 14(4), 186-196. DOI: 10.1016/j.istr.2010.04.004

Da Veiga, A. & Eloff, J.H.P. (2010) A framework and assessment instrument for information security culture, *Computer & Security*, 29, 196-207.

Deal T.E. & Kennedy A. A. (1982). *Organization cultures: the rites and rituals of organisation life.* Reading, UK: Addison-Wesley.

Detert J. R., Schroeder R. G. & Mauriel J. I. (2000). A Framework for Linking Culture and Improvement in Organizations, *Academy of Management Review*, 25(4), 850-863

Dhillon G. (1997). *Managing Information System Security*. Houndmills, Basingstoke, Hampshire: Macmillan Press LTD

Dhillon G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal*, 16, 293-314.

Duffy J. (1999). *Harvesting experience: reaping the benefits of knowledge*, ARMA International, Kansas, USA

Guptara P. (1994). Lessons of experience – learning from others, D. Lock (ed.) *Handbook of Quality Management*, Gower, Aldershot

Fitzgerald, T. (2007). Building Management Commitment through Security Councils, or Security Council Critical Success Factors, H. F. Tipton (Ed.), *Information Security Management Handbook*, Hoboken: Auerbach Publications, pp. 105-121.

Hagberg Consulting Group (2009). *Corporate culture/organisational culture: understanding and assessment.*

Helokunnas, T., & Kuusisto, R. (2003). Information Security Culture in a Value Net. IEEE International Engineering Management Conference. DOI: 10.1109/IEMC.2003.1252258

Hofstede G. (2001). *Culture's consequences: Comparing values, behaviors, institutions, and organizations across nations*. Thousand Oaks, Calif: Sage Publications, Inc.

Jakovljević, D., & Grujić, V. (1998). *Menadžment u zdravstvenim ustanovama.* Beograd: Evropski centar za mir i razvoj.

James H.L. (1996). *Managing Information Systems Security: A Soft Approach*. IEEE

Knapp, K.N., Morris Jr., R.F., Marshall, T.E., & Byrd, T.A. (2009). Information security policy: An organizational-level process model. Computers & Security, 28(7), 493-508.

Kros, J.R., Foltz, C.B., & Metcalf, C.L. (2004/2005). Assessing & quantifyingthe loss of network intrusion. *Journal of Computer Information Systems*, 45(2), 36-43.

Lin, J. S., Chang, S., Maynard, S. & Ahmad, A. (2009). Exploring the Relationship between Organizational Culture and Information Security Culture. Dostupno na http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1011&context=ism

OECD. (2002). *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*, Recommendation of the OECD Council, 1037th Session on 25 July 2002.

OECD. (2003). *Implementation Plan for OECD Guides for the Security of Information Systems and Networks: Towards a Culture of Security*. Dostupno na http://www.oecd.org/internet/ieconomy/31670189.pdf

OECD. (2005). *The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries*. Dostupno na http://www.oecd.org/internet/ieconomy/35884541.pdf

Ramachandran, S., Srinivasan, V.R. & Tim, G. (2008). Information Security Cultures of Four Professions: A Comparative Study, Proceedings of the 41st Hawaii International Conference on System Sciences - 2008, Hawaii

Schein, E.H. (1992). *Organizational Culture and Leadership*: San Francisco: Jossey-Bass,

Schlienger, T., & Teufel, S. (2003). Analyzing information security culture: increased trust by an appropriate information security culture. 405-409.

Shedden, P., Ahmad, A. & Ruighaver, A.B. (2006). Risk Management Standard-the Perception of Ease of Use, Proceedings of the fifth annual security conference, Las Vegas, Nevada, USA.

Thomson, K., von Solms, R., & Louw, L. (2006). Cultivating an Organizational Information Security Culture. *Computer, Fraud & Security*, 2006(10), 7-11.

Von Solms, B. (2000). Information Security - the Third Wave? *Computers & Security*, 19(7), 615-620.

Wright, P.M., & Boswell, W.R. (2002). Desegregating HRM: A review and syntehesis of micro and macro human resource management. *Journal of Management*, 28(3), 247-276. DOI: 10.1177/014920630202800302

DOI: 10.15308/Synthesis-2015-321-326