UDK: 351.78:316.7

Originalni naučni rad

INFORMACIONO-BEZBEDNOSNA KULTURA – IMPERATIV SAVREMENOG DRUŠTVA[1]

Zoran Milanović[2]
Radovan Radovanović[3]
Kriminalističko-policijska akademija, Beograd

Sažetak: Značaj izgradnje informaciono-bezbednosne kulture svakog društva postala je dobro utemeljena ideja. Cilj takve kulture je uticaj na različita ljudska ponašanja koja se mogu odraziti na ukupne rezultate zaštite informacione imovine.

Autori rada smatraju da je kultura „ključ" informacione bezbednosti.

Obimnim pregledom i analizom literature o informacionoj bezbednosti došlo se do zaključka da je kolektivna svest o upotrebi informacionih tehnologija i zaštiti u domenu savremenih oblika kriminaliteta na veoma niskom nivou.

U tom smislu, cilj rada je da se, razmatranjem informaciono-bezbednosne kulture sa stanovišta najbolje prakse, podrži stav da znanje i obrazovanje igraju važnu ulogu u izgradnji bezbednog ambijenta sa posebnim akcentom na podizanju svesti krajnjih korisnika o potrebi i važnosti zaštite podataka, informacija i znanja.

Ključne reči: Informacione tehnologije, informaciono-bezbednosna kultura.

Uvod

Informaciono-bezbednosna kultura jeste imperativ savremenog društva. Razlozi za to su mnogobrojni i raznovrsni.

1 Ovaj rad je rezultat realizovanja internog projekta „Forenzički metodi u kriminalistici"
2 Nastavnik kriminalističko-policijskih i bezbednosnih veština, *zoran.milanovic@kpa.edu.rs*.
3 Redovni profesor, *radovan.radovanovic@kpa.edu.rs.*

Informacione tehnologije danas predstavljaju najvažniji segment ljudske zajednice koji je promenio njihov način života, učenja, rada i zabave. Takođe, velika ljudska zavisnost od informacionih tehnologija prouzrokovala je da sve bitne odlike društva dobiju prefiks „informacioni". Tako i bezbednost kao osnovna potreba pojedinca i društva u celini postaje informaciona bezbednost, a kultura, temelj svakog društva, dobija još jedan aspekt u vidu informaciono-bezbednosne kulture.

Informaciono-bezbednosna kultura je proizvod individualnih i grupnih vrednosti, stručnosti i obrazaca ponašanja koji karakterišu posvećenost, stil i znanje usmereno ka „zdravoj atmosferi" u organizaciji i upravljanju bezbednošću.

Glavne okosnice rada su informaciona bezbednost i kultura, koje se uzajamno prožimaju i prepliću. Sa ciljem što boljeg razumevanja ovih fenomena, oni će biti pojedinačno razmatrani, kao i njihov sinergijski uticaj na društveno-poslovni ambijent.

1. O bezbednosti i kulturi

Bezbednost je jedna od osnovnih ljudskih potreba[4]. Biti bezbedan znači biti zaštićen od uticaja neželjenih pojava i osećati se zaštićenim (sigurnim, bez straha) u predvidivom i kontrolisanom ambijentu[5]. Prema Oksfordskom rečniku, bezbednost se definiše kao „stanje bez opasnosti ili pretnje"[6].

Autori Vitman i Maturd[7] bezbednost u najopštijem smislu, definišu kao „kvalitet ili stanje biti bezbedan – biti oslobođen od opasnosti", tj. kao zaštitu od opasnosti koje će učiniti štetu, namerno ili na drugi način. Navedena definicija se može posmatrati i u kontekstu nacionalne bezbednosti, kao zaštita spoljnopolitičkih interesa u međunarodnim odnosima – zaštita teritorije od spoljne agresije, pri čemu je u središtu dešavanja bezbednost ljudi i njihovo učestvovanje u globalnoj bezbednosti[8]. Može se posmatrati i u kontekstu organizacione bezbednosti, gde je strateški cilj sačuvati svoja sredstva, resurse i ljude u dinamičnom i kompleksnom okruženju.

Ključni segment savremene bezbednosti, koji se razmatra i u kontekstu nacionalne, a i organizacione bezbednosti, jeste informaciona bezbednost.

Glavna filozofija informacione bezbednosti nije da ukloni sav rizik, niti da određuje način poslovanja, već da korisnicima informacionih tehnologija (u

4 A. Burke, *Aporias of Security*, Alternatives: Global, Local, Political 27(1), 2002, str. 1–27.
5 S. Mijalković i saradnici, *Korelacija informacione i nacionalne bezbednosti*, Savetovanje o zloupotrebi IT – ZITEH, Beograd, 2010, dostupno na: *http://www.singipedia.com/content/1057-Korelacija-informacione-i-nacionalne-bezbednosti* (20. 12. 2015).
6 Oxford Dictionaries, dostupno na: *http://www.oxforddictionaries.com/definition/english/security* (20. 12. 2015).
7 M. Whitman, H. Mattord, *Principles of Information Security*, Fourth Editional, Course Technology, Cengage Learning, 2012.
8 S. Mijalković, *Nacionalna bezbednost – od vestfalskog koncepta do posthladnoratovskog*, Vojno delo 2, 2009, str. 55–73, Beograd, dostupno na: *http://www.odbrana.mod.gov.rs/odbrana-stari/vojni_casopisi/arhiva/VD_2009-2/Vono%20delo%20br.%202-2009.pdf* (20. 12. 2015).

svim svojim segmentima i slobodama) omogući da koriste pogodnosti i dobrobiti koje im savremene tehnologije nude: na Internetu, u lokalnoj mreži ili kod potpuno izolovanih računarskih sistema. Informaciona bezbednost pored zaštite privatnosti i neometanog korišćenja IT, treba da obezbedi i zaštitu intelektualne i materijalne informacione imovine korisnika i korporacija.

Nije moguće dati apsolutni odgovor na pitanje kako i na koji način ostvariti ovu filozofiju. Borba u virtualnom svetu se vodi kao i u realnom životu; to je „borba dobra i zla" koja neprestano traje, od samog početka kada su se ove tehnologije pojavile.

Takođe, jedan od njenih važnih zadataka jeste i čuvanje ugleda korisnika i korporacija od različiti kompromitacija i prevara[9].

Posebno je važno to što su problemi sa kojima se informaciona bezbednost susreće daleko složeniji od tehničkih rešenja ili proizvoda. To potvrđuje i izjava stručnjaka za bezbednost Šnejera: „Ako mislite da tehnologijom možete rešiti vaš bezbednosni problem, onda ne razumete ni problem ni tehnologiju".[10]

Informaciona bezbednost podrazumeva veoma složene procese koji obuhvataju različite aspekte korišćenja i zaštite informacionih tehnologija, a pre svega postupak definisanja odgovornosti za sve učesnike u tim sistemima, jer su oni uglavnom najosetljivije mesto u svakoj bezbednosnoj šemi. Faktor „čovek" može da poništi i najbolju zaštitu: zlonameran radnik, nepažljiv radnik, radnik koji nije svestan politike i važnosti bezbednosti sistema u celini (organizacije)[11], a pre svega bezbednosti informacione imovine kao njegovog ključnog elementa.

Iz svega navedenog može se konstatovati da informaciona bezbednost predstavlja temelj bezbednosti u najširem smislu i kao takva postaje prioritetna za očuvanje poslovnih i svih drugih državnih i društvenih dobara i procesa.

Prvi korak u kreiranju ovog ambijenta, tj. uređenog sistema bezbednosti, treba započeti izgradnjom kulture društva odnosno u kontekstu rada, informaciono-bezbednosnom kulturom korisnika informacionih tehnologija.

Svako društvo i svaka organizacija su jedinstveni i imaju svoju kulturu i potkulturu. Reč kultura je latinskog porekla, a znači obrađivanje, negovanje. Slično značenje ima i reč civilizacija koja je takođe latinskog porekla a znači oplemenjivanje, uglađivanje[12]. Prema Oksfordskom rečniku[13], kultura se definiše kao: ideje, običaji i društvena ponašanja određenog naroda ili grupe ljudi.

9 Prevara je složeno krivično delo i potrebno je da bude ispunjeno više uslova: umišljaj, namera, dovođenje u zabludu, a sa ciljem pribavljanja imovinske koristi sebi ili drugom ili nanošenje štete. Prevare predstavljaju najraširenij oblik kompjuterskog kriminaliteta. Dostupno na: *http://www.prevare.info/01_zakon.html* (20. 12. 2015).

10 B. Schneier, 2015, RM Education, dostupno na: *https://www.rm.com/sustrort/technicalarticle.asp?cref=tec377232* (20. 12. 2015).

11 Z. Milanović, *Organizacioni model implementacije bezbednosne politike u obrazovnim ustanovama*, Savetovanje o zloupotrebi IT – ZITEH, Beograd, 2006.

12 Oxford Dictionaries, dostupno na: *http://dictionary.reference.com/browse/culture* (20. 12. 2015).

13 Oxford Dictionaries, http://www.oxforddictionaries.com/definition/english/culture

Takođe, u literaturi se mogu naći različita objašnjenja i shvatanja kulture, kao na primer autora Palispisa[14]:

- Kultura predstavlja dizajn ili recepte za život – međusobno povezanih mreža, normi i uloga. Ona obuhvata modele razmišljanja, osećanja i delovanja koji se obično mogu naći u društvu i uključuje sve što je čovek stekao kao član tog društva;
- Kultura je, dakle: (a) karakterističan proizvod ljudske interakcije; (b) složeno društveno nasleđe koje se prenosi kroz društvo. To je naučeno ponašanje koje se deli sa drugima; (c) sastoji se od eksplicitnih i implicitnih prihvatljivih obrazaca za ispunjavanje bioloških i društvenih potreba, a ponašanje se sticalo i prenosilo simbolima, koji predstavljaju karakteristična dostignuća ljudskih grupa. Bitno jezgro kulture čine tradicionalne ideje i njihove promovisane vrednosti; (d) kumulativna je jer se prenosi sa generacije na generaciju u datom društvu; (e) čista je apstrakcija; (f) ljudima pruža smisao jer je simbol kvaliteta; (g) naučena je od svake osobe, kao osnova koja determiniše njenu ličnost i (h) zavisi od dužine kontinuiranog funkcionisanja društva, ali je nezavisna od bilo koje specifične grupe;
- Srce kulture nalazi se u pronalasku i upotrebi alata, a pre svega u sposobnosti ljudi da uče iz grupe kojoj pripadaju.

Značaj i uticaj kulture na ljude, kao i sve veća potreba za njihovom bezbednošću, doveli su do nove naučne discipline – bezbednosne kulture. Od nje se očekuje da kod ljudi podigne svest na prihvatljiv nivo, a time i promenu njihovih ustaljenih ponašanja, u bezbedna: raditi prave stvari, na pravi način, na pravom mestu i u pravo vreme.

Konačno, društveni tokovi promovišu opštu informatičku pismenost i kulturu kao glavne odrednice vremena u kome živimo.

1.1. Bezbednosna kultura

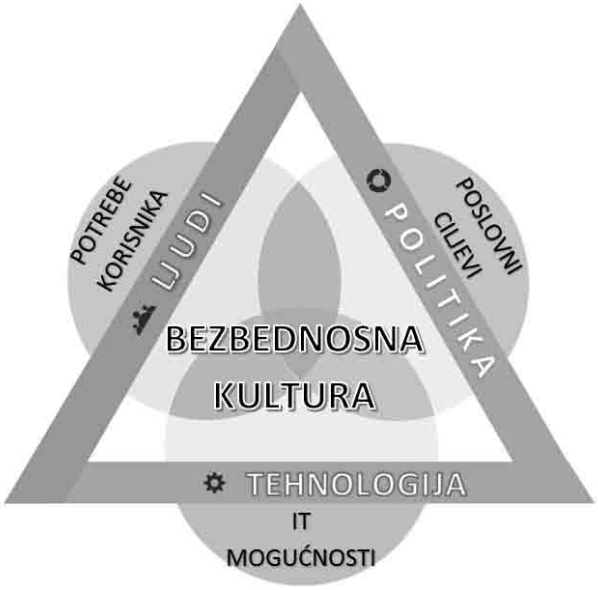
Prema „Pojmovniku bezbednosne kulture", „pod bezbednosnom kulturom može se podrazumevati bezbednosna aktivnost koja izražava spremnost delovanja i ponašanja u skladu sa stečenim znanjima i veštinama, kao i u skladu sa prihvaćenim vrednosnim stavovima". Takođe, bezbednosna kultura „ogleda se u prepoznavanju opasnosti, reagovanju na njih izbegavanjem opasnosti, otklanjanjem opasnosti ili upućivanjem na one subjekte koji će profesionalno reagovati i sačuvati ugrožene vrednosti."[15].

Bezbednosna kultura treba da pomogne korisnicima da razumeju rizik i treba da ih nauči adekvatnim odgovorima.

14 E. Palispis, *Introduction to "Sociology and Anthropology"*, Rex Book Store, Inc. and Epitacio S. Palispis, Philistrine, 2007, str. 42–43. Dostupno na: *http://books.google.rs/books?id=PtPLp_wuECkCC&printsec=frontcover&hl=sr&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false* (20. 12. 2015).

15 S. Stanarević, F. Ejdus, *Pojmovnik bezbednosne kulture*, Centar za civilno-vojne odnose, Beograd, 2009. Dostupno na: *http://www.wbrc.rs/wp-content/uploads/2012/11/Pojmovnik-bezbednosne-kulture-grupa-autora-2009.pdf* (20. 12. 2015).

Prema mišljenju Stajića i saradnika,[16] bezbednosna kultura predstavlja skup usvojenih stavova, znanja, veština i pravila iz oblasti bezbednosti, ispoljenih kao ponašanje i proces, o potrebi, načinima i sredstvima zaštite ličnih, društvenih i međunarodnih vrednosti od svih izvora, oblika i nosilaca ugrožavanja, bez obzira na mesto ili vreme njihovog ispoljavanja. Bezbednosna kultura je u tesnoj vezi sa našim vaspitanjem, vrednostima i vrednosnim sistemima koje podržavamo. Promena bezbednosne kulture kod korisnika nije ni lak ni brz proces.



Slika 1: Elementi bezbednosne kulture

Bezbednosna kultura korisnika informacionih tehnologija reflektuje se, direktno ili indirektno, na njihovu ukupnu bezbednost i zaštitu od rizika kojima su izloženi.

Shodno iznetim obrazloženjima i definicijama, mogu se konstatovati tri glavna elementa koja zajedno čine bezbednosnu kulturu (slika 1): tehnologija, politika (pravila) i njihovi korisnici[17]. Ova tri elementa su u neraskidivoj interakciji i svaki od njih direktno utiče na druga dva. Ljudi politikom utiču na način upotrebe tehnologije, a svakodnevni razvoj novih tehnologija zahteva i nove politike.

Društveno ponašanje, ideje i običaji su u velikoj meri zasnovani na politikama. Neke su napisane u zakonima, propisima i standardima. Ostale (većina njih, u stvari) jesu nepisana pravila i dolaze u obliku etike, moralnih kodeksa, kao i u međusobnim idejama o tome šta je prihvatljivo ponašanje u različitim grupama kojima pojedinac pripada.

Politike, pravila i zakoni su deo osnovnog funkcionisanja ljudskog uma.

16 Lj. Stajić, S. Mijalković, S. Stanarević, *Bezbednosna kultura mladih: kako živeti bezbedno*, Draganić, Beograd, 2006.
17 K. Roer, *Build a Security Culture*, IT Governance Publishing, United Kingdom, 2015.

Konkretno, za uspostavljanje elemenata bezbednosne kulture u organizacijama neophodno je sprovesti i ostvariti pet ključnih komponenti bezbednosne kulture (slika 2).[18]

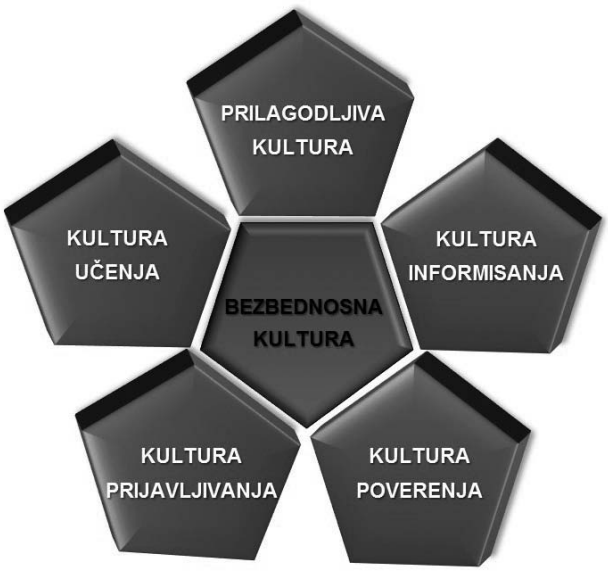
1) Kultura informisanja (*Informed culture*) – u organizaciji se prikupljaju i analiziraju relevantni podaci i aktivno distribuiraju bezbednosne informacije i saveti na osnovu te analize.

2) Kultura poverenja (*Just culture*) podrazumeva prepoznavanje prirodnih ograničenja ljudskog učinka. Kultura poverenja ukazuje da greške i nebezbedne akcije korisnika neće biti kažnjene ako su bile nenamerne. Međutim, oni koji se ponašaju nepromišljeno, ili neopravdano preuzimaju određene rizike, biće disciplinski kažnjeni.

3) Kultura prijavljivanja, tj. izveštavanja (*Reporting culture*), predstavlja stvaranje atmosfere u kojoj ljudi imaju poverenja da prijave bezbednosne probleme bez straha od krivice, i čak se podstiču i nagrađuju za pružanje informacija vezanih za bezbednost. Zaposleni moraju da znaju da će biti ostvarena kultura poverenja i da će se postupiti po podnetim informacijama, u suprotnom će odlučiti da nema koristi od njihovog izveštavanja.

4) Kultura učenja (*Learning culture*) potvrđuje da je organizacija u stanju da uči iz svojih grešaka i da je spremna da napravi promene. Svrha kulture učenja je da ljudi razumeju procese bezbednosnog menadžment sistema na ličnom primeru.

5) Prilagodljiva kultura (*Flexible culture*) jeste ona u kojoj su organizacija i ljudi sposobni da se efikasno prilagođavaju promenljivim zahtevima.



Slika 2: *Pet ključnih komponenti bezbednosne kulture*[19]

18 Air Safety Sustrort International, dostupno na: *http://www.airsafety.aero/Safety-Information-and-Reporting/Safety-Management-Systems/Safety-Culture.aspx* (20. 12. 2015).
19 Bezbednost, dostupno na: *http://www.smatsa.rs/Lat/PrintShowContent.aspx?mi=32* (20. 12. 2015).

Kada je svako u organizaciji obučen da radi svoj posao na bezbedan način i proaktivno prepoznaje opasnosti, može se postići viši nivo bezbednog ponašanja. Svi elementi bezbednosne kulture moraju biti aktivno isticani i demonstrirani od strane menadžmenta kako bi se zaposleni redovno podsticali da učestvuju u ostvarivanju i održavanju projektovanog nivoa bezbednosne kulture.

Program koji donosi bezbednosna kultura usmeren je ka uspehu samo ako ga prihvate svi učesnici.

1.2. Uticaj bezbednosne kulture na podizanje svesti o bezbednosti

Svest o bezbednosti prestavlja veoma ograničenu i slabo definisanu oblast. Ne postoji opšteprihvaćena definicija koja opisuje svest korisnika o informacionoj bezbednosti, što zauzvrat znači da ne postoji ni zajedničko razumevanje svesti o bezbednosti.

Prema Oksfordskom rečniku, svest je „znanje ili percepcija situacije ili činjenica".[20] Ta definicija se svodi na dve stvari: primeniti odgovarajući nivo stručnosti i sposobnosti na nadležnost u određenoj situaciji.

Glavna razlika između svesti o bezbednosti i bezbednosne kulture je u tome što je kultura mnogo više nego svest. Bezbednosna kultura je kombinacija ljudi, politike (pravila) i tehnologije, dok je svesnost vezana samo za ljude i predstavlja njihovo znanje. Svest se može posmatrati i kao kompetentnost ljudi da urade pravu stvar. Ključ je u razmatranju kompetencija kao jednog od načina izgradnje kulture, a ne cilj sam po sebi.

Svest o bezbednosti pomaže ljudima da shvate ili budu svesni važnosti edukacije i treninga vezanih za bezbednost. Znati nešto nije isto kao i promeniti ponašanje i stečene navike. Cilj treninga je zapravo praktična primena novostečenih znanja i promena ponašanja pri korišćenju novih tehnologija, a znanje o nečemu je samo jedan korak ka promeni tog ponašanja.

U kognitivnom procesu sticanja novih znanja izdvajaju se četiri koraka: pažnja, pamćenje, reprodukcija i motivacija[21]. Svi oni su podjednako važni pri edukaciji korisnika i podizanju njihove svesti na viši nivo.

2. Informaciono-bezbednosna kultura

Činjenica da ogromna većina korisnika informacionih tehnologija nema elementarno obrazovanje, niti minimalna znanja iz oblasti informatike, predstavlja poseban problem, koji ih sputava u jasnom definisanju i iskazivanju sopstvenih zahteva i potreba, kao i u sagledavanju stvarnih mogućnosti, prednosti i ograničenja digitalnog života.

20 Oxford Dictionaries (2015), http://www.oxforddictionaries.com/definition/english/awareness.
21 A. Bandura, 1999, dostupno na: *http://www.muskingum.edu/~psych/psycweb/history/bandura.htm* (20. 12. 2015).

Osnovu za rešavanje ove problematike mnogi autori i naučni istraživači videli su u informaciono-bezbednosnoj kulturi, sagledavajući je sa različitih aspekata, iz čega je, takođe, proizašao veliki broj njenog tumačenja i definisanja. Prema Čiji i saradnicima, ne postoji jedna, jasna i opšteprihvaćena definicija informaciono-bezbednosne kulture.[22] Neke od najčešće navođenih su sledeće:

- Dilon[23] definiše bezbednosnu kulturu kao „sveukupnost ljudskih osobina, kao što su ponašanje, stavovi i vrednosti, koje doprinose zaštiti svih vrsta informacija u datoj organizaciji".
- Solms[24] poziva na stvaranje informaciono-bezbednosne kulture u okviru organizacije, tako što će se „svakom zaposlenom usaditi informaciono-bezbednosni aspekat kao rutina u vršenju svakodnevnog posla".
- Martins i Elof[25] opisuju je kao proizvod ponašanja zaposlenih u vezi sa informacionom bezbednošću, koja tokom vremena prerasta u „načine na koje se rade stvari".
- Šlajnger i Tujfel[26] definišu informaciono-bezbednosnu kulturu kao „sve društveno-kulturološke mere koje podržavaju aktivnosti tehničkih metoda, tako da informaciona bezbednost postaje prirodan aspekt dnevnih aktivnosti svakog zaposlenog".
- Kizisto i saradnici[27] navode da „proces formiranja bezbednosne kulture podrazumeva uključivanje skupa vrednosti svih zainteresovanih strana"; oni tvrde da, ako se objedine vrednosti svih članova organizacije, onda se objedinjena kultura može formirati za manje od nekoliko godina; međutim, ako vrednosti svih u organizaciji nisu jedinstvene, onda je za proces formiranja bezbednosne kulture potrebno značajno više vremena;
- Gou i saradnici[28] definišu informaciono-bezbednosnu kulturu kao način na koji „zaposleni i organizacija kao celina rade stvari (tj. kako prihvataju ponašanje i aktivnosti) koje se odnose na informacionu bezbednost";
- Roer[29] u knjizi „Izgradnja bezbednosne kulture", ističe: Bezbednosna kultura pomaže i olakšava ljudima da koriste informacione tehnologije na zadovoljavajući način, bez opasnosti i pretnji.

22 A. Chia, B. Ruighaver, B. Maynard, *Understanding Organizational Security Culture*, Proceeding of PACIS Japan, 2002.
23 G. Dhillon, *Interpreting the Management of Information Systems Security*, London School of Economics and Political Science, London, 1995.
24 B. Solms, *Information security – The third wave? Computers & Security*, 19(7), 2000, str: 615–620.
25 A. Martins, J. Eloff, *Information security culture*. In: IFIP TC11 international conference on information security, Cairo, Egypt, 2002, str: 7–9.
26 T. Schlienger, S. Teufel, *Information security culture – from analysis to change*, International institute of management in telecommunications, University of Fribourg, 2003. Dostupno na:*http://icsa.cs.up.ac.za/issa/2003/Publications/INFORMATION%20SECURITY%20CULTURE.pdf* (20. 12. 2015).
27 T. Kuusisto, I. Ilvonen, *Information security culture in small and medium size enterprises*. Frontiers of E-business Research, 2003.
28 L. Ngo, V. Zhou, M. Warren, *Understanding transition towards information security culture change*. In: Proceedings of the third Australian information security management conference, Perth, Australia, 2005.
29 K. Roer, *Build a Security Culture*, IT Governance Publishing, United Kingdom, 2015.

Informaciono-bezbednosnu kulturu su na sličan način definisali i drugi istraživači, uključujući Kizista i Ilvonena[30], Vruma i Solmsa[31] i Tomsona i saradnike[32].

U svetlu gore navedenih definicija, može se zaključiti da se informaciono-bezbednosna kultura u okviru organizacije manifestuje kroz različite aspekte bezbednosti koji se odnose na: vrednosti, ponašanja, stavove, akcije, aktivnosti menadžmenta, kao i fizičko okruženje.

Istraživači su primenili teorije nastale iz različitih perspektiva kao osnove za istraživanje informaciono-bezbednosne kulture: perspektiva organizacione kulture[33],[34], perspektiva organizacionog ponašanja[29], perspektiva upravljanja znanjem[30], perspektiva komunikacije[35], perspektiva upravljanja promenama[36] i perspektiva menadžmenta totalnim kvalitetom[37].

U nekim studijama bezbednosno-informaciona kultura je posmatrana u okviru nacionalne kulture, dok je u drugima fokus bio na organizacionoj kulturi[29,31,32,33,38]. Rezultati tih studija ukazuju da organizacije moraju da preduzmu pozitivne korake za stvaranje ambijenta u kome je bezbednost „odgovornost svakog pojedinca" i gde je obaveza raditi „pravu stvar".

2.1. Informaciono-bezbednosna kultura mladih i dece

Nedostatak bezbednosne kulture najviše pogađa decu i mlade, i to kako zbog njihovog posebnog mesta u sistemu zaštite, tako i zbog njihove naivnosti. Prema Mišelu Sen Lou[39], direktoru UNICEF-a u Srbiji, „sve više dece koristi digitalne alatke za učenje, društveno angažovanje i druženje. Međutim, putem njih se izlažu i novim rizicima – nasilju, neprikladnom sadržaju, nepoznatim ljudima, a rizik za njihov razvoj predstavlja i prekomerna upotreba digitalnih sadržaja".

30 T. Kuusisto, I. Ilvonen, *Information security culture in small and medium size enterprises*. Frontiers of E-business Research, 2003.
31 C. Vroom, R. Solms, *Towards information security behavioral compliance*. Computers & Security, 23(3), 2004, str: 191–198.
32 K. Thomson, R. Solms, L. Louw, *Cultivating an organizational information security culture*. Computer Fraud & Security. 10, 2006, str. 7–11.
33 O. Zakaria, *Understanding challenges of information security culture: a methodological issue*. In the second Australian information security management conference, Perth, Australia; 26 November 2004.
34 E. Chang, S. Lin, *Exploring organizational culture for information security management*. Industrial Management & Data Systems, 107(3), 2007, str. 438–458.
35 T. Schlienger, S. Teufel, *Information security culture the socio-cultural dimension in information security management*. In: IFIP TC11 International Conference on Information Security, Cairo, Egypt; 2002, str: 7–9.
36 L. Ngo, V. Zhou, M. Warren, *Understanding transition towards information security culture change*. In: Proceedings of the third Australian information security management conference, Perth, Australia, 2005.
37 A. Chia, B. Ruighaver, B. Maynard, *Understanding Organizational Security Culture*, Proceeding of PACIS Japan, 2002.
38 E. Chang, B. Ho, *Organizational factors to the effectiveness of implementing information security management*. Industrial Management & Data Systems, 106(3), 2006, str. 345–361.
39 M. Lo, 2015, dostupno na: *http://www.netokracija.rs/prvo-razmisli-telenor-92304* (20. 12. 2015).

Naime, mladi imaju probleme koje ne mogu uvek da prepoznaju i objasne, susreću se sa različitim pojavama i pretnjama bez prethodne psihološke zaštite. Probleme uglavnom ne mogu sami da reše i/ili ne znaju kome da se obrate za pomoć.

Opasnosti i pretnje kojima je mlađa populacija korisnika Interneta svakodnevno izložena jesu brojne i raznovrsne, a posebno sa ekspanzivnim razvojem društvenih mreža. One danas predstavljaju sadržaje koji su popularni i kao takvi veoma uticajni na mlađu populaciju korisnika Interneta.

Mladi su najugroženija ciljna grupa većine pojavnih oblika zloupotrebe, a posebno nastajanju, razvoju i širenju dečije pornografije. Edukacija i upozorenja na nivou roditelja igraju možda najvažniju ulogu u prevenciji i rešavanju ovog problema. Adekvatna bezbednosna kultura svih korisnika, a naročito mladih, imperativ je savremenog društva.[40]

Decu i mlade treba podsticati da postanu aktivniji, sa većim opsegom znanja, razumevanja i mogućnosti da se suoče sa problemima, kao i da neguju ona ponašanja koja će značajno podići njihov nivo bezbednosne kulture[41]. Da bi se ovaj cilj postigao, neophodno je da informaciono-bezbednosna kultura postane sastavni deo planova i programa svih nivoa obrazovanja i vaspitanja. Prihvatanjem osnovnih načela informaciono-bezbednosne kulture stvorio bi se preduslov za uspostavljanje bezbednog ambijenta u kome bi mladi neometano mogli da koriste sve prednosti i blagodeti informacionih tehnologija i tako ostvare svoja prava na kvalitetno obrazovanje, informisanje i lični razvoj.

Autori rada su svoju celokupnu posvećenost informaciono-bezbednosnoj kulturi u daljem tekstu usmerili na korisnike i njihov menadžment u organizaciji, ali izneti predlozi i primeri biće adekvatni i za pojedinačne korisnike informacionih tehnologija.

2.2. Okvir informaciono-bezbednosne kulture sa stanovišta najbolje prakse

Kultura se ne može nametnuti i dekretom propisati. Potrebno je suptilnije delovanje na korisnike kroz sprovođenje pet ključnih komponenti bezbednosne kulture (slika 2). Autori Šlinger i Teufil[42] insistiraju na: a) internoj komunikaciji, b) programima edukacije i treninga i c) inicijativi menadžmenta, čije ponašanje treba da služi kao primer.

a) Internu komunikaciju treba sprovesti kroz uspostavljanje dijaloga između top menadžmenta i zaposlenih, sa ciljem deljenja informacija, znanja i motivacije, kao i dobijanja povratnih informacija. Na taj način se stvara klima prihvatanja i

40 Ž. Bjelajac, M. Zirojević, *Bezbednosna kultura u eri globalizacije*, Institut za međunarodnu politiku i privredu Beograd, 2014. Dostupno na: *http://kpolisa.com/KP23/kp23-II-3-BjelajacZirojevic.pdf* (20. 12. 2015).

41 F. Ejdus, J. Unijat, M. Milošević, *Istraživanje i podizanje nivoa bezbednosne kulture mladih*, 2009. Dostupno na: *http://www.bezbednost.org/Svi-projekti/700/Istrazivanje-i-podizanje-nivoa-bezbednosne.shtml#sthash.IRucHXPn.dpuf* (20. 12. 2015).

42 T. Schlienger, S. Teufel, *Information security culture – from analysis to change*, International institute of management in telecommunications, University of Fribourg, 2003, dostupno na: *http://icsa.cs.up.ac.za/issa/2003/Publications/INFORMATION%20SECURITY%20CULTURE.pdf* (20. 12. 2015).

posvećenosti korporativnim ciljevima i strategijama. Dva osnovna oblika interne komunikacije su:

- interpersonalna komunikacija (diskusija između zaposlenog i poslodavca, seminari, obuke i radionice) i
- komunikacija preko medija (intraneta, elektronske pošte, elektronskih vodiča i oglasnih tabli).

b) Programi redovne edukacije i treninga su ključni elementi za podizanje bezbednosne svesti, kako kod zaposlenih tako i kod menadžmenta. Zaposleni moraju razumeti zašto je informaciona bezbednost važna za organizaciju. Oni moraju da shvate da je svako od njih odgovoran za bezbednost u svojoj sferi delovanja, bez obzira da li u svom radu koriste informacione tehnologije ili ne. Ovi programi su od vitalnog značaja za sprovođenje bezbednosne politike. Konkretni primeri dati su u tački 4 ovog rada.

c) Pre samog sprovođenja prve dve tačke, neophodno je „ubediti" menadžment u važnost informacione bezbednosti i potrebu za njom. Svojevrstan problem kod sprovođenja mera bezbednosti je to što se ne može odmah izračunati dobit od bezbednosnih investicija. Tako postoje i situacije u kojima različite strukture menadžmenta smatraju da je ulaganje u bezbednost trošak, a ne investicija koja će im sačuvati posao i višestruko se isplatiti.

U nastojanju promene percepcije menadžmenta o važnosti i potrebi za informacionom bezbednošću, neophodno je nastupiti sa objektivnim argumentima i konkretnim bezbednosnim studijama slučaja, statističkim analizama i primerima iz prakse. Oni treba da budu upoznati sa mogućim rizicima koji vrebaju zaposlene i celokupan proces rada. Takođe, treba primeniti i emocionalne argumente kroz primere, poređenja ili predloge kako bi se motivisao menadžment da podrži procese informacione bezbednosti. Ponekad i „racionalne" odluke, čak i pored objektivnih argumenata, često se zasnivaju, pre svega, na osećanjima.

Za potpuni uspeh primene mera informacione bezbednosti u organizaciji neophodno je da im menadžment bude u potpunosti posvećen i da svojim ličnim primerom, u svakodnevnim aktivnostima, bude uzor zaposlenima čime bi im informaciona bezbednost postala prirodno stanje i radno okruženje.

3. Praktični primeri izgradnje i uspostavljanja informaciono-bezbednosne kulture

Praktični primeri izgradnje i uspostavljanja informaciono-bezbednosne kulture sagledani su sa tri aspekta:

1) podizanje svesti korisnika informacionih tehnologija,

2) celovita zaštita i

3) digitalna forenzika.

Ni jedan od navedenih aspekata sam za sebe nije dovoljan i ne garantuje sveobuhvatnu bezbednost, već ih je neophodno kombinovati i planski primenjivati.

3.1. Svest o informacionoj bezbednosti

Podizanje svesti o informacionoj bezbednosti postiže se kroz: ličnu odgovornost, lojalnost zaposlenih i aktivnosti menadžmenta.

Lična odgovornost i lojalnost zaposlenih se ogleda u ophođenju i načinu korišćenja informacionih tehnologija, kao što su: bezbedno ponašanje u radu sa javnim i deljenim podacima i informacijama, načinom na koji se koristi hardver (fleš memorije, CD/DVD, računari, serveri, mobilni uređaji...), softver (operativni sistemi i aplikacije, pravljenje rezervnih kopija, antivirusna i fajervol zaštita...), mreža (Internet i intranet, pristupanje drugoj informacionoj imovini i servisima, kopiranje velikih fajlova...), zatim okruženje u kome se radi, kao i poštovanje svih drugih procedura i mera bezbednosti.

Aktivnosti menadžmenta treba da stimulišu, podstiču i sugerišu zaposlenima da aktivno učestvuju u programima edukacije i treninzima. Aktivno učešće zaposlenih u predviđenim programima predstavlja osnov bezbednosti. Ovi programi treba da pruže dovoljno znanja o potrebi i načinima zaštite, da objasne razloge za poštovanje i primenu standardnih mera i procedura zaštite, kao i da daju odgovor zašto je informaciona bezbednost važna za organizaciju. Usvajanje novih znanja i promena percepcije zaposlenih, kao i praktična primena odgovarajućeg nivoa stručnosti i sposobnosti na nadležnosti u određenoj situaciji, jesu osnov za uspeh svakog bezbednosnog sistema. Takođe, programi edukacije i treninzi za zaposlene treba da obuhvate i konkretna tehnička pitanja vezana za bezbednost (korišćenje popularnih društvenih mreža i servisa, slanja elektronske pošte, pretraživanje Interneta, ali i odbrana od zlonamernih korisnika i njihovih destruktivnih proizvoda). Kod svih programa treba redovno obavljati proveru kvaliteta edukacije i treninga, kao i njihovu periodičnu nadogradnju.

3.2. Celovita zaštita kao osnov informaciono-bezbednosne kulture

Na elementarnom nivou zaštite sistema potrebno je primeniti: mere normativnog karaktera, kriptološke mere, logičke mere i fizičko-tehničke mere[43].

Mere normativnog karaktera, u koje spadaju pravne, organizacione i kadrovske, pripadaju kategoriji netehničkih mera. Osnovna karakteristika ovih mera je da ne degradiraju rad sistema, već, naprotiv, znatno doprinose povećanju njegove raspoloživosti i produktivnosti, a istovremeno značajno utiču na efikasnost sistema zaštite. Ovim merama se utvrđuje politika zaštite („kućni red"), koja određuje šta se smatra prihvatljivim i kakve su sankcije za neprihvatljivo ponašanje. To im daje karakter samostalnog i delotvornog instrumenta u pravcu preventivnog odvraćanja od nedozvoljenih aktivnosti, dok istovremeno predstavljaju najjeftinije i najefikasnije sredstvo u sprečavanju i otkrivanju brojnih nedozvoljenih ponašanja i aktivnosti.[44]

43 Z. Milanović, M. Srećković, *Znanjem protiv zloupotrebe enkripcije*, Naučno-stručni skup sa međunarodnim učešćem „Suprostavljanje savremenim oblicima kriminaliteta – analiza stanja, evropski standardi i mere za unapređenje", Zbornik, Tom 3, Tara, 2015, str. 135–147.
44 S. Petrović, *Zaštita računarskih sistema*, Viša železnička škola, Beograd, 2004.

1) Pravne mere obuhvataju sledeće:
- zakonska regulativa (nacionalna, Savet Evrope, Ujedinjene nacije…);
- interna akta, propisi, pravila i druga dokumenta;
- akt o bezbednosnoj proceni rizika;
- zaštita privatnosti i intelektualne svojine;
- sankcionisanje svih vidova kiberkriminala.

2) Organizacione mere obuhvataju standarde, misiju viziju i ciljeve, bezbednosnu politiku, kodeks ponašanja i bezbednosne procedure za kontrolu pristupa.

Najvažniji standardi su ISO, NIST, CRAMM, EBIOS, OCTAVE, HIPAA, COBIT, ITIL, FISAP, FISMA i drugi. Organizacija treba da prati sve bezbednosne preporuke koje su date u međunarodnim standardima i standardima najbolje prakse, a posebno odredbe koje se odnose na ugrožavanje ljudskih prava, privatnosti i identiteta zaposlenih i ostalih zainteresovanih strana, kao i ugrožavanja autorskih prava i licenci.

Misija, vizija, ciljevi su „sveto trojstvo" svake organizacije. Na osnovu navedenih dokumenta i sopstvenih potreba, organizacija definiše bezbednosne ciljeve koje postavlja pred svoje zaposlene.

Bezbednosna politika deklariše obavezu organizacije da poslovi bezbednosti budu njen prioritet. Ona pribavlja okvir za najbolju praksu koju mogu razumeti i ispratiti svi zaposleni, čime presudno pomaže da se obezbedi minimiziran rizik i da se na bilo koji bezbednosni incident efikasno odgovori[45]. Opšti zahtevi i preporuke bezbednosne politike podrazumevaju sledeće:
- organizacija je vlasnik celokupne informacione imovine, kao i svih procesa i elektronskih transakcija;
- stepen zaštite i održavanja podizati na najviši mogući nivo uz korišćenje svih preporuka bezbednosnih stručnjaka i proizvođača informatičkog hardvera i softvera, kao i svih raspoloživih sredstava;
- menadžment je odgovoran za uspostavljanje i primenu standarda i procedura, kao i za kontrolu pristupa informacionoj imovini organizacije i kontrolu pristupa korisnika Internetu i intranetu; menadžment ličnim primerom treba da pokaže i podrži podizanje svesti korisnika o potrebi zaštite informacione imovine, kao i da kroz različite nivoe obučavanja pripremi korisnike na samozaštitu i smanjenje rizika od kiberkriminala;
- novozaposleni, kao i svi ostali, treba da potpišu *Izjavu o čuvanju i zaštiti poverljivih informacija*, pre nego što dobiju korisničke naloge i ovlašćenja za pristup informacionoj imovini;
- korisnici kojima je ova politika namenjena obavezni su da usaglase praksu zaštite sa ovom politikom i sa referentnim standardima, uputstvima i procedurama zaštite koje je podržavaju;

45 D. Danchev, *Building and Implementing a Successful Information Security Policy*, Dostupno na: *http://www.windowsecurity.com/pages/security-policy.pdf* (20. 12. 2015).

- korisnici računarskog sistema su dužni da se brinu o celokupnoj informatičkoj imovini (hardveru, softveru, računarskoj mreži i podacima) i da u slučaju uočenih nepravilnosti (oštećenja, smetnji i nedostataka) pismeno obaveste nadležno lice; ovaj izveštaj mora da sadrži: datum, vreme, detaljan opis uočenog problema i potpis;
- korisnici se slažu da će pravilno i adekvatno svojim ovlašćenjima koristiti informacionu imovinu; to znači da nije dozvoljeno: nekontrolisano korišćenje mrežnih resursa i opreme; skladištenje fajlova (filmova, muzike, slika...) na serveru ili radnim stanicama; preinstalacija i podešavanje postojećeg softvera, kao ni instalacija novog, a naročito nelicenciranog softvera; zatim, korišćenje tuđih naloga i lažno predstavljanje; korišćenje i uništavanje tuđih podataka; napadanje i nanošenje štete drugim računarima u lokalnoj i Internet mreži; nedolično ponašanje na Internetu i slanje kompromitujuće elektronske pošte, kao i poruka koje predstavljaju neželjenu poštu – spam; prijavljivanje na forumima, čet grupama i drugim Internet servisima, kao i ostavljanje adrese organizacije;
- korisnici će uklanjati poznate ranjivosti na sistemu, redovnim ažuriranjem operativnog sistema, antivirus programa i drugih korisničkih aplikacija, i neće isključivati zaštitne programe na sistemu ni zaobilaziti bezbednosne dijaloge;
- korisnici neće praviti neautorizovane kopije podataka i softvera;
- korisnici će pristupati sistemu i podacima samo na autorizovan način;
- korisnici će izabrati bezbednosnu lozinku na promišljeno (a ne pro forme), držati je i čuvati kao tajnu; isto važi i za druge identifikacione parametre za pristup sistemu;
- korisnici će redovno praviti rezervne kopije svih važnih fajlova sa računara na odvojenim medijima ili drugim diskovima koji nisu stalno povezani na računar (prenosni disk, brza memorija, CD, DVD, itd.); pravljenje rezervnih kopija na Internetu (tzv. sistemi „oblaka", *cloud*), koji nude nezavisan pristup resursima od lokacije, ne preporučuju se, a za one koji to koriste neophodno je da isključe automatsku sinhronizaciju; takođe, korisnicima koja je ova opcija dostupna ne bi trebalo da kače (postavljaju) svoje liče podatke (skenirana lična dokumenta: lične karte, pasoše, platne kartice, zdravstvene knjižice, zatim, slike, nezaštićena autorska dela, anonimne poruke i sve što bi direktno moglo da ugrozi njihovu privatnost) ili poslovne informacije, ako za to nemaju odobrenje od menadžmenta;
- korisnici će koristiti tzv. bezbedne računare ili virtualne mašine za eksperimentisanje, rizične sajtove, otvaranje sumnjive elektronske pošte itd.;
- korisnici će preuzimanje programa sa Interneta uvek obavljati kod ovlašćenih distributera i sa sajtova proizvođača; najbezbedniji programi su otvorenog koda, a najopasniji su besplatni;
- korisnici neće instalirati programe za koje je link dobijen putem elektronske pošte, društvenih mreža, četa (*chat*), itd.;
- korisnici neće otvarati elektronsku poštu od nepoznatog pošiljaoca i neće slati poruke sa ličnim podacima ili poverljivim podacima organizacije;

- korisnici će podržati zamenu i potpuno izbaciti iz upotrebe operativne sisteme za koje ne postoji podrška proizvođača, kao i programe: *Internet Explorer, Adobe Acrobat/Reader, Adobe Flash Player, Java* itd.;
- korisnici se slažu sa politikom praznog ekrana i praznog stola; svi zaposleni će prilikom završavanja svog radnog vremena regularno isključiti sve aktivne konekcije ka udaljenim računarima, kao i svoj računarski sistem; zaposleni treba da vode računa da poverljive informacije (elektronski i optički mediji, dokumenta i zabeleške) nikada ne ostavljaju otvorene na radnom stolu, bez nadzora;
- svi korisnički računari i serverske stanice treba da imaju digitalne sertifikate, koji su izdati od poverljivog sertifikacionog tela, a koji služe za jednoznačnu identifikaciju računara;
- potrebno je izvršiti fizičko razdvajanje (separaciju) Internet i intranet mreže ili izvršiti segmentaciju sistema na funkcionalne celine, gde bi se obavezno u intranet mreži uspostavila demilitarizovana zona za komunikaciju sa javnom mrežom – Internetom; kontrolisati i nadgledati fajervol servisima na mrežnoj kapiji (*Gateway*) kroz koje prolazi celokupni saobraćaj; iza ovog fajervola treba instalirati detektor upada u internu mrežu (IDS/IPS tipa) koji detektuje sve napade na mrežu, ali i slabosti konfigurisanja graničnog fajervola;
- bezbednosna politika mora biti objavljena i učinjena dostupnom svim korisnicima.

Kodeks poslovnog ponašanja i poslovne etike, sa posebnim akcentom na informacionoj bezbednosti, jeste dokument koji važi za sve zaposlene i čija je svrha da ih uputi kako da svoje ponašanje prilagode radnom okruženju, u skladu sa moralnim i profesionalnim normama i opšteprihvaćenim vrednostima. Kodeks treba da sadrži sledeće elemente: odnos prema poslu i saradnicima, odnos prema klijentima i poslovnim partnerima i odnos prema imovini.

Bezbednosne procedure za kontrolu pristupa – korišćenje lozinki, elektronske pošte, antivirusne zaštite, društvenih mreža, o posete sajtovima i preuzimanje programa i fajlova, sve do procedure za pravljenje rezervnih kopija podataka, procedure u slučaju opasnosti i nastanka bezbednosnog incidenta, kao i procedure za tretman rizika.

3) Kadrovske mere podrazumevaju najpre dobro planiranje i dobar izbor stručnih kadrova. To direktno utiče na kvalitet informacione bezbednosti. Novozaposlene kadrove treba upoznati sa bezbednosnom politikom i drugim bezbednosnim merama u organizaciji, a kod postojećih kadrova treba održavati postignuti nivo znanja redovnim, periodičnim edukacijama i treninzima. Zaposleni treba da budu upoznati sa svim bezbednosnim rizicima i mogućim pretnjama koje su vezane za njihov delokrug rada. Pravovremena i egzaktna identifikacija bezbednosnih rizika i stvaranje „nerizičnog ambijenta" jesu ključ uspeha savremene organizacije. U tom kontekstu moraju se razmatrati i prekidi radnog odnosa, unapređivanje i nagrađivanje zaposlenih i međuljudski odnosi.

Kriptološke mere omogućavaju ostvarivanje najvišeg mogućeg nivoa zaštite (Ranđelović, 2009). Ipak, kao i sve druge mere, one su potrebne, ali ne i dovoljne da samostalno ostvare potreban nivo bezbednosti. Obuhvataju:

- kriptozaštitu podataka na mreži – IP saobraćaja, Wi-Fi konekcije, virtuelne privatne mreže (VPN), elektronske pošte i tekstualnih poruka, mobilne telefonije, glasovne komunikacije i drugih otvorenih sistema za komunikaciju;
- kriptozaštitu podataka izvan mreže – USB, HDD, fajlova i softvera;
- kvantnu i DNK kriptografiju;
- digitalni potpis i vremenski (digitalni) žig;
- digitalni sertifikati (javni ključ + sertifikat + jedan ili više digitalnih potpisa).

U **logičke mere** ubrajamo sve vidove logičke kontrole koje organizacija primenjuje kako bi kontrolisala pristup svojim informacijama i drugoj informacionoj imovini. Reč je o sledećem:

- kontrola pristupa za identifikaciju i autentifikaciju korisnika i autorizaciju prava pristupa korisnika informacionoj imovini, kao i mehanizmima za integraciju fizičke i logičke kontrole pristupa informacionoj imovini; standardi i procedure za kontrolu pristupa koji su previše kruti ili previše fleksibilni, mogu ometati svakodnevne aktivnosti organizacije i frustrirati zaposlene; na to treba obratiti posebnu pažnju kod definisanja pravila u bezbednosnoj politici;
- kod davanja prava za pristup sistemu treba primenjivati princip davanja minimalnih privilegija; minimum privilegija je bezbednosni zahtev koji zaposlenima daje samo onoliko prava pristupa koliko je neophodno za obavljanje poslova, a da pri tom ne ometa poslovanje;
- vremensko ograničenje konekcija – kontrola pristupa pojedinim servisima može se vršiti i ograničenjem trajanja sesije, u zavisnosti od njihove namene;
- za pristup računarskom sistemu (lokalnoj radnoj stanici), u svakodnevnom radu, upotrebljavati korisničke naloge sa restriktivnim pristupom, a ne administratorskim;
- zaštita lozinkom, smart karticom ili nekom biometrijskom metodom: administratorski i sve ostale naloge i ako je moguće, uključiti dvostepenu autentifikaciju (kao što nude skoro svi veći onlajn servisi *Google*, *Yahoo*, *Mozilla*…); lozinke treba redovno menjati (minimalno na 30 dana); *nikada* ne koristiti dva puta istu lozinku za dva ili više: računara, aplikacije ili servisa; lozinka mora biti kompleksna i teška za krekovanje (otkrivanje), treba da sadrži velika i mala slova, specijalne karaktere i brojeve – sve ukupno više od 12 karaktera; lozinke se ne mogu deliti ni sa jednim drugim licem ni u kom slučaju.

Fizičko-tehničke mere obuhvataju:

- fizičko obezbeđenje na ulazu u zgradu i prostorije gde se nalaze računarski sistemi, kao i uklanjanje svih kablova, utičnica i konekcija koje izlaze iz zgrade kao javni medijum;
- biometrijske metode – fizičke/fiziološke: čitanje DNK zapisa, skeniranje rožnjače, prepoznavanje lica, geometrija šake, provera vena, otisak prsta; ponašajne: prepoznavanje glasa, rukopisa ili potpisa, dinamika kucanja, dinamika hoda, dinamika mirisa;
- elektronsko obezbeđenje – video-nadzor, identifikacija pristupa, protivpožarni i protivprovalni sistemi zaštite.

3.3. Digitalna forenzika i merenje informaciono-bezbednosne kulture

Dobro je poznato da moderan kriminal često ostavlja elektronske tragove. Pronalaženje i očuvanje tih dokaza zahteva pažljive metode, kao i tehničke veštine[46].

Digitalno-forenzičke metode i alati, umnogome doprinose kod procesa napredne zaštite sistema, analizi kiberkriminala, u rešavanju sudskih sporova, ali i kod merenja bezbednosne kulture.

Merenje bezbednosne kulture je proces koji se zasniva na snimanju ponašanja zaposlenih pri korišćenju informacionih tehnologija, i to kroz: praćenje log fajlova na sistemu koji mogu poslužiti za analizu bezbednosnog incidenata, zatim monitoring sistema, procesa i servisa, nadgledanje mrežnog pristupa, kao i sprovođenje interne bezbednosne provere korisnika pomoću intervjua, anketa, testova, upitnika itd. Na primer, merenje da li korisnici: poštuju pravila bezbednosne politike; posećuju edukativne skupove/sastanke i aktivno učestvuju u bezbednosnim programima on-line; koriste lozinku za prijavljivanje na sistem; koriste jake lozinke i redovno ih menjaju; prave rezervne kopije svih važnih fajlova, ili možda: narušavaju nečiju privatnost; posećuju kritične sajtove; šalju kompromitujuće i spam poruke; čitaju elektronsku poštu nepoznatih pošiljalaca i u njima popunjavaju razne obrasce i upitnike; isključuju aktivne programe zaštite (antivirus, fajervol...).

Zaključak

Razlog za konstataciju da „svi sve znaju o bezbednosti, a ipak nisu ni blizu bezbedni" nalazi se u činjenici nedostatka bezbednosne kulture.

Informaciono-bezbednosna kultura treba da podstakne na razmišljanje i upozori korisnike da ozbiljan i odgovoran posao koji rade na računarima i mobilnim uređajima nikako ne ide zajedno sa zabavom: onlajn igricama, korišćenjem piratskog softvera, skidanjem piratskih filmova, serija i muzike, kao i posećivanje hakerskih i porno sajtova. Korisnici moraju da čuvaju kako svoju privatnost i lične podatke, tako i od organizacije za koju rade.

Ozbiljnost, neophodnost i hitnost u primeni navedenih standarda, mera i programa je naglašena time što tamna strana informacionog društva „cveta". Skoro da ne postoji ni jedan trenutak u kome se ne pojavljuju nove tehnike, metode i alati za različite napade i pretnje, kao i otkrivanja novih ranjivosti i slabosti u sistemu.

Pronalaženje novih strategija i jedinstvenih programa koji će pravovremeno i efikasno odgovoriti na bezbednosne izazove, rizike i pretnje, te osposobiti korisnike informacionih tehnologija za život u svetu koji se konstantno menja, su imperativ savremenog društva.

46 American Scientist, 2013, dostupno na: *http://www.americanscientist.org/issues/feature/2013/5/digital-forensics* (20. 12. 2015).

Pristupi pri rešavanju problema informacione bezbednosti mogu biti različiti, ali ono u čemu se svi slažu i na čemu se najviše stavlja akcenat je konstantna edukacija korisnika informacionih tehnologija, podizanje svesti o neophodnosti zaštite i izgradnja informaciono-bezbednosne kulture.

Društvena uloga i značaj kulture u savremenom svetu imaju potpuni legitimitet, jer je ona povezana sa svim tokovima društvenog života, integrisana u sve društvene pojave i procese[47].

Program razvoja informaciono-bezbednosne kulture i podizanja svesti o neophodnosti zaštite, pre svega, treba utemeljiti u ključne stubove svake države: vojsci, policiji, tužilaštvu i sudstvu, ali i u celoj naciji, jer jedino „znanjem se možemo boriti protiv zloupotrebe znanja“[48].

Literatura

1. Air Safety Support International, Dostupno na: *http://www.airsafety.aero/Safety-Information-and-Reporting/Safety-Management-Systems/Safety-Culture.aspx* (20. 12. 2015).
2. American Scientist, 2013. Dostupno na: *http://www.americanscientist.org/issues/feature/2013/5/digital-forensics* (20. 12. 2015).
3. Bandura A.; 1999. Dostupno na: *http://www.muskingum.edu/~psych/psycweb/history/bandura.htm* (20. 12. 2015).
4. Bezbednost, Dostupno na: *http://www.smatsa.rs/Lat/PrintShowContent.aspx?mi=32* (20. 12. 2015).
5. Bjelajac, Ž., Zirojević, M.; *BEZBEDNOSNA KULTURA U ERI GLOBALIZACIJE*, Institut za međunarodnu politiku i privredu Beograd, 2014. Dostupno na:
6. *http://kpolisa.com/KP23/kp23-II-3-BjelajacZirojevic.pdf* (20. 12. 2015).
7. Burke A., *Aporias of Security*, Alternatives: Global, Local, Political 27(1), 2002, str. 1–27
8. Chang, S. E., Ho, C. B.; *Organizational factors to the effectiveness of implementing information security management*. Industrial Management & Data Systems, 106(3), 2006, str. 345–361.
9. Chang, E., Lin, S.; *Exploring organizational culture for information security management*. Industrial Management & Data Systems, 107(3), 2007, str. 438–458.
10. Chia, A., Ruighaver, B., Maynard, B., *Understanding Organizational Security Culture*, Proceeding of PACIS Japan, 2002.
11. Danchev, D.; *Building and Implementing a Successful Information Security Policy*, Dostupno na: *http://www.windowsecurity.com/pages/security-policy.pdf* (20. 12. 2015).

47 S. Stanarević, M. Bodin, *Bezbednosna kultura kao društveni resurs nacionalne bezbednosti*, Časopis Vojno delo, Beograd, 2014. Dostupno na: *http://www.odbrana.mod.gov.rs/odbrana-stari/vojni_casopisi/arhiva/VD_2014-prolece/66-2014-1-06-Stanarevic.pdf* (20. 12. 2015).

48 S. Petrović, *Znanjem protiv zloupotrebe znanja*, Savetovanje o zloupotrebi IT – ZITEH, Beograd, 2010.

12. Dhillon. G.; *Interpreting the Management of Information Systems Security*, London: London School of Economics and Political Science, 1995.
13. Ejdus, F., Unijat, J., Milošević M.; *Istraživanje i podizanje nivoa bezbednosne kulture mladih*, 2009. Dostupno na: *http://www.bezbednost.org/Svi-projekti/700/Istrazivanje-i-podizanje-nivoa-bezbednosne.shtml#sthash.IRucHXPn.dpuf* (20. 12. 2015).
14. Kuusisto, T., Ilvonen, I.; *Information security culture in small and medium size enterprises*. Frontiers of E-business Research, 2003.
15. Kuusisto, R., Nyberg, K., Virtanen, T.; *Unite security culture may a unified security culture be plausible?* Proceedings of the 3rd European Conference on Information Warfare and Security (ECIW 2004), str. 221–229.
16. Lo, M.; Dostupno na: *http://www.netokracija.rs/prvo-razmisli-telenor-92304* (20. 12. 2015).
17. Martins, A., Eloff, J.; *Information security culture*. In: IFIP TC11 international conference on information security, Cairo, Egypt, 2002, str. 7–9.
18. Mijalković, S., *Nacionalna bezbednost – od vestfalskog koncepta do posthladnoratovskog*, Vojno delo 2, 2009, str. 55–73, Beograd. Dostupno na:
19. *http://www.odbrana.mod.gov.rs/odbrana-stari/vojni_casopisi/arhiva/VD_2009-2/Vono%20delo%20br.%202-2009.pdf* (20. 12. 2015).
20. Mijalković, S., Arežina-Đerić, V., Bošković, G., *Korelacija informacione i nacionalne bezbednosti*, Savetovanje o zloupotrebi IT – ZITEH, Beograd, 2010.
21. Dostupno na: *http://www.singipedia.com/content/1057-Korelacija-informacione-i-nacionalne-bezbednosti* (20. 12. 2015).
22. Milanović, Z., *Organizacioni model implementacije bezbednosne politike u obrazovnim ustanovama*, Savetovanje o zloupotrebi IT – ZITEH, Beograd, 2006.
23. Milanović, Z., Srećković, M., *Znanjem protiv zloupotrebe enkripcije*, Naučno-stručni skup sa međunarodnim učešćem „Suprostavljanje savremenim oblicima kriminaliteta – analiza stanja, evropski standardi i mere za unapređenje", Zbornik Tom 3, Tara, 2015, str. 135–147.
24. Ngo, L., Zhou, V. V., Warren, M.; *Understanding transition towards information security culture change*. In: Proceedings of the third Australian information security management conference, Perth, Australia, 2005.
25. Oxford Dictionaries, 2015, Dostupno na: *http://www.oxforddictionaries.com/definition/english/* (20. 12. 2015).
26. Oxford Dictionaries, 2015, Dostupno na: *http://dictionary.reference.com/browse/culture* (20. 12. 2015).
27. Palispis E.; *Introduction to "Sociology and Anthropology"*, Rex Book Store, INC and Epitacio s. Palispis, Philippine, 2007, str. 42–43. Dostupno na: *http://books.google.rs/books?id=PtPLp_wuECkC&printsec=frontcover&hl=sr&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false* (20. 12. 2015).
28. Petrović, S.; *Zaštita računarskih sistema*, Viša železnička škola, Beograd, 2004.

29. Petrović, S.; *Znanjem protiv zloupotrebe znanja*, Savetovanje o zloupotrebi IT – ZITEH, Beograd, 2010.
30. Ranđelović, D., Petrović, L., Radovanović, R., Popović, A.; *Securiti protocols*, NBP – Žurnal za kriminalistiku i pravo, Vol. 1, 2009. str. 89–116.
31. Roer K., *Build a Security Culture*, IT Governance Publishing, United Kingdom, 2015.
32. Schlienger, T., Teufel, S.; *Information security culture the socio-cultural dimension in information security management*. In: IFIP TC11 International Conference on Information Security, Cairo, Egypt; 2002, str. 7–9.
33. Schlienger, T., Teufel, S.; *Information security culture – from analysis to change*, International institute of management in telecommunications, University of Fribourg, 2003. Dostupno na: *http://icsa.cs.up.ac.za/issa/2003/Publications/INFORMATION%20SECURITY%20CULTURE.pdf* (20. 12. 2015).
34. Schneier, B.; 2015, RM Education. Dostupno na: *https://www.rm.com/support/technicalarticle.asp?cref=tec377232* (20. 12. 2015).
35. Solms, B., *Information security – The third wave? Computers & Security*, 19(7), 2000, str. 615–620.
36. Stajić, Lj., Mijalković, S., Stanarević, S.; *Bezbednosna kultura mladih: kako živeti bezbedno*, Draganić, Beograd, 2006.
37. Stanarević, S., Ejdus, F., Pojmovnik bezbednosne kulture, Centar za civilno-vojne odnose, Beograd, 2009. Dostupno na: *http://www.wbrc.rs/wp-content/uploads/2012/11/Pojmovnik-bezbednosne-kulture-grupa-autora-2009.pdf* (20. 12. 2015).
38. Stanarević, S., Bodin, M.; *Bezbednosna kultura kao društveni resurs nacionalne bezbednosti*, Časopis Vojno delo, Beograd, 2014. Dostupno na:
39. *http://www.odbrana.mod.gov.rs/odbrana-stari/vojni_casopisi/arhiva/VD_2014-prolece/66-2014-1-06-Stanarevic.pdf* (20. 12. 2015).
40. Thomson, K., Solms, R., Louw, L.; *Cultivating an organizational information security culture*. Computer Fraud & Security. 10, 2006, str. 7–11.
41. Vroom, C., Solms, R., *Towards information security behavioral compliance*. Computers & Security, 23(3), 2004, str. 191–198.
42. Whitman, E. M., Mattord, J. H.; *Principles of Information Security*, Fourth Editional, Course Technology, Cengage Learning, 2012.
43. Zakaria, O.; *Understanding challenges of information security culture: a methodological issue*, In the second Australian information security management conference, Perth, Australia; 26 November 2004.

INFORMATION-SECURITY CULTURE – IMPERATIVE OF CONTEMPORARY SOCIETY

Zoran Milanovic
Radovan Radovanovic
Academy of Criminalistic and Police Studies, Belgrade

Summary: The importance of building information-security culture of each society has become a well-established idea. The aim of such a culture is the impact on different human behaviors that may affect the overall results of protection of information assets.

The authors believe that culture is the "key" of the information security.

Extensive review and analysis of the information security literature have come to the conclusion that the collective consciousness about the use and protection in the field of contemporary forms of crime is very low.

In this sense, the goal of this paper is that the examination of information security culture from the standpoint of best practices, support the view that knowledge and education play an important role in building a secure environment with a special emphasis on raising awareness of end-users about the need and importance of data protection, information and knowledge

Keywords: Information technology, information security culture.