UNIVERZA V LJUBLJANI

FAKULTETA ZA DRUŽBENE VEDE

KATJA RANČIGAJ

# INFORMACIJSKA VARNOSTNA KULTURA V DRŽAVNI UPRAVI

MAGISTRSKO DELO

MENTOR: doc. dr. Uroš Svete

SOMENTOR: izr. prof. dr. Bojan Dobovšek

LJUBLJANA, 2010

*»V enem samem zrnu živ*

*v tisoč njiv sem posejan.*

*Bom vzklil?*

*Bom sam sebi ostal neznan?«*

*Ciril Zlobec*

***ZAHVALA***

*Iskrena hvala mentorju, doc. dr. Urošu Svetetu in somentorju, izr. prof. dr. Bojanu Dobovšku za strokovno pomoč in usmeritve pri pisanju magistrske naloge. Hvala dr. Alešu Dobnikarju in g. Nikolaju Simiču, ki sta mi omogočila izvedbo raziskave.*

*Hvala tudi vsem domačim in prijateljem, ki ste mi na študijski poti stali ob strani.*

*And finally, l would like to thank my partner Victor for his love and support throughout this entire journey.*

**POVZETEK**

**Naslov: Informacijska varnostna kultura v državni upravi**

V organizacijah, kjer je primarna dejavnost močno odvisna od sodobnih informacijsko-komunikacijskih tehnologij, predstavljajo varnostne navade in ravnanja zaposlenih pomemben intelektualni kapital, ki se oblikuje postopoma in prehaja od samega oblikovanja varnostnih politik do dejanskega organizacijskega znanja. Kljub precejšnemu porastu znanstvenih proučevanj v obdobju zadnjih let, še vedno ni enotnih odgovorov na vprašanje, kakšen je delež informacijske varnostne kulture pri vzpostavljanju in zagotavljanju informacijske varnosti oz. kako le-ta vpliva na varnostno osveščenost in vedenje zaposlenih. Magistrska naloga dopolnjuje obstoječa spoznanja v luči sodobnih vidikov varnostnih ogrožanj in poglobljeno obravnava prispevek posameznikov, skupin ter celotne organizacije k doseganju visoke stopnje informacijske varnostne kulture. Osredotoča se tako na kulturni vidik, torej na vrednote in prepričanja zaposlenih, ki vplivajo na oblikovanje vedenjskih norm, kot tudi na organizacijske lastnosti, ki vplivajo na varnost delovnega okolja in predstavljajo temelj za razumevanje in poosebljanje varnostnih politik, standardov in pravil.

Magistrska naloga proučuje informacijsko varnostno kulturo v državni upravi, natančneje v Direktoratu za e-upravo in upravne procese in Direktoratu za informacijsko družbo, ki predstavljata reprezentativna organa državne uprave z vidika informacijsko-komunikacijskih procesov. Zaradi primarnih dejavnosti, ki so usmerjene v načrtovanje, razvijanje in izvajanje najrazličnejše elektronske podpore, pomembno prispevata h gradnji informacijske družbe in sta zaradi specifičnega delovnega okolja še posebej aktualna tudi z vidika proučevanja socialnih in organizacijskih dejavnikov informacijske varnosti.

Stopnja obstoječe informacijske varnostne kulture je v izbranih direktoratih ocenjena nadpovprečno visoko, kar kaže na to, da so v zadostni meri vzpostavljeni nujno potrebni ukrepi za zagotavljanje informacijske varnosti. Nekoliko več pozornosti je potrebno nameniti vlogi, ki jo ima vodstveno osebje, saj je njihov prispevek izmed vseh indikatorjev informacijske varnostne kulture najslabše ocenjen. Poleg tega je potrebno več truda vložiti tudi v znanje in varnostno osveščenost zaposlenih.

**Ključne besede:** informacijska varnostna kultura, informacijska varnost, varnostna osveščenost

**ABSTRACT**

**Title: Information security culture in the state administration**

The security habits and behaviour of employees constitute an important intellectual asset in organizations with a primary activity highly dependent on information-communication technology. This asset is gradually shaped and transforms from the formation of security politics to the actual organizational knowledge.

Despite a substantial rise in scientific research in the last years the question remains how information security culture is associated with establishing and executing information security, and how it affects security awareness and the behaviour of employees. This master's thesis complements the existing body of knowledge from the perspective of behavioural security hazards, and at the same time deals with the contribution of individuals, groups or the whole organization to achieving a high level of information security culture. It focuses on the cultural aspect: values and principles of employees, which have an effect on behaviour. Moreover, organizational characteristics provide a foundation for understanding and integrating security politics, standards and regulations that affect safety in the working environment.

This master's thesis examines information security culture in the state administration, more precisely in the Directorate for e-Government and Administrative Processes and the Directorate for Information Society, which comprise the representative bodies of the state administration regarding information-communication processes. Because of their primary activities directed at planning, development and execution of various electronic services they have an important contribution to the construction of an information society. Due to their specific work environment, they are also important from the aspect of investigating of social and organizational factors of information security.

The level of the currently existing information security culture in the two directorates turned out to be above-average which illustrates that the essential measurements for assuring information security have been established to a sufficient extent. Somewhat more attention needs to be devoted to the role of management, since their contribution has been evaluated least positive among all indicators of information security culture. Furthermore, more effort should be devoted into the increasing knowledge and security awareness of employees.

**Key words:** information security culture, information security, security awareness

**KAZALO VSEBINE**

## KAZALO TABEL



## KAZALO SLIK



## KAZALO GRAFOV

**SEZNAM UPORABLJENIH KRATIC**

IVK – INFORMACIJSKA VARNOSTNA KULTURA
OK – ORGANIZACIJSKA KULTURA
IKT – INFORMACIJSKO-KOMUNIKACIJSKA TEHNOLOGIJA
MJU – MINISTRSTVO ZA JAVNO UPRAVO
MVZŠ – MINISTRSTVO ZA VISOKO ŠOLSTVO, ZNANOST IN ŠPORT
DEUUP – DIREKTORAT ZA E-UPRAVO IN UPRAVNE PROCESE
DID – DIREKTORAT ZA INFORMACIJSKO DRUŽBO

# 1 UVOD

*»Mistakes are a fact of life. It is the response to the error that counts.«*
*(Nikki Giovanni, rojen 1943)*

Sodobna organizacija je v 21. stoletju postavljena v globalno in tehnološko usmerjeno okolje, ki postaja v čedalje večji meri odvisno od t. i. infrastrukture informacijsko-komunikacijskih tehnologij (v nadaljevanju IKT). Potenciali elektronskega komuniciranja, intenzivnost in nepredvidljivost razvoja ter zlasti otežen nadzor nad uporabo IKT-ja vplivajo na to, da postajajo vprašanja povezana z varnostjo mrežnih okolij in zaščito pred nedovoljenimi posegi v temeljne človekove pravice in svoboščine, kot tudi razprave o morebitnih tveganjih, vse pomembnejše.

Ob predpostavki, da razpolagamo s tehnološko dovršenimi orodji in da lahko na spremembe v zunanjem okolju vplivamo le bolj ali manj uspešno, je posameznik, torej zaposleni, verjetno eden izmed šibkejših elementov v organizacijskem sistemu. Dovzetnost za vplive, kot ena izmed osebnih značilnosti ljudi, lahko dolgoročno zmanjšuje sposobnosti in kompetence ter vpliva na to, koliko posameznik osebno prispeva k celotni informacijski varnosti v določeni organizaciji. Usmerjenost k posamezniku oz. k socialnemu kapitalu predstavlja mejnik med »organizacijo včeraj« in »organizacijo jutri«. Slednja temelji na zavedanju, da je uspeh ali neuspeh organizacije v veliki meri odvisen od tega, kar zaposleni naredijo dobro oz. od tistega, kar je bilo narejeno slabo. Če se je računalniška in informacijska varnost pri preprečevanju pomanjkljivosti in napadov še včeraj pretežno nanašala na tehnične rešitve, se je danes potrebno osredotočiti tudi na bolj socialno-tehnične vidike in poudariti doprinos posameznika in same organizacije (Dhillon in Backhouse 2001).

Sistematično opredeljevanje postopkov, ki je v splošnem značilno za zagotavljanje informacijske varnosti, je pomembno z vidika preventive, saj prispeva k zmanjševanju, preprečevanju in izogibanju nevarnostim, ki so povezane s tako občutljivim področjem dela. Vendar pa to ni edini ter sam po sebi najbolj učinkovit način usmerjanja in spremljanja vedenja ljudi (ENISA, European Network and Information Security Agency 2007). Na rokovanje z občutljivimi informacijami vplivajo tudi osebne predpostavke o varnosti v organizaciji, ki so odraz posameznikovega zaznavanja oz. razumevanja tako varnostnih

politik, kot tudi dejanskih groženj (Zakaria 2006). Zaznavanje in interpretacija varnosti sta v veliki meri odvisna od splošne varnostne kulture. Za ponazoritev – če zapisana pravila ali postopki v določeni organizaciji štejejo za jalova in nepomembna, bo takšen tudi odnos do varnostnih pravil. V organizacijo se bo naselil negativen odnos do delovnih orodij, ki se najmileje kaže v obliki izgovorov, da določena stvar ni bila narejena zaradi tega, ker je pravila ne narekujejo (Guldenmund 2000, 249).

Aktiven odnos posameznika do zaščite in varovanja osebnih ter zaupnih podatkov, ki zajema celotno znanje o zaščiti in varovanju teh podatkov ter se manifestira z zavestnim vedenjem v konkretni situaciji, lahko opredelimo kot izraz visoke stopnje varnostne kulture. Ta ne predstavlja zgolj vedenja, ampak predvsem vsebino, globlje motive in vzroke, kjer je ogroženost vrednot glavni povod za njihovo zaščito (Košmrlj 1982). Varnostna kultura je torej odraz usklajenih organizacijskih prizadevanj, da se elemente (organizacijske) kulture usmeri k doseganju varnostnih ciljev, vključujoč člane organizacije, sisteme in delovno aktivnost (Cooper 2000). Pri tem gre za prehod splošnega varnostnega zavedanja v varnostno kulturo, kar se zgodi v tistem trenutku, ko prične skupina kot celota varnostne kršitve socialno in moralno dojemati kot nesprejemljive za okolje, v katerem delujejo (Lobnikar in drugi 2009, 47) in se začne (samo)varnostno tudi obnašati.

Informacijske grožnje predstavljajo poleg vojaških, okoljskih, gospodarskih, političnih in zdravstvenih groženj ter groženj identitete in kulture, terorizma in kriminala, ključne dimenzije ogrožanja nacionalne varnosti sodobne družbe (Prezelj 2002, 625). Za dvigovanje zavesti o nevarnostih, ki pretijo v informacijskih sistemih in vzpostavljanje kulture informacijske družbe (Marinšek 2009) sta v Republiki Sloveniji posredno odgovorna dva direktorata, Direktorat za e-upravo in upravne procese in Direktorat za informacijsko družbo. Direktorata sta ustanovljena kot organa v sestavi Ministrstva za javno upravo in Ministrstva za visoko šolstvo, znanost in tehnologijo. Kot naslednika Centra vlade RS za informatiko, Ministrstva za informacijsko družbo in Direktorata za elektronske komunikacije nudita informacijske storitve ključnim skupnim funkcijam državne uprave in sta zaradi svojih nalog še posebej aktualna z vidika analiziranja njune interne informacijske varnostne kulture.

Ker je področje proučevanja informacijske varnostne kulture v Slovenskem okolju, v primerjavi s tujino, na precej nizki stopnji oz. je vrednost človeškega kapitala še vedno premalo cenjena, je eden izmed glavnih namenov magistrske naloge ugotoviti v kakšen

obsegu je informacijska varnostna kultura prisotna v omenjenih direktoratih. Vprašanje, ki ga bom poskušala zasledovati skozi celotno nalogo se tako nanaša na raven informacijske varnostne kulture in sicer, ali je ta v okviru osrednjih nosilcev informacijskega razvoja v državi na stopnji, ki omogoča učinkovito implementacijo informacijske varnostne politike in ostalih standardov. Osredotočila se bom na doprinos posameznika, skupin in celotne organizacije k informacijski varnostni kulturi v okviru državne uprave ter pri tem zasledovala tiste elemente, ki jo značilno opredeljujejo.

Kljub temu, da sodi Slovenija v družino najbolj razvitih tranzicijskih držav in bi pričakovali visoko stopnjo varnostne osveščenosti, ki je že prerasla usmerjanje pozornosti na tehnične mehanizme varovanja občutljivih ali zaupnih podatkov, je realnost verjetno še vedno precej drugačna. Menim, da prav okoliščine tranzicije prispevajo k počasnejšemu razumevanju ne le sodobnih trendov, temveč predvsem golih dejstev, da je vrednost posameznikov v organizaciji neizmerna in predvsem ključna za dolgoročen obstoj organizacije. Glede na relativno kratko zgodovino obstoja proučevanih direktoratov ter okoliščine mlade države, ki se svojih ranljivosti počasneje zaveda, pričakujem, da bodo rezultati raziskave opozorili na marsikatere pomanjkljivosti informacijske varnostne kulture in ponudili izhodišča za ukrepe ter morebitne izboljšave obravnavanega področja.

# 2 METODOLOŠKO HIPOTETIČNI OKVIR

## 2.1 CILJI IN POMEN NALOGE

Nebrzdan razvoj IKT-ja je v obdobju zadnjih dveh dekad prinesel poleg številnih izboljšav v okviru delovnih procesov tudi marsikatera nepredvidljiva tveganja in vplival na porast vprašanj, ki se dotikajo varnega poslovanja in upravljanja (ne)varnosti. V magistrski nalogi bom sledila odgovoru na vprašanje na kakšen način upravljati z organizacijskimi značilnostmi, da postane komponenta varnosti del prepričanj, dejanj in vedenj zaposlenih. Zanimalo me bo, kaj je tisto, kar mora zrela organizacija dodati obstoječim predpisom, paleti postopkov evidentiranja in odpravljanja napak, vključno s pravili sankcioniranja kršitev in nenehnih usposabljanj, če želi večjo učinkovitost svojih dejavnosti. Pregled publikacij s področja informacijske varnosti namreč kaže, da se relativno malo prispevkov nanaša na obravnavo informacijsko-varnostne ozaveščenosti in usposobljenosti, na odzivnost na incidente in človeški vidik informacijske varnosti (družbeni, kulturni in etični vidiki človeških virov in organizacijskih politik) (Dlamini in drugi 2009).

Teoretični del naloge bo izveden s pomočjo analize primarnih in sekundarnih virov s poudarkom na opredelitvi številnih pojmov, ki se pojavljajo v terminologiji v povezavi z varnostno kulturo in poudarkom na že opravljenih raziskavah. V teoretičnem delu bo uporabljena tudi deskriptivna analiza. Študija raziskav bo opravljena v skladu s kronološkim potekom razvoja varnostih konceptov in se bo osredotočila na varnostno kulturo v okviru okolij, ki so usmerjena v razvoj IKT-ja.

Empirični del naloge se bo nanašal na proučevanje informacijske varnostne kulture v Direktoratu za e-upravo in upravne procese ter Direktoratu za informacijsko družbo. Oba posredno vplivata na izgradnjo in oblikovanje informacijske družbe, poleg tega pa preko njiju potekajo tudi ključne informacijsko-komunikacijske aktivnosti v državi. Analiza rezultatov bo narejena s pomočjo statističnih metod, dopolnila bo teoretična spoznanja iz literature in pripravila izhodišča za nadaljnja proučevanja (meritve) informacijske varnostne kulture v organizacijskih enotah javne uprave, kot tudi v organizacijah nejavnega sektorja.

## 2.2 RAZISKOVALNE HIPOTEZE

V magistrskem delu bom preverjala dve hipotezi:

**H1: Informacijska varnostna kultura je v izbranih organih državne uprave na zadovoljivi ravni – to pomeni, da se uslužbenci zavedajo problemov varnosti.**

Predpostavljam, da je v javnem IKT-podjetju informacijska varnostna kultura na zadovoljivi ravni, ki pa se lahko z določenimi strategijami zviša.

Informacijsko varnostno kulturo bom proučevala s pomočjo devetih komponent, tj. politike in postopkov, analize tveganj, samozavedanja, etičnega ravnanja, zaupanja, finančnih sredstev, menedžmenta, benchmarkinga oz. zgledovalnega primerjanja in z vidika sprememb. Predvidevam, da bo analiza faktorjev pokazala, da prihaja do večjih težav pri posredovanju varnostnih informacij, skratka pri zaupanju in organizacijski pripravljenosti za uvajanje sprememb.

**H2: Pozitivno ocenjeni indikatorji informacijske varnostne kulture na organizacijski in skupinski ravni vplivajo na pozitivno oceno indikatorjev na individualni ravni.**

Indikatorji (ali komponente) informacijske varnostne kulture se odražajo na organizacijski, skupinski in individualni ravni. Predpostavljam, da organizacijska in skupinska raven vplivata na individualno raven, kar pomeni, da dobro ocenjene komponente na organizacijski in skupinski ravni vplivajo tudi na dobro ocenjene komponente, ki se nahajajo na individualni ravni. Oz. na vedenje posameznika je v veliki meri mogoče vplivati s pomočjo sprememb na organizacijski in skupinski ravni.

## 2.3 UPORABLJENE METODE – POTEK IN METODOLOGIJA RAZISKAVE

Za potrebe magistrske naloge bo uporabljena kvantitativna metoda raziskovanja, natančneje neeksperimentalno kvantitativno raziskovanje. Kot metoda zbiranja podatkov bo uporabljen

anketni vprašalnik, avtorja Martinsa (2002), ki sem ga priredila in dopolnila v skladu s cilji in nameni naloge.

Informacijska varnostna kultura bo v izbranih direktoratih merjena s pomočjo devetih indikatorjev (politike in postopki, analiza tveganja, samozavedanje, etično ravnanje, zaupanje, finančna sredstva, menedžment, benchmarking oz. zgledovalno primerjanje, vidik sprememb), ki odsevajo doprinos posameznika, skupine in celotne organizacije k ustvarjanju varnostne kulture. Na osnovi rezultatov opravljene raziskave bom primerjala ocene posameznih faktorjev in poskušala bodisi potrditi bodisi zavreči hipotezo 1, ki predvideva, da je informacijska varnostna kultura v organih državne uprave z visoko stopnjo informacijsko-komunikacijskih procesov na zadovoljivi ravni. Nato pa bom s pomočjo multivariatne statistične analize (regresijska analiza) poskušala napovedati vpliv indikatorjev na organizacijski in skupinski ravni na indikatorje na individualni ravni (hipoteza 2). V zaključnem delu naloge bom na podlagi rezultatov pripravila smernice, kako izboljšati oz. ohraniti trenutno stopnjo informacijske varnostne kulture v proučevanem okolju. Te bodo imele uporabno vrednost tako za vključena organa, kot tudi za vse tiste organizacije, ki se zavedajo razsežnosti njihovega socialnega kapitala.

## 2.4 STRUKTURA DELA

Magistrska naloga je sestavljena iz dveh vsebinskih sklopov, iz teoretičnega in empiričnega. V prvem sklopu je predstavljen koncept informacijske varnostne kulture, kot eden izmed možnih odgovorov na informacijska ogrožanja. V drugem, raziskovalnem sklopu pa je analizirana raven informacijske varnostne kulture v dveh direktoratih državne uprave, ki imata zaradi svojih delovnih nalog izrazito pomembno in vplivno vlogo pri varnem delu z občutljivimi podatki.

# 3 SODOBNO OBRAVNAVANJE VARNOSTI

Zaznavanje in razumevanje varnosti je v sodobni družbi podrejeno novim, spremenjenim oblikam groženj, ki premikajo kompleksnost pojava (varnost kot interes, potreba, vrednota, koncept, izziv itd.) od tradicionalnih proučevanj t. i. nacionalne varnosti oz. varnosti države do sodobnih proučevanj, ki se nanašajo na varnost posameznika in mednarodne skupnosti. Če je imelo varnostno okolje v preteklosti predvsem vojaško-politične razsežnosti, danes vključuje tudi širše socialne in kulturno-civilizacijske dimenzije (Grizold 2005, 7). Teorije kompleksnosti in kaosa poskušajo razcepljenost varnostnega okolja (»bifurcated security environment«) pojasniti kot posledico kompleksnosti družbenega in naravnega okolja, ki ob procesu globalizacije, decentralizacije moči in ohranjanja legitimnosti državnih ukrepov[1], vpliva na vedno bolj težko delitev groženj varnosti na notranje in zunanje (Prezelj, 2005). Kot pravi Prezelj (2005, 44) je teoretično aplikacijo obeh teorij na sodobno varnostno stvarnost mogoče ponazoriti z naslednjimi tezami:

- kompleksnost in kaos sta kot elementa sodobnega družbenega sistema sestavni del sodobnega varnostnega okolja opazovanih referenčnih objektov;
- enostavno varnostno okolje generira enostavne grožnje varnosti, kompleksno varnostno okolje pa kompleksne grožnje varnosti, ki temeljijo na prevelikem številu spremenljivk;
- vedenja (kompleksne) grožnje varnosti ali kompleksne krize ni mogoče povsem predvideti, saj je mogoče, da majhne grožnje varnosti povzročijo velike (kompleksne) krize in da velike potencialne grožnje sploh nimajo kriznih učinkov;
- kompleksna grožnja varnosti in kompleksna kriza sta več kot zgolj vsoti posameznih groženj in nista razpoznavni z njihovo delno (parcialno) analizo;
- ključna raziskovalna spremenljivka postanejo povezave med elementi proučevanega kompleksnega pojava (elementi kompleksne grožnje in krize ali akterji, ki izvajajo krizni menedžment);
- nadzor nad kompleksno grožnjo in kompleksno krizo je nezanesljiv in težak.

[1] Vidik zadostne stopnje legitimnosti državnih ukrepov se je okrepil zlasti po koncu obdobja hladne vojne (leta 1990) in postaja zaradi prenosa odločitev z državnega na lokalni nivo ter porasta nevladnih organizacij, vse pomembnejši element demokratičnega zagotavljanja in spoštovanja človekovih temeljnih pravic in svoboščin.

Sodobno varnostno razpravo definirajo predvsem trije referenčni objekti, ki so: na koga se varnost nanaša, kdo ali kaj to varnost ogroža in seveda, na kakšen način se varnost zagotavlja (preko varnostnih mehanizmov) (Liotta v Svete, 2005, 55). Kot je razvidno iz Tabele 3.1, lahko s pomočjo teh objektov razlikujemo med tradicionalnimi pogledi, ki razlagajo varnost z vidika zaščite nacionalnega teritorija in širših političnih interesov, medtem, ko se koncept človekove varnosti (ang. human security) povezuje z ranljivostjo mednarodne skupnosti in je po mnenju teoretikov mlajših generacij temeljni gradnik za izgradnjo stabilnih lokalnih, nacionalnih, regionalnih in globalnih okolij.

**Tabela 3.1:** Primerjava med tradicionalnimi in sodobnejšimi pogledi na koncept varnosti

| | **Tradicionalna nacionalna varnost** | **Varnost posameznika**[2] |
|---|---|---|
| **Varnost koga (referenčni objekt)** | Primarno države | Primarno posameznikov |
| **Vrednote države (varnost katerih vrednot)** | Teritorialna integriteta in nacionalna neodvisnost | Posameznikova varnost in individualna svoboda |
| **Varnost zaradi česa (ogrožanja in tveganja)** | Tradicionalne grožnje (vojaške grožnje, nasilje s strani držav) | Netradicionalne in tudi tradicionalne grožnje |
| **Sredstva za dosego varnosti** | • Sila kot osnoven instrument za zagotavljanje varnosti, ki je uporabljena enostransko za lastno varnost države<br><br>• Uravnoteženost moči je pomembna, moč je izenačena z vojaškimi sposobnostmi<br><br>• Sodelovanje med državami je nepomembno v primerjavi z zavezniškimi odnosi<br><br>• Norme in institucije imajo omejeno vrednost, še posebej v varnostni/obrambni sferi | • Sila kot sekundarni instrument, ki se ga primarno uporablja v splošnih primerih in skupaj s kaznovanjem, osebnim razvojem ter človekovim nadzorom kot ključno orodje za k posamezniku usmerjeno varnost<br><br>• Uravnoteženost moči ima omejeno korist, blaga moč je vse pomembnejša<br><br>• Sodelovanje med državami, mednarodnimi in nevladnimi organizacijami je lahko učinkovito in trajno<br><br>• Norme in institucije so pomembne, demokratizacija in zaposleni v teh institucijah prispevajo k njihovi učinkovitosti |

Vir: Bajpai (2000, 45)

[2] Varnost posameznika je postavljena v središče sodobnih varnostnih proučevanj.

Spremenjen referenčni objekt varnosti (namesto države je v ospredje postavljena družba, posamezniki, okolje, vse bolj tudi kritična informacijska infrastruktura) je sicer ob skoraj nepreglednem številu novih ogrožanj varnosti v t. i. mrežni družbi (ang. network society) razumljiv, vendar bi bilo napačno, če bi ga razumeli kot pravilnejši način zagotavljanja varnosti. Veliko varnejše je na diskusije o varnostni paradigmi včeraj in danes gledati z vidika dodane vrednosti ter jih razumeti kot dva različna pogleda na to, kako odgovoriti na varnostna tveganja in zagotavljati visoko raven varnosti.

Poleg omenjenih metodoloških sprememb sodobna varnostna obravnavanja opredeljujejo tudi konceptualne nejasnosti med pojmi, ki jih uporablja stroka, vse bolj pa tudi splošna javnost, vključno s politiko. Izrazi kot so: družba negotovosti in tveganj, ogrožanja varnosti, varnostni izzivi, nevarnosti za varnost itd., so nemalokrat uporabljeni brez poglobljenega razmisleka o tem, kaj pravzaprav pomenijo in na kaj se nanašajo. Varnostno tveganje v sodobni družbi se lahko pojasni z opredelitvijo razmerja med tveganjem in varnostjo ter tveganjem in nevarnostjo. Luhman (1997, 21–23 v Prezelj, 2001, 135) pravi, da se je v družbi ustalilo pojmovanje tveganja kot nekaj, kar je nasprotno pojmu varnosti, ob predpostavljanju, da obstoja absolutne varnosti ni. Pri razmerju med tveganjem in varnostjo je tako posameznik tisti, ki odloča o tveganju in je občutek tveganja stvar njegove lastne presoje ali odločitve. Ko pa govorimo o razmerju med tveganjem in nevarnostjo, je v razmerje vrinjeno še vprašanje negotovosti v povezavi z škodo, ki je bodisi posledica lastne odločitve (notranji dejavnik) bodisi zunanjih dejavnikov. V tem primeru torej govorimo o nevarnosti, ki jo pripisujemo predvsem okolju, odgovornost za tveganja pa nosijo posamezniki sami s svojimi odločitvami. Sodobna družba je prav zaradi odsotnosti otipljivih nevarnosti (npr. očitna nevarnost vojaškega napada), ki jo obdajajo, poimenovana kot družba negotovosti in tveganj. Razsežnosti znanstveno-tehnološkega razvoja brišejo izmerljive nevarnosti in vplivajo na to, da se kot družba počutimo veliko bolj izpostavljeni nepredvidljivim ali nepoznanim tveganjem, kot realnim nevarnostim. Na tem mestu se nam postavlja vprašanje, kakšno potencialno škodo nosijo tveganja in grožnje ter kako najbolj učinkovito odgovoriti nanje oz. upravljati z njimi. Prispodoba, ki jo je za opis odnosa med nevarnostjo in grožnjo varnosti (torej tega, da je naša varnost ogrožena) uporabil Flaker (1994 v Prezelj 2001,133–134) na preprost in dokaj banalen način ponazarja, kako pomembna so ravnanja nas samih, ostalih ljudi, pri tem, da se obstoječa grožnja pretvori v nevarnost. Npr., če je bananin olupek grožnja, potem se nevarnost, ki nam grozi, nahaja v dejstvu oziroma dogodku, da nam na olupku spodrsne in pademo. Da nam spodrsne na bananinem olupku, mora biti izpolnjen

pogoj, da leži olupek na tleh (predstavlja grožnjo), vendar pa olupek na tleh še ne pomeni, da nam bo na njem tudi spodrsnilo (predstavlja nevarnost). Skratka, grožnje in tveganja so predpogoj, da smo lahko izpostavljeni neki nevarnosti, a same po sebi še niso zadosten predpogoj, da se nam bo tudi dejansko kaj zgodilo (Prezelj 2001, 133–134). Nesreče, ki se nam pripetijo kot posamezniku ali kot organizaciji, so tako verjetno v večini primerov rezultat neprimernega upoštevanja varnostnih predpisov, malomarnosti, ki je lahko posledica tudi neznanja ali prenizke osveščenosti oz. so v splošnem posledica neprimernega vedenja, ki deluje kot sprožilec na obstoječo grožnjo.

## 3.1 VARNOSTNE TEORIJE – VARNOST KOT VREDNOTA

Literatura razlikuje med tremi smermi varnostnih paradigem ali pogledov, med tradicionalnimi (realizem, liberalizem, kopenhagenska šola), kritičnimi (kritična teorija, kritične varnostne študije, kritična teorija varnosti) in alternativnimi (konstruktivizem, koncept človekove varnosti, (neo)marksizem) (Grošelj 2007). Sodobne varnostne teorije temeljijo v večji meri na idejah realizma, liberalizma in konstruktivizma in zaradi tega je smiselno, da prikažemo varnostne implikacije uporabe IKT-ja na njihovi podlagi (Svete 2006).

Varnostne implikacije uporabe IKT-ja so s konceptom varnosti povezane posredno in neposredno. Neposredna povezanost se nanaša na vpliv, ki ga ima IKT na družbene konstrukte, na zaznavanje realnosti preko različnih sodobnih komunikacijskih tehnik in vključuje tudi zlorabe s strani uporabnikov, ki so usmerjene na različne referenčne objekte varnosti. Pri posrednih implikacijah pa uporaba IKT-ja vpliva na varnost predvsem s položaja zbiranja in obdelave podatkov (za civilne namene in potrebe nacionalno-varnostnega sistema), pri čemer lahko govorimo o vplivu na fizična razmerja moči in organizacijske spremembe (Svete 2006, 61). Kljub temu, da so neposredne povezave bolj opazne kot posredne, še posebej zaradi naraščajočega števila zlorab sodobne tehnologije, je smiselno poudariti, da je znanstveno-raziskovalno proučevanje povezanosti med varnostjo in uporabo IKT-ja še vedno na precej nizki ravni. Vse skupaj pa otežujejo še slaba odzivnost referenčnih objektov varnosti, pomanjkanje znanja in tudi težka sledljivost razvoju IKT-ja.

*Realizem*

Realizem predpostavlja, da je (a) država glavni subjekt varnostnih obravnav, (b) da država deluje racionalno z namenom zaščititi svoje nacionalne interese ter (c) da sta moč in varnost njeni temeljni vrednoti (Eriksson in Giacomello 2006). Realizem se centralistično osredotoča na blaginjo države, torej na njeno varnost in vidi grožnje predvsem v prisotnosti drugih držav v mednarodni skupnosti. Odgovor na vprašanje, kako zagotavljati varnost, išče posledično v okviru militarističnih idej in premoči nad drugimi državami v okviru vojaških sposobnosti. Klasična realistična misel je tako ozko vezana na varnost kot obliko vojaške moči (avtoritete) držav, ki bi naj zagotavljala stanje varnosti. Medtem ko neorealizem, kot oblika realizma, ki se je razvila ob boku klasičnih realističnih idej, na drugi strani najpomembnejši izvor moči išče v kombinaciji zmožnosti, ki so dane znotraj posamezne države in se ne osredotoča zgolj na vojaško moč. Neorealisti še vedno izpostavljajo pomembnost bojevanja držav za lastno prevlado oziroma nadvlado, a usmerjajo svojo pozornost tudi k temu, da druge države ne bi pridobile preveč na moči. Za njih je namreč ravnotežje moči rešitev za doseganje reda v mednarodnem sistemu (Lamy 2007, 268).

*Liberalizem*

Liberalizem odlikujejo štiri temeljne prvine, ki jih Rizman (1992, 15) poimenuje:

- individualistična prvina – zagovarja moralno primarnost osebe pred zahtevami katerekoli družbene kolektivitete;
- egalitarna prvina – ima za legitimen samo tisti družbeni red, ki med ljudmi ne dela razlike glede na njihovo (enako)vrednost ter moralni status;
- univerzalistična prvina – se izraža skozi načelo moralne enotnosti vseh ljudi ne glede na raso ali etično pripadnost in pripisuje sekundarni pomen njihovemu historičnemu formiranju;
- melioracijska prvina – zagotavlja, da je vedno mogoče popravljati in izboljševati družbene institucije in vsakršne politične dogovore.

Varnost in ekonomski napredek sta v liberalistični misli kombinacija demokracije in tržnega kapitalizma. Demokratične vrednote uveljavljajo spoštovanje pravne države ter zagotavljajo

temelj za vsesplošno moralno in politično soglasje med državami, ki so pravni državi zavezane. Tržni kapitalizem ustvarja meddržavne vezi s spodbujanjem soodvisnosti med državami, ki zaradi ekonomskih koristi v miru odtehtajo morebitne koristi v vojni in tako v primerjavi z vojskovanjem zagotavljanja učinkovito alternativno metodo za doseganje blagostanja (Freedman 1994, 109 v Malešič 1994, 101). Pripravljenost držav na uporabo sredstev ali popuščanje drugim državam tako ni odvisno od zmožnosti, kot je to pri realizmu, ampak od referenc (Moravcsik 1997, 523). Pri tem se liberalisti seveda strinjajo z realisti, da ostajajo države glavni akterji svetovnih politik, a so v nasprotji z njimi prepričani, da države niso edini subjekt, ki igra pomembno vlogo v mednarodnih odnosih. Pri tem poudarjajo zlasti vlogo nedržavnih mednarodnih akterjev, kot so npr. transnacionalne korporacije, socialna gibanja, interesne skupine, omrežja političnih strank, migranti in teroristi (Eriksson in Giacomello 2006, 230).

*Konstruktivizem*

Če realisti vidijo grožnje, ki jih prinaša uporaba IKT-ja, kot pretežno ekonomski problem, ki ne nujno zadeva varnosti držav in zaradi tega sam po sebi še ne predstavlja grožnje varnosti (Eriksson in Giacomello 2006, 229), se konstruktivisti v svojih idejah veliko bolj naklonjeni prepoznavi sodobnih oblik tveganj. Konstruktivizem proučuje zagotavljanje varnosti s pomočjo razlikovanja med materialno resničnostjo (npr. računalniki, kabli) in družbeno realnostjo (identitete, interesi, norme in institucije). V nasprotju z materialno resničnostjo, je družbena realnost pogojena s strani ljudi in zaradi tega vseskozi občutljiva na raznovrstne vplive. To pomeni, da je ne moremo razumeti kot stalno obliko realnosti, temveč kot nekaj, kar se vseskozi spreminja in na novo ustvarja (ibid, 233). Če so za realiste in liberaliste, kot pristaše materialne resničnosti, moč in nacionalni interesi najpomembnejše gonilo mednarodnih odnosov, se konstruktivisti zavedajo tudi pomena idej, konceptov ter se trudijo razumeti materialni svet širše. Finnemore (1996, 128 v Jackson in Sørenses 2007, 170) pravi, da »dejstvo, da živimo v mednarodni družbi pomeni, da je tisto, kar želimo in na nek način, tudi tisto, kar smo, izoblikujejo družbene norme, pravila, razumevanje in odnosi, ki jih imamo z drugimi. Te družbene realnosti so enako vplivne kot materialne realnosti pri kreiranju obnašanja. Dejansko so tisto, kar daje materialnim realnostim smisel in namen. V političnem smislu so prav te družbene realnosti tiste, ki določajo na kakšen način se lahko uporabi moč in izobilje.«

Uporaba orožja in drugih sredstev kot fizičnih materij, je z vidika konstruktivizma pogojena z družbeno realnostjo, ki jo ustvarjajo ljudje in je sekundarnega pomena, če je ne povezujemo s komponento inteligence. Mednarodni sistem varnosti in obrambe tako ni definiran le z elementi ozemlja, populacije in orožja, saj na smernice njegovega gibanja vplivajo tudi nacionalni karakterji držav oz. posamezne identitete držav, ti pa so odraz idej, prepričanj in kulture okolja (Jackson in Sørenses 2007).

Kratek pregled obstoječih varnostih teorij kaže, da vpliva informacijske revolucije na sodobno obravnavanje varnosti ne moremo v celoti pojasniti s pomočjo omenjenih teorij. Nobena izmed varnostnih teorij se namreč ne ukvarja temeljito z vprašanjem, kako učinkovito odgovoriti na netradicionalne oblike nevarnosti, ki ogrožajo državljane, države in globalno skupnost. Kljub vsemu lahko ocenimo, da sta s svojimi pogledi liberalizem in konstruktivizem vseeno bliže varnostim implikacijam IKT-ja kot realizem. Liberalizem zajema elemente varnosti v digitalni družbi, ko govori o porastu nedržavnih akterjev, katerih zmožnosti segajo čez nacionalne meje, o gospodarskih omrežjih, »ranljivi neodvisnosti« in prosojnosti formalno suverenih meja. Konstruktivizem pa je primeren predvsem z vidika analiziranja simboličnih, retoričnih in identitetnih dimenzij digitalne dobe (Eriksson in Giacomello 2006, 236). Neposredna uporaba IKT-ja s sabo prinaša namreč spremembe na področju varnosti, ki so povezane z zaznavo stvarnosti. Ta ni več omejena s časom in prostorom ter je zato ne moremo več zadovoljivo proučevati s pomočjo in samo s tradicionalnimi materialističnimi oziroma pozitivističnimi pristopi (Svete 2006). Svete (2006, 63) tudi meni, da družbene in kulturne predispozicije (strateška kultura – kulturalizem) tako posameznega uporabnika kakor tudi družbenih institucij determinirajo, kako bo uporaba IKT-ja vplivala na varnost države, družbe ali posameznika. Zaradi tega je pomembno, da varnostne strategije vključujejo dognanja konstruktivizma in sodobnih pogledov na zagotavljanje varnosti, saj večja navzočnost IKT-ja v državi še ne pomeni nujno tudi sorazmerno pomembnejših varnostih implikacij.

## 3.2 DIMENZIJE OGROŽANJ SODOBNE VARNOSTI

Organizacija združenih narodov (v nadaljevanju OZN) v poročilu Visokega panela o grožnjah, izzivih in spremembah (United Nations 2004, 1) ugotavlja, da počiva sodobno pojmovanje kolektivne varnosti na naslednjih treh stebrih: današnje grožnje ne poznajo nacionalnih meja, med sabo so povezane in zoperstavljati se jim je potrebno na globalni in

regionalni, kot tudi na nacionalni ravni. Večdimenzionalnost groženj izvira že iz samega opredeljevanja pojavov, ki jih pojmujemo kot ogrožajoče za nacionalno varnost. Npr. Ullman (1983, 133) opredeljuje za grožnje nacionalne varnosti vse dogodke ali sekvence dogodkov, ki a) grozijo, da bodo v kratkem drastično zmanjšali kakovost življenja prebivalcev države, ali b) da bodo močno zožili izbiro možnih političnih akcij, ki jih ima na voljo država ali zasebni nevladni subjekti (posameznikom, skupinam, korporacijam) znotraj države. Skratka, grožnje sodobne varnosti torej definira, če si izposodimo znani rek filozofa Aristotela, »verjetnost, da se bo malo verjetno zgodilo« in prav zaradi tega je pomembno, da si nekoliko podrobneje pogledamo katere družbene vrednote so v sodobnem času najbolj ogrožene.

Pregled strokovne literature kaže, da se tradicionalne grožnje varnosti v času postmoderne družbe povezujejo s številnimi drugimi netradicionalnimi oblikami groženj, ki imajo bodisi makro bodisi mikro vpliv na varnost posameznika. Zaradi sistematične preglednosti si bomo izposodili klasifikacijsko tabelo dimenzij ogrožanj nacionalne varnosti (glej Tabelo 3.2), ki jo je pripravil Prezelj (2002, 625). Prezelj namreč poleg tradicionalnih vojaških groženj, opozarja tudi na okoljske, gospodarske, politične, informacijske, identitetne, kulturne ter zdravstvene grožnje, ki jim dodaja še grožnje kriminala in terorizma.

**Tabela 3.2:** Dimenzije ogrožanja nacionalne varnosti in odgovarjajoči nacionalni varnostni interesi

| **Dimenzije ogrožanja nacionalne varnosti sodobne države (RS) z osnovnimi indikatorji:** | **Nacionalni varnostni interesi:** | **Dimenzije ogrožanja nacionalne varnosti sodobne države (RS) z osnovnimi indikatorji:** | **Nacionalni varnostni interesi:** |
|---|---|---|---|
| **Vojaške grožnje:**<br>– oborožena (JKB ali konvencionalna) agresija na državo in njeno suverenost<br>– demonstracija vojaške sile<br>– geografska bližina oboroženega konflikta<br>– geografska bližina reguliranega (oboroženega) konflikta<br>– širjenje orožja za množično uničevanje | – odvračanje, zagotavljanje bojne pripravljenosti, vojaška obramba<br>– odvračanje, vojaška obramba<br>– odvračanje, nudenje vojaške pomoči, sklepanje vojaških oziroma obrambnih koalicij, sodelovanje v mednarodnih operacijah vsiljevanja miru in nadziranja ali vsiljevanja | **Politične grožnje:**<br>– nedemokratičnost političnega sistema<br>– nespoštovanje človekovih pravic in svoboščin<br>– medijska nesvoboda<br>– visoka stopnja korupcije | – zagotoviti transparentnost, pluralnost in demokratičnost političnega procesa (oblikovanja in izvajanja politik)<br>– zagotoviti spoštovanje človekovih pravic in svoboščin<br>– zagotovitev svobode medijev, izogibanje cenzuriranim |

| | | | |
|---|---|---|---|
| | sankcij<br>– sodelovanje v mednarodnih mirovnih in humanitarnih operacijah<br>– onemogočiti širjenje orožja za množično uničevanje | | pritiskom, korektno obveščanje širokega spektra javnosti<br>– preprečevanje korupcije na vseh državnih in nedržavnih nivojih |
| **Okoljske grožnje:**<br>– naravne in antropogene nesreče (poplave, potresi, požari, nevihte…)<br>– onesnaževanje okolja, globalno segrevanje<br>– pomanjkanje vode | – preprečevati nastanek naravnih in antropogenih nesreč, učinkovito obveščanje prebivalstva o nevarnostih, izvajanje zaščite in reševanja prebivalstva, premoženja in državnih institucij na kriznih območjih<br>– upoštevanje okoljevarstvenih standardov, zmanjševanje onesnaževalnih emisij v zrak, vodo in zemljo<br>– zagotoviti zadostne količine tega temeljnega sredstva za življenje, smotrna izraba obstoječih vodnih virov | **Identitetne in kulturne grožnje:**<br>– etnična, verska in jezikovna heterogenost, če povzroča neenotnosti in konflikte<br>– izginjanje oziroma omejevanje temeljnih kulturnih vzorcev<br>– velika stopnja ilegalne migracije<br>– veliko število beguncev | – zmanjšanje negativnih (varnostnih) posledic teh konfliktov<br>– prispevanje k ohranjanju in razvoju nacionalnega jezika ter negovanje splošnih tradicij<br>– omejiti pritok ilegalnih migrantov<br>– sprejemati zmerno število beguncev |
| **Gospodarske grožnje:**<br>– nizka stopnja gospodarskega razvoja, nizek BDP, revščina (v tej funkciji tudi visoka stopnja zadolženosti in visoka inflacija)<br>– visoka stopnja brezposelnosti<br>– velika odvisnost od uvoza materialnih dobrin (tudi veliko nesorazmerje med uvozom in izvozom) | – zagotovitev čim večje stopnje gospodarske razvitosti, produktivnosti in rasti ob upoštevanju novih tveganj, ki se pojavijo s tem<br>– neposredno ali posredno zmanjšati brezposelnost v družbi<br>– zagotovitev suverenega razpolaganja s strateškimi surovinami in viri | **Zdravstvene grožnje:**<br>– velika razširjenost nalezljivih bolezni (AIDS, tuberkuloza, ebola itd.) | – preprečiti nastanek in širitev nalezljivih bolezni, zavarovanje področij, ki so izpostavljena nalezljivim boleznim |
| **Kriminal:**<br>– visoka stopnja kriminalitete v družbi (ropi, umori, trgovanje z drogami itd.)<br>– tihotapljenje JKB materialov in konvencionalnega orožja itd.) | – nizka stopnja kriminalitete v družbi, odkrivanje ter preprečevanje uporabe drog in trgovanja z drogami<br>– učinkovit nadzor nad tokovi ilegalnega trgovanja z orožjem in drugimi nevarnimi materiali | **Terorizem:**<br>– obstoj in delovanje mednarodnih ali nacionalnih terorističnih skupin (sabotaže, bombni napadi, JKB terorizem, politični umori, ugrabitve letal, talcev, napadi na ambasade itd.) | – omejitev možnosti in razlogov za nastanek nacionalnih terorističnih skupin, odkrivanje in preprečevanje delovanja terorističnih skupin |

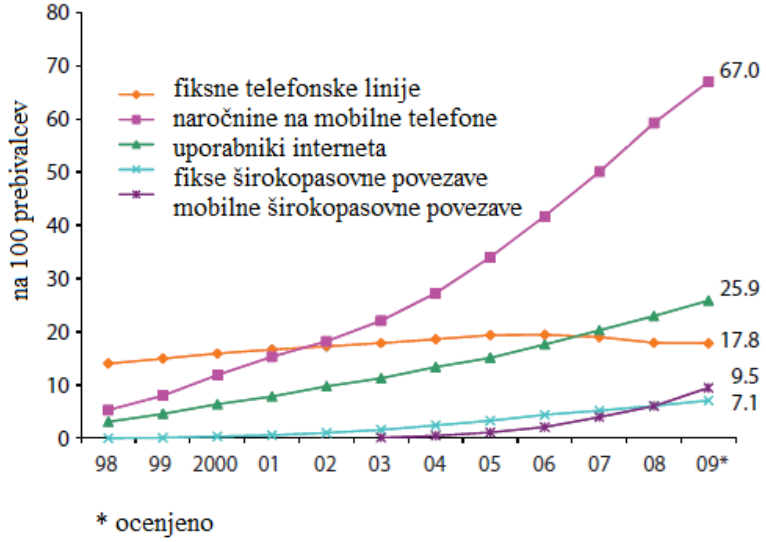
| | | | |
|---|---|---|---|
| **Informacijske grožnje:** – vdor v ključne informacijske mreže in njihova onesposobitev | – zagotavljanje visoke stopnje zaščite pred (kiber) vdorom v ključne nacionalne informacijske sisteme, baze itd. | | |

Vir: Prezelj (2002, 625)

Za primerjavo – OZN (2004) v prej omenjenem Panelu, izpostavlja šest skupin ogrožanj, ki zahtevajo pozornost in predloge za preprečevanje njihovega širjenja. Te skupine vključujejo ekonomske in družbene grožnje (skupaj z revščino, nalezljivimi boleznimi in slabšanjem ekološke vrednosti okolja), meddržavne konflikte, konflikte znotraj držav (vključno s civilnimi vojnami, genocidi in ostalimi grozodejstvi), jedrska, radiološka, kemična in biološka orožja ter terorizem in transnacionalni organizirani kriminal. Oceniti je mogoče, da se klasifikaciji najvidnejših groženj med sabo bistveno ne razlikujeta, OZN morda nekoliko očitneje izpostavi le grožnjo varnosti, ki jo s sabo nosijo neklasične oblike orožja s tem, ko poudarja, da mora postati preprečevanje širjenja in potencialne uporabe jedrskih, radioloških, kemičnih in bioloških orožij, ena izmed ključnih prioritet kolektivne varnosti. Nasprotno pa klasifikacija ogrožanj po Preglju izpostavlja še pojavne oblike groženj v IKT-ju, ki so drugače pogosto zajete v skupini ekonomskih in družbenih ogrožanj.

Naraščajoča uporaba in neprestan razvoj IKT-ja, ki je prikazan v spodnji Sliki 3.1, vplivata na povečano poudarjanje pomena informacijske varnosti in potencialnih spremljevalnih tveganj. Če se je še do nedavnega na informacijsko varnost gledalo kot na področje, ki ne pogojuje uspešnosti podjetja, se danes vse več organizacij zaveda njene integralne vrednosti. Zaradi neposredne povezanosti informacijske varnostne kulture z informacijsko varnostjo, saj je prva pomemben gradnik druge, bomo nekoliko več pozornosti namenili tudi informacijskim grožnjam, torej grožnjam zaradi katerih je razvijanje informacijske varnosti sploh potrebno.

**Slika 3.1:** Globalni razvoj IKT, 1998–2009




Vir: ITU World Telecommunication/ICT Indicators database v International Telecommunication Union (2010, 1)

### 3.2.1 Informacijska ogrožanja

Za področje varovanja informacij lahko rečemo, da je staro toliko, kolikor so stare prve informacije. Od trenutka dalje, ko se je informacijo preneslo, preoblikovalo ali shranilo, je bila potrebna tudi njena zaščita. Ta se je skozi zgodovinska obdobja seveda spreminjala in prešla od iskanja načinov, kako zaščiti vsebino zaupnih pisem, do tega, kako zavarovati telegrame in telefonske pogovore in danes išče predvsem poti, kako narediti računalniško okolje varnejše (Dlamini in drugi 2009).

Čas od 1940 do 1950 je zaznamovala prva generacija računalnikov, ki s sabo še ni prinesla širše uporabnosti. Mrežne povezave med računalniki še niso delovale, poleg tega je imelo dovoljenje za dostop in uporabo računalnikov le nekaj računalniških operaterjev. S pojavom t. i. neumnih terminalov (ang. dumb terminals) pa dobijo računalniki v obdobju poznih 60. let do zgodnjih 70. let tudi širšo uporabnost. Ti t. i. neumni terminali so imeli nalogo posredovanja vhodnih signalov centralnemu računalniku in prikaz (povratnih) izhodnih signalov iz centralnega računalnika ter so s svojim delovanjem omogočili številnim uporabnikom dostop in uporabo podatkov na daljavo. Novost je s sabo seveda prinesla tudi nevarnost pred nepooblaščenim dostopom. Ker fizično varovanje pri zaščiti pred nepooblaščenim dostopom do podatkov ni prineslo vidnejših rezultatov, so prvi postopki

identifikacije in dokazovanja pristnosti, prišli v uporabo že v začetku 70. let. Postopki so bili izredno preprosti, saj v tistem času še niso poznali varnostih politik glede uporabe zahtevnejših gesel, posledično pa so bili tudi zelo izpostavljeni zlorabam. Obdobju terminalov je sledilo obdobje manjših računalnikov, ki so zaznamovali začetek omrežij in sistemov širše uporabe, prav tako je v veljavo stopil javni kriptografski ključ. 80. leta so razvoj računalništva samo še pospešila, saj je predstavitev osebnih računalnikov povzročila povečanje števila zasebnih uporabnikov. Podjetja so začela avtomatizirati svoje postopke, s tem pa vplivala na oblikovanje novih tveganj, saj so bili sedaj občutljivi poslovni podatki shranjeni na lahko dostopnih virih. Področje informacijske varnosti se je zaradi tega okrepilo in intenziviralo tudi z zabeleženjem prvih vdorov v računalnike, ki so se zgodili v Standfordskem kampusu in vojaški bazi v ZDA v 80. letih in zaradi pojavov računalniških virusov. 90. leta so bila v znamenju odprtih sistemov in mobilnega računalništva. Vse več osebnih računalnikov se je začelo povezovati z internetom, kar je privedlo do novih tveganj, ki so bila sicer zaradi odprtosti internetnih povezav pričakovana. Proti koncu 90. let se uporaba osebnih računalnikov nenehno viša, prav tako se vse več ljudi povezuje z internetom. Opazno se spremenijo tudi oblike napadov na računalniške sisteme, ki so v primerjavi s preteklo uporabo različnih virusov in črvov, veliko bolj zapletene. V tem času se prvič pojavi t. i. porazdeljena zavrnitev storitve (ang. distributed denial of service) kot oblika napada na računalnik, poleg tega tudi zlonamerne kode, ki jih prejemnik sprejme skupaj z elektronsko pošto. Oboje vpliva na uvedbo filtrirnih požarnih zidov in sistemov nadzora (Dlamini in drugi 2009, 190–191).

Vstop v novo stoletje je s sabo prinesel pričakovane spremembe. Informacijsko-komunikacijska infrastruktura je postala pomemben element v panogah, saj je vse več dejavnosti odvisnih od elektronskih povezav. Razvilo se je spletno bančništvo, prav tako je neverjeten razmah mobilnega računalništva. Sorazmerno z razvojem IKT-ja pa se seveda razvija tudi temna stran napredka. Računalniški hekerji so intelektualne izzive vdiranja v računalniške sisteme zamenjali s finančnimi razlogi in tako postali veliko drznejši. To pa povzroča nove oblike groženj informacijski varnosti, kot so npr. kraja identitete, socialni inženiring, spletno ribarjenje itd., saj lahko storilci brez večjih težav pridejo do podatkov, ki jim omogočijo upravičen dostop do številnih baz (ibid.).

Prezelj (2005, 51–52) pravi, da je z vidika informacijskih tveganj najbolj problematično in paradoksalno prav to, da se večina groženj širi transnacionalno prek obstoječih komunikacijskih sredstev. In pravzaprav vsaka nova stopnja tehnološkega razvoja prinaša s

seboj tudi posredne ali neposredne negativne posledice, ki jih lahko označimo za grožnje varnosti.

#### *3.2.1.1 Vrste informacijskih groženj*

Informacijske grožnje delimo v splošnem v dve temeljni skupini:

- grožnje okolja;
- grožnje, ki jih povzroča človek (Benson in drugi, 2010).

K tema osrednjima skupinama pa je potrebno dodati tudi tehnične grožnje, ki so sicer posredno povzročene s strani ljudi, a predstavljajo tako veliko skupino, da jih je potrebno omeniti posebej. Pomembno je namreč, da organizacije ne pozabijo na ranljivosti v informacijskih in komunikacijskih sistemih, ki lahko same privedejo do nesreč oz. jih izkoristi nekdo drug (grožnja s strani ljudi). Preverjanje tehničnih ranljivosti mora biti zato periodično in proaktivno.

Grožnje, ki izvirajo iz narave, so nepredvidljive in organizacije se težko ubranijo pred njimi. Naravne nesreče kot so potresi, poplave, neurja s strelami, požari, itd., lahko povzročijo ogromno škodo na računalniških sistemih. Ta je tako materialne (poškodovanje strojne opreme) kot tudi vsebinske narave (izguba programske opreme), saj se z uničenim računalnikom pogosto uničijo tudi podatki, ki so shranjeni na njem. V skupino groženj iz okolja uvrščamo tudi grožnje nemirov, vojn in terorističnih napadov, ki se, čeprav so posledica človeških ravnanj, uvrščajo v to skupino ravno zaradi svojih razsežnosti in videza nesreče. Poleg tega se je zoper njih nemogoče ubraniti z varnostnimi politikami in nadzorovanjem zaposlenih (ibid.).

Drugo skupino groženj sestavljajo t. i. človeške groženje oz. tveganja, ki jih povzroča vedenje ljudi. Ločujemo med grožnjami varnosti, ki so posledica zlonamernih in nenamernih ravnanj. Nenamerne grožnje so navadno posledica nevednih uporabnikov in zaposlenih, ki niso zadosti usposobljeni za delo z računalnikom in ne poznajo raznolikosti računalniških tveganj. Medtem ko so zlonamerni napadi navadno storjeni s strani oseb, ki v organizaciji niso zaposlene ali nezadovoljnih in razočaranih zaposlenih, ki skušajo z zlorabo doseči določen namen (ibid.).

Med glavne kategorije groženj informacijske varnosti, ki so posledica človeških ravnanj, se uvrščajo številne oblike računalniške, internetne in telekomunikacijske kriminalitete. Zaradi lažje preglednosti, jih prikazujemo v nekoliko daljši Tabeli 3.3.

**Tabela 3.3:** Najbolj pogoste in najbolj znane tehnike računalniške kriminalitete

| Računalniška in internetna kriminaliteta | | | |
|---|---|---|---|
| Angleški izraz | Slovenski izraz | | Kaj izraz pomeni – pojavne oblike |
| Computer Crime (CC)<br><br>Computer related<br>Crime – CRC | računalniška kriminaliteta (RK)<br><br>(pogovorno: računalniški kriminal)<br><br>kriminaliteta povezana z računalnikom<br><br>(pogovorno kriminal povezan z računalnikom) | | KD povezano ali strojeno z računalnikom in IT. Ključne pojavne oblike računalniške kriminalitete so:<br>• vdori v tuje računalnike in računalniške sisteme in komunikacijska omrežja IT<br>• neopravičena manipulacija s podatkovnimi bazami in nepooblaščeno spreminjanje podatkov<br>• razne oblike špijonaže (poslovna, vojaška, industrijska, politična)<br>• računalniško piratstvo<br>• pornografija<br>• napadi z elektronsko pošto (DDOS)<br>• prestrezanje uporabniških gesel<br>• kraja identitete (spoofing)<br>• goljufije vseh vrst, vključno s kreditnimi karticami<br>• prestrezanje ali spreminjanje elektronskih sporočil itd. |
| Internet Crime<br><br>Cyber Crime | internetna kriminaliteta<br><br>pogovorno: internetni kriminal | | KD, pri katerih storilec uporablja internet kot orodje za dosego svojega cilja ali pa napade internet (medmrežje) kot tako in uporabnikom povzroči škodo ali neprijetnosti |
| Telecommunications Crime | telekomunikacijska kriminaliteta | | nepooblaščen dostop do sistemov telefonije, kloniranje mobilnih telefonov, prestrezanje elektronskih komunikacij, izdelava in pošiljanje lažnih elektronskih komunikacij |
| | | | |
| Vrste računalniške kriminalitete | | | |
| Hacking | neavtoriziran dostop v sistem | | uporaba računalnika ali računalniškega sistema za pridobitev nedovoljenega dostopa v druge računalnike ali računalniške sisteme ter programe in podatkovne zbirke, ki so v lasti drugih fizičnih in pravnih oseb in vladnih organov |
| Cracking<br><br>Cracker | krekanje, razbijanje kode<br><br>kreker | | kreker je oseba, ki: 1) vdira v računalniške sisteme 2) išče načine, da bi obšla varnostne in licenčne zaščite izdelka 3) namenoma izrablja luknje v sistemu in razbija računalniško zaščito |

| | | | |
|---|---|---|---|
| Robbery, burglary, theft of computers or their components | rop, vlomna tatvina, tatvina računalnikov ali njihovih komponent | | • klasično KD, uperjeno zoper računalnike in računalniške sisteme, podatkovne zbirke, programsko opremo itd.<br>• uporaba računalnika ali računalniškega sistema za načrtovanje, pripravo in izvedbo omenjenih KD |
| Financial Crimes | finančna kriminaliteta | | • kraja identitete<br>• goljufija in preslepitev<br>• ponarejanje<br>• kraja sredstev s pomočjo računalnika ali računalniškega programa oz. s pomočjo elektronskih pripomočkov IKT-ja, itd. |
| Exploitation of children | izkoriščanje in zloraba otrok | | • otroška pornografija<br>• prežanje in napad na otroka (child predators) |
| Drug Crimes | hudodelstva povezana z nedovoljenimi drogami | | • shranjevanje podatkov o strankah na računalniku<br>• shranjevanje in pripravljanje receptur za proizvodnjo nedovoljenih drog<br>• finančni podatki o prodaji, nakupih nedovoljenih drog |
| Counterfeiting | ponarejanje | | uporaba računalnikov in tiskalnikov za protizakonito izdelavo bankovcev, menic, čekov, denarnih nakazil, različnih dokumentov, kuponov za popuste v trgovinah, ovitkov itd. |
| Theft of telecommunications Services | kraja telekomunikacijskih storitev | | KD pri katerih storilec nepooblaščeno dostopa v telekomunikacijski sistem in si protipravno prilašča storitve tega sistema |
| Homicide | umor | | dokazi pridobljeni z računalnika žrtve ali storilca, povezani z načrtovanjem, poskusom ali storitvijo KD umora |
| Spying | vohunjenje | | nedovoljeno in nezakonito zbiranje obveščevalnih podatkov |
| | | | |
| Najpogostejši tipi računalniške kriminalitete | | | |
| Altering website | predrugačenje spletne strani | | Nepooblaščeno in protipravno spreminjanje oblike ali vsebine tuje spletne strani. |
| Defacement | predrugačenje spletne strani | | Nepooblaščeno in protipravno spreminjanje oblike ali vsebine tuje spletne strani. |
| DoS –Denial of Service Attack | onemogočanje storitev | | *Denial-of-service attack* (DoS attack) je poskus, da se onemogoči določen računalnik s preobremenitvijo – pošiljanjem ogromnih količin elektronske pošte ali zahtevkov na določen IP naslov. Običajno so tarče znane internetne firme (Amazon, Yahoo – Young in Aitel 2004, 65) pri nas pa so znani napadi na SIOL in 24ur.com. Pri teh napadih gre tudi za to, da postane spletna stran nedostopna za druge uporabnike, zaradi ogromnega prometa.<br><br>V bistvu gre za dve vrsti napadov:<br><br>– pri prvem se z njimi doseže to, da napadeni računalniki |

| | | | |
|---|---|---|---|
| | | | ne morejo več opravljati svoje naloge ali pa postanejo nedosegljivi. Potrebno jih je resetirati<br><br>– pri drugi obliki gre za onemogočanje komunikacije med napadenim strežnikom oziroma spletnim mestom in drugimi uporabniki interneta. (Tripton in Krause 2004, 260–261) |
| DDoS – Disturbed Denial of Service Attack | porazdeljeni napadi zavrnitve storitve | | Storilci z njimi preplavijo določeno tarčo z uporabo podračunalnikov, kar povzorči njeno zrušenje. |
| Spoofing | sleparjenje | | Spoofing je ustvarjanje TCP/IP paketov z uporabo IP naslova nekoga drugega. Ruterji uporabijo namembni IP naslov za posredovanje paketov pri čemer zanemarijo izvorni IP naslov, ki ga uporablja le namembni strežnik za odgovor izvornemu. |
| IP spoofing | IP slepljenje ali IP sleparjenje | | Napadalec uporabi izvorno usmerjene pakete za vstavljanje ukazov v povezavo med dvema vozliščema omrežja, pri čemer sam sebe prekrije in nastopa kot eden od avtentificiranih uporabnikov. Ta način napada je mogoč, ker je avtentifikacija narejena običajno le enkrat, na začetku TCP seje (komunikacije). |
| E-mail spoofing | e-poštno sleparjenje | | Pošiljanje e-poštnih sporočil, katerih oblika in slog spominjajo na neko uveljavljeno blagovno znamko, npr.: e-bay, City bank, NLB d.d. itd. Z namenom zavesti prejemnika, da stori nekaj, s čimer razkrije pomembne podatke o sebi ali da stori nekaj, zaradi česar bo utrpel materialno škodo na svojem bančnem računu |
| Phishing | pošiljanje e-poštnih zahtevkov, lažno predstavljanje, ribarjenje v kalnem, lovljenje zaupnih podatkov, fišing | | Pošiljanje e-sporočil, ki od prejemnika zahtevajo neko akcijo, najpogosteje posredovanje osebnih in bančnih podatkov, ki jih storilci KD uporabijo pri goljufijah, v zadnjem času tudi uporabniškega imena in gesla za dostop do poštnega strežnika itd. |
| Pilfering | ni prevoda | | Kraja lastniške informacije: domači naslov, domača štev. telefona, imena moža in otrok, znesek plače, zdravstvena datoteka, informacije o kreditni kartici, TRR, poročila o rezultatih. |
| Pharming | zvabljanje | | Preusmerjanje uporabnikov z določene spletne strani na lažne, a podobne spletne strani. |
| Salami slicing | ponavljajoča se kraja majhnih vsot denarja s pomočjo računalniškega programa | | Kriminalci, najpogosteje uslužbenci, ki sodelujejo pri pretoku denarja, izdelajo program, ki zelo majhne vsote nakazuje na poseben račun; najpogosteje gre za zaokroževanje zneskov, npr. stotinov na najbližje celo število; ker pa je teh operacij veliko, se naberejo na računu znatna sredstva; predvsem gre za to, da zaradi zelo majhnih vsot skoraj nihče ne opazi primanjkljaja, medtem ko ves ta drobiž skupaj lahko predstavlja milijonske vsote. |
| Spam | neželena pošta – spam | | SPAM je sinonim za neželeno elektronsko pošto; izraz SPAM je prvič uporabilo podjetje Hormel Foods na pločevinki konzervirane šunke. V humoristični TV seriji Monty Python's Flying Circus je bil kasneje prikazan skeč, v katerem neka restavracija streže raznovrstno |

| | | | |
|---|---|---|---|
| | | | hrano, ki je vsa polna šunke, tako da natakarica mnogokrat ponovi besedo spam, ko opisuje, iz česa je posamezen obrok. Skeč se konča, ko skupina Vikings v ozadju začne peti spam, spam, spam, tako da preglasi vse ostale in se sliši samo še spam. |
| Session hijacking<br><br>TCP session hijacking | ugrabljanje povezav | | Napad na uporabnikovo povezavo preko zaščitenega omrežja. Najpogostejši načini so IP sleparjenje; drug način ugrabljanja povezave je znan pod izrazom man-in-the-middle – napad vmesnega moža, pri katerem napadalec uporablja t. i. sniffer; na ta način spremlja komunikacijo med posameznimi računalniki in zbira podatke, ki se prenašajo med njimi. |
| Skimming | ni prevoda | | Skimming je tatvina podatkov o kreditni kartici, ki jo storilec izvede med drugo legalno transakcijo, običajno tako, da namesti v bralnik kreditnih kartic posebno napravo, ki podatke prenaša na server, ki ga prej pripravi in istočasno z mikro kamero posname PIN kodo, ki je sicer ni na magnetnem zapisu kartice. Kasneje podatke prenese na bianco kartico in z njo dviga denar na bankomatih. |
| Abuse of Steganography | zloraba steganografija (v grščini pomeni zakrito pisanje) | | Boni in Kovacich (2000, 118) pišeta, da je to datoteka, vstavljena v drugo obliko datoteke, ki je najpogosteje grafika, zvok, tekst, HTML in PDF file. Nedolžna slika, ki nosi informacijo se imenuje »kontejner«, »sporočilo« pa je zakrita informacija. Uporablja se lahko kot oblika komunikacije v okviru sodobnega terorizma in organiziranega kriminala. |
| "Security Through Obscurity" | besedno zvezo opisal neznani avtor/heker (2000, 62) | | Besedna zveza se nanaša na cel kup softvera, ki ima sistemske luknje, ki jih odkrivajo ter zlorabljajo hekerji. |

Vir: prirejeno po Dvoršak in Dobovšek (2009, 446–450)

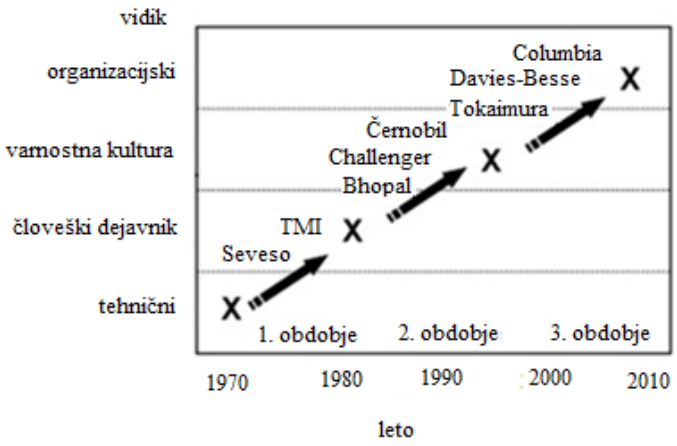
Poleg omenjenih groženj je potrebno izpostaviti tudi socialni inženiring kot vedno bolj razširjeno obliko ogrožanja informacijske varnosti, ki v tabeli ni zajeta. T. i. socialni inženiring, kljub temu da ni povezan s kriptografijo, išče točke, ki so v večini varnostih sistemov najšibkejše, torej ljudi, ki te sisteme uporabljajo in vzdržujejo (Howard in drugi 2001, 117) ter poskuša preko njih uresničiti svoje namene. Storilci poskušajo potencialne »žrtve« prepričati z apeliranjem na njihova čustva kot sta vznemirjenost ali strah oz. uporabljajo različne načine za vzpostavitev medsebojnih odnosov, preko katerih se razvije zaupanje in celo predanost (Gao in Kim, 2007 v Workman, 2008).

## 3.3 SISTEMSKI POGLEDI NA ORGANIZACIJSKO VARNOST

V organizacijah se je odnos do varnostne paradigme v zadnjih tridesetih letih precej spremenil. Od poudarjanja pretežno tehničnega vidika, se je pozornost preusmerila najprej na človeške napake in nato na varnostni management ter varnostno kulturo. Rečemo lahko, da predstavlja priznavanje vloge, ki jo imajo organizacijski dejavniki na splošno varnost, t. i. tretje obdobje varnosti, če so bile tehnične zaščite prvo in človeški dejavniki drugo obdobje (Mengoli in Debarberis, 2008).

Kronološki razvoj konceptov varnosti (glej Sliko 3.2) kaže, da so na pristop k obravnavanju varnosti v organizacijah pretežno vplivali zgodovinsko odmevni dogodki. Razsežnosti nesreč, ki smo jim priča zadnjih trideset let, so močno krojile pristope upravljanja s tveganji ter vplivale na razmah številnih raziskav in preiskav tudi samih dogodkov z namenom, da se odkrijejo vzroki in postopki sanacije oz. najdejo rešitve, kako se podobnim incidentom izogniti v prihodnje.

**Slika 3.2:** Kronološki razvoj varnostnih konceptov




Vir: Mengoli in Debarberis (2008, 244)

Poglejmo si omenjene incidente na Sliki 3.2. nekoliko pobliže. Obdobje varnosti, ki je bilo obravnavano predvsem s tehničnega vidika (delno tudi že z vidika človeškega dejavnika), sta določila incidenta Seveso in TMI. Nezgoda Seveso je poimenovana po mestu v Italiji, ki je bilo v njej najbolj prizadeto in se nanaša na dogodek znotraj kemičnega obrata ICMESA (Industrie Chimiche Meda Societa). Kemični obrat je proizvajal vmesne spojine za kozmetično in farmacevtsko industrijo, sama kemična nesreča pa je odjeknila kot posledica

nepoznavanja kemičnih procesov, junija 1976. Dogodek je vplival na sprejetje t. i. Saveso direktive v letu 1982 s strani Evropske komisije z namenom, da se zmanjša vire nevarnosti za tehnološka tveganja (Kletz 2001, 103–109). TMI (pravzaprav TMI-2, ker gre za drugi blok elektrarne) je kratica za nesrečo v jedrski elektrarni Otok treh milj-2 (TMI-2), ki se je zgodila marca 1979 v Middletonnu (Pensylvanija) v ZDA. Nesreča je bila povod za sprejetje in izvedbo ukrepov v vseh sorodnih elektrarnah po svetu, na podlagi katerih se je verjetnost podobnega dogodka bistveno zmanjšala (Hertsgaard 2004).

Obdobje, ki je sledilo pretežno tehničnemu pogledu na zagotavljanje varnosti, je krivce za nastanek nesreč iskalo zlasti v človeških napakah in pomanjkljivi varnostni kulturi. To obdobje so začrtale industrijska nesreča v indijskem mestu Bhopal, decembra 1984 (največja industrijska nesreča, ki se je kdaj koli zgodila), nesreča raketoplana Challenger (ena izmed najhujših nesreč v zgodovini vesoljskih poletov), januarja 1986, in jedrska nesreča v Černobilu, aprila 1986, kjer je Mednarodna agencija za atomsko energijo (IAEA) kot ključni dejavnik za katastrofo, izpostavila »pomanjkljivo varnostno kulturo« organizacije (IAEA 1986 v Antonsen 2009, 1). Izraz varnostna kultura se je zgodovinsko gledano tako prvič omenil v povezavi z jedrsko nesrečo v Černobilu.

Za tretje obdobje pogledov na organizacijsko varnost je značilen vse izrazitejši prehod od poudarjanja varnostne kulture do bolj celovitih organizacijskih pristopov k zagotavljanju varnosti in zavedanja vpetosti v širše družbeno okolje. Gre pravzaprav za prepletanje varnostne in organizacijske kulture, ki poleg dovršene tehnološke podpore zagotavlja dolgoročno varno poslovanje, ki smo mu priča zadnjih deset let. Tretje obdobje je opredelila najhujša jedrska nesreča po Černobilu, nesreča v japonskem mestu Tokaimura (september 1999), ki je nastala kot posledica uporabe nepreverjenih načinov obratovanja za katere so zaposleni morali vedeti, da niso primerni (jedrsko gorivo so poskušali zmešati v plastičnem vedru) (Albright, 1999). Sem prištevamo tudi nezgodo v nuklearni elektrarni Davis-Besse v zvezni državi Ohio in nesrečo raketoplana Columbia, ki sta se zgodili januarja 2003. Analize dogodkov so pokazale ne samo tehnološke pomanjkljivosti, ampak tudi slabo organizacijsko zavedanje posledic pomanjkljive varnosti. Raziskave, ki so bile opravljene v tem obdobju kažejo, da je več kot 90 odstotkov vseh incidentov posledica samega organizacijskega sistema in načina njegovega delovanja, kar pomeni, da so bili vzroki za incidente sistematično vgrajeni in sproženi s strani sistema samega ter niso nujno posledica človeških ravnanj, ki bi bila zlonamerna ali malomarna na delovnem mestu (Smith, 2009).

### 3.3.1 Taksonomija organizacijskih vzrokov za pomanjkljivo varnost

Organizacijska veda pozna kar nekaj t. i. vzorčnih modelov nesreč (ang. accident causation models), s katerimi se poskuša pojasniti delovanje in sosledje vzrokov, ki botrujejo nastanku nesreč v organizacijah. Večina jih temelji na Heinrichovi teoriji domine in predstavlja v večji meri njeno nadgradnjo, kot izvirni pristop k pojasnjevanju nesreč. Heinrichova teorija domine predpostavlja, da nesreče povzroči zaporedje dogodkov, ki vplivajo eden na drugega kot padajoče domine. S tem, ko pade prva domina, povzroči nestanovitnost druge, ta povzroči nestanovitnost tretje in tako dalje, vse dokler ne pride do vedenj, ki niso varna ali nastanka okoliščin, ki povzročijo nesrečo raznolikih razsežnosti. Heinrichove padajoče domine predstavljajo niz osebnih značilnosti delavca (celota dednih lastnosti in vplivov okolja), njegovih napak pri delu, tveganih ravnanj in/ali nevarnih okoliščin, posledičnih incidentov in končnih poškodb. V kolikor organizacija ne poskušata zaustaviti nestanovitnost posamezne domine ter zlasti domine, ki se nanaša na tvegana ravnanja (gre za najmočnejšo domino, ki prenese svojo težo na vse ostale), je pojavnost nesreče skorajda neizbežna. O tem govori tudi Pravilo 80:20, ko predpostavlja, da približno 80 odstotkov nesreč povzročijo zgolj tvegana vedenja ali ravnanja, preostalih 20 odstotkov pa je povzročenih s strani nevarnih okoliščin (Cooper, 2001, 6–7).

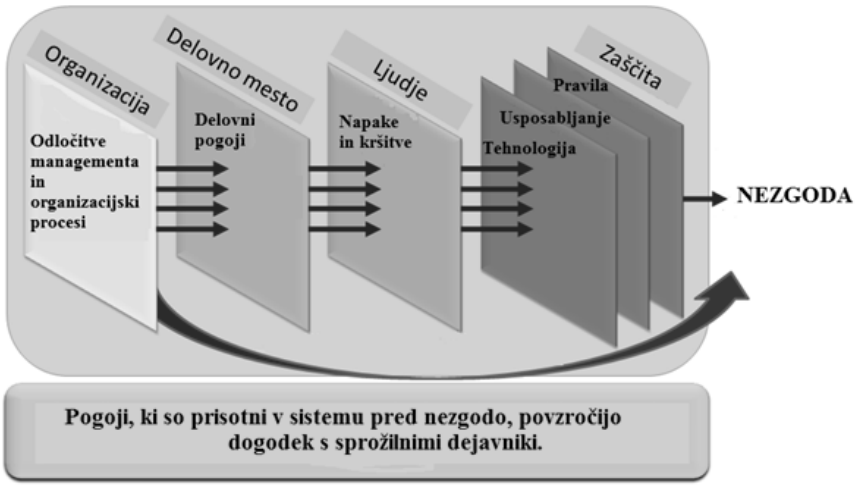
Poleg Heinrichove teorije domine, pojasnjujejo vzroke za nastanek incidentov v organizacijah še Weaverjeva, Adamsova ter Bird in Loftusova teorija domine. Weaverjev vzročni model nesreče išče odgovornost za nesrečo v slabem nadzorstvu in linijskem menedžmentu ter prepoznava povezanost med sistemi upravljanja in incidenti. Adams preusmerja pozornost od posameznika k značilnostim organizacije in prvi opozori na varnostno kulturo s tem, ko meni, da se osebnost organizacije odraža v stabilnosti organizacijskih elementov. Njegov model se od prejšnjih dveh razlikuje tudi potem, da obravnava tvegana vedenja in okoliščine (t.i. taktične napake) kot rezultat strateških napak višjega menedžmenta. Podobno kot Adamsov model opisuje vzročno zaporedje tudi model Birda in Loftusa. Model vidi vzroke v slabem nadzorstvu s strani menedžmenta, ki vpliva na razvoj šibkih osebnih faktorjev (npr. pomanjkljivost primerne usposobljenosti) ali delovnih faktorjev (npr. nenadzorovani stroji) (Cooper, 2001,7–10).

V okviru iskanja organizacijskih vzrokov ima pri nastanku nesreče izrazito pomembno vlogo »inkubacijska doba«, ki se nanaša na obdobje, ki mine od razvoja pogojev za nastanek

nesreče oziroma okužbe do dejanskega izbruha prvih vidnih simptomov ali že dejanskega nastanka nesreče. Turner (1976 v Shaluf, 2008, 115) opisuje inkubacijsko dobo kot čas v katerem se kopičijo napake, ki so posledica človeškega ravnanja. Če se le-te kopičijo dalje in jih nihče ne poskuša odpraviti, postopoma privedejo organizacijo v stanje, kjer je nastanek nesreče skorajda neizbežen. In v takšnih okoliščinah je pogosto zadosti samo majhna nepazljivost, drobna napaka, ki deluje kot zažigalna vrvica pri povzročitvi nesreče.

Kako delujejo vzroki za nastanek incidenta v okviru organizacije nazorno prikazuje Slika 3.3, kjer je prikazan model vzročne povezanosti med organizacijskimi dejavniki in dejavniki menedžmenta (t. i. sistemski dejavniki). Model je razvil britanski psiholog James Reason in je poznan pod imenom Reasonov patogeni model, pogovorno pa pod imenom Model švicarskega sira. Ploskve iz spodnje Slike 3.3 predstavljajo več skupaj zloženih rezin švicarskega sira (sira z značilnimi luknjicami). Vsaka ploskev predstavlja obrambno plast, ki je vgrajena v sistem organizacije in ščiti pred neprimernim postopanjem ali slabimi odločitvami na vseh ravneh sistema. Luknje v siru predstavljajo šibke točke sistema (njihova povezanost je grafično prikazana v obliki puščic), ki lahko ob pogoju, da se te med sabo pokrijejo, sprožijo nastanek incidenta. Model temelji na ideji, da večina nezgod in nesreč ni posledica ene same napake (npr. zgolj napake v mehanizmu ali človeškega faktorja), temveč nastanejo kot posledica več med sabo povezanih dejavnikov (International Civil Aviation Organization 2005).

**Slika 3.3:** Koncept vzrokov za incident




Vir: International Civil Aviation Organization (2009)

Reason (1990 v van Vuuren 2000, 32) tako nadaljuje Turnerjevo razpravo o organizacijskih vzrokih nesreč in jo dopolnjuje z razlikovanjem med aktivnimi in latentnimi (prikritimi) napakami ali pomanjkljivostmi. Učinki aktivnih neuspehov so vidni skoraj nemudoma, medtem ko se posledice latentnih lahko neopazno skrivajo precej časa znotraj sistema in pokažejo svoj pravi obraz šele takrat, ko se povežejo skupaj z ostalimi latentnimi in aktivnimi dejavniki nesreč.

Van Vuuren (2000) pravi, da je možno organizacijske vzroke za nastanek nesreč strniti v tri večje skupine. Na podlagi obstoječih teorij in raziskav ločuje med:

- napakami, ki so v povezavi s strukturo organizacije;
- napakami, ki so v povezavi s strategijo in cilji organizacije;
- napakami, ki so v povezavi s kulturo organizacije (glej Tabelo 3.4).

**Tabela 3.4:** Taksonomija organizacijskih vzrokov za varnostne incidente

| **Skupina** | **Podkategorije** | **Definicija** |
|---|---|---|
| **Struktura** | zahteve dela/nalog | Nanaša se na napake, ki so posledica neujemanja med sposobnostmi delavca in delovnimi zahtevami. |
| | odgovornost | Nanaša se na napake, ki so posledica izostanka ali nepravilnega dodeljevanja odgovornosti med oddelki, skupinami in ljudmi. |
| | veščine in znanje | Nanaša se na napake, ki so posledica neučinkovitih ukrepov, da bi se situacijske in specifične veščine ter znanja prenesli na nove in manj izkušene sodelavce. |
| | delovni postopki | Nanaša se na napake, ki so povezane s kvaliteto in razpoložljivostjo delovnih postopkov znotraj oddelka (preveč zapleteni, netočni, nerealistični, ne obstajajo, slabo predstavljeni). |
| | nadzorstvo | Nanaša se na napake, ki so povezane z odsotnostjo nadzora nad delom s povečano stopnjo tveganja. |
| **Strategija in cilji** | prioritete menedžmenta | Nanaša se na napake, ki so posledica odločitev menedžmenta, saj je varnost v podrejenem položaju v odnosu do zahtev ali ciljev dela. |

| | | |
|---|---|---|
| **Varnostna kultura** | norme in pravila pri delu, ki je povezano s tveganji | Nanaša se na napake, ki so povezane s pomanjkanjem jasnih ali sprejetih norm in pravil kako ravnati z nevarnostmi. |
| | varno vedenje | Nanaša se na napake, ki so povezane s splošnimi prepričanji o tveganjih in pomembnosti področja varnosti, skupaj z motivacijo delovati v skladu s temi prepričanji. |
| | refleksivnost varnostnih praks | Nanaša se na napake, ki izvirajo iz slabega na lastnih izkušnjah. |

Vir: van Vuuren (2000, 35).

Struktura se nanaša na zahteve samega dela, odgovornost, veščine in znanje, delovne postopke in nadzorstvo, ki skupaj omogočajo učinkovito delovanje organizacije. Strategije in cilji so naloga in prioriteta vodstva, njihovo prilagajanje spreminjajočemu se okolju pa garancija, ki zagotavlja dolgoročno stabilnost na trgu konkurenčnih sil. Napake, ki so v povezavi s kulturo organizacije, se nanašajo na kršitev obstoječih norm in pravil, varnega vedenja in pomanjkanje refleksije o uspešnih varnostnih praksah (van Vuuren 2000).

Uspešno poslovanje organizacij je v vse večji meri odvisno od informacij in njihove izmenjave, ki pa seveda zahteva tudi večjo pozornost za to, kako informacije zavarovati pred nepooblaščenim dostopom in nezaželenim razkritjem. Podatki Eurostata, European Commisson (2009) na primer kažejo, da je bil delež podjetij EU-27, ki so imela v letu 2008 dostop do interneta že 93-odstoten, medtem ko je 81 odstotkov vseh podjetij uporabljalo širokopasovne povezave. Visoka stopnja uporabe interneta, kot enega izmed kazalcev razvoja informacijske družbe, nakazuje, da je uporaba IKT-ja praktično nepogrešljiva na vseh področjih življenja, od zasebnega do korporacijskega in državnega. Varen pretok informacij predstavlja danes enega izmed osnovnih pogojev za stabilno in uspešno poslovanje organizacij, pri tem pa se seveda zastavlja vprašanje, kako odpravljati organizacijske vzroke, ki vplivajo na to, da je varnost v organizaciji slabša, kot bi lahko bila. Naloga se bo v nadaljevanju osredotočila na obravnavo informacijske varnostne kulture, ki postaja v naprednih IKT okoljih vse pomembnejši kazalec t. i. skrite vrednosti organizacije in poskušala odgovoriti na to, kako se v marsikaterem pogledu najučinkoviteje boriti proti sodobnih oblikam varnostnih ogrožanj, tj. informacijskim grožnjam.

# 4 INFORMACIJSKA VARNOSTNA KULTURA

Pregled publikacij s področja informacijske varnosti kaže, da se relativno malo prispevkov nanaša na obravnavo informacijsko-varnostne ozaveščenosti in usposobljenosti, na odzivnost na incidente in človeški vidik informacijske varnosti (družbeni, kulturni in etični vidiki človeških virov in organizacijskih politik) (Dlamini in drugi 2009). Kljub temu, da je zadosti že majhna napaka (npr. geslo za dostop v računalnik je shranjeno na vidnem mestu, vrata pisarne so odprta ali nezaklenjena in v njej osebni računalnik, manipulacija preko socialnega inženiringa), da napredek sodobne tehnologije popolnoma zbledi, se organizacije še vedno premalo zavedajo, da so uporabniki z nizko stopnjo varnostne osveščenosti pravzaprav ena izmed najšibkejših vrzeli v organizaciji (Shaw in drugi 2009). Za primer, Orgill in drugi (2004 v Bakhshi in drugi 2009, 54) ugotavljajo v raziskavi, da bi kar 80% zaposlenih zaupalo svoje uporabniško ime in 60% svoje geslo osebi, ki bi se pretvarjala, da prihaja z oddelka za računalniško podporo. Podatki, da sta socialni inženiring in neprevidno vedenje ljudi odgovorna za več kot polovico vseh varnostih zlorab (Mackenzie 2006, 3. odstavek), kažejo, da pravzaprav ni pomembno kako učinkovite so oblike tehnične zaščite, saj je varnost navsezadnje odvisna od primernega vedenja končnih uporabnikov (Rhee in drugi 2009). Čeprav se na zagotavljanje informacijske varnosti še vedno gleda z vidika tehničnega problema, je pomembno izpostaviti tudi socialen vidik ter poudariti, da na človeške in organizacijske vidike informacijske varnosti lahko primerno odgovori le socialno-tehničen pristop (Kraemer in drugi 2009).

Raven varnostne kulture kot dela organizacijske kulture postaja vse pomembnejši parameter t. i. skrite vrednosti organizacije in skrbi za vzpostavljanje učinkovitih mehanizmov obvladovanja in upravljanja z občutljivimi podatki. Varnostno (samo)zavedanje namreč predstavlja segment, ki si ga vodstveno osebje prizadeva doseči preko različnih pristopov zavednega in nezavednega vplivanja na zaposlene. Predpisi, varnostne politike, protokoli in standardi sami po sebi za varno vedenje še niso zadosti, saj na ravnanje z občutljivimi podatki vplivajo tudi osebne predpostavke o varnosti, ki so odraz posameznikovega zaznavanja oz. razumevanja tako varnostnih predpisov, kot tudi dejanskih groženj (Zakaria 2006).

V poglavju Informacijska varnostna kultura bom pozornost namenila socialnemu vidiku zagotavljanja varnosti v okolju, kjer je ranljivost podatkov še posebej občutljiva in

spregovorili o informacijski varnostni kulturi. Zaradi vpetosti informacijske varnostne kulture v splošno organizacijsko kulturo posamezne organizacije, bom najprej predstavila pojem organizacijske kulture in nato nadaljevala z opisom varnostne kulture. Pojem varnostne kulture bom opredelili nekoliko širše, saj je v neposredni povezavi z relativno novim pojmom informacijske varnostne kulture, o kateri se govori predvsem v okoljih, ki si prizadevajo za visoko raven informacijske varnosti.

## 4.1 ORGANIZACIJSKA KULTURA

Robbins (1998 v Treven 2001, 79) meni, da je organizacijska kultura značilni duh organizacije in skupek prepričanj njenih članov, ki se kažejo v vrednotah in normah. Te so sprejete v organizaciji glede na to, kako naj se ljudje vedejo, med seboj komunicirajo in kakšne delovne odnose naj razvijajo. Vrednote in norme delujejo na nezavedni ravni kot samoumevna prepričanja, ki pogosto niso jasno izražena, pa vendar jih zaposleni v organizaciji prevzamejo za svoja, brez da bi jih poskušali natančneje razložiti. Podobno jo definira tudi Schein (1987 v Mesner–Andolšek 1995, 21), ki pojasnjuje kulturo kot globljo raven temeljnih predpostavk in prepričanj, ki so skupne članom organizacije in delujejo na nezavedni ravni ter so temeljni samoumevni način percepcije samega sebe in svojega okolja.
Za organizacijsko kulturo je v splošnem mogoče reči, da predstavlja lepilo, ki drži organizacijo skupaj (pogosto uporabljen izraz) in povezuje menedžment (planiranje, organiziranje, vodenje in kontroliranje dela) z organizacijskim vedenjem (vpliv, ki ga imajo zaposleni in organizacijska struktura na uspešnost organizacije). Z vidika usmerjanja zaposlenih, kako naj mislijo, ravnajo in čutijo, je kultura nekakšen »operacijski sistem« organizacije (Hagberg and Heifetz 1997 v Chang in Lin 2007, 441).

Zagovorniki strateškega spreminjanja organizacijske kulture izhajajo iz štirih predpostavk. Prvič, da v organizacijah obstaja opazna kultura, ki vpliva na kakovost in uspešnost dela. Drugič, da kljub odpornosti organizacijske kulture na spremembe, obstaja določena možnost njenega oblikovanja in upravljanja[3]. Tretjič, da je možno prepoznati določene značilnosti organizacijske kulture, ki spodbujevalno ali zaviralno vplivajo na uspešnost organizacije, kar

[3] Kulturo lahko razdelimo na statično in dinamično komponento. Statičnost se nanaša na to, kar kultura je oziroma na splošne in nespreminjajoče se vrednote, ki jih goji organizacija in na prepričanja, ki označujejo njene člane. Dinamična komponenta pa je povezana s tem, kako organizacija deluje in kakšni so njeni delovni procesi (Hudson 1999).

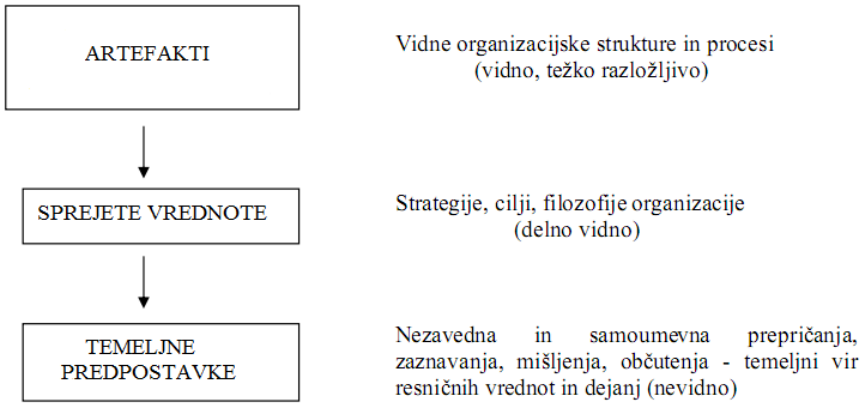
omogoča menedžerjem, da razvijajo strategije za spreminjanje kulture. In zadnja prepostavka, prednosti spremenjene kulture odtehtajo morebitne disfunkcionalne posledice (Pagon 2004).

Pogledov na to, kaj so bistveni sestavni deli organizacijske kulture, je precej. Schein (2004, 17) v klasiki organizacijskega vedenja, naslovljeni »Organisational Culture and Leadership«, ločuje med tremi ravnmi:

- vedenjski vzorci in načini ravnanja, t. i. artifakti;
- prevzeta prepričanja in vrednote in
- temeljne predpostavke (glej Sliko 4.1).

*Artefakti* so na zunaj vidni kot značilni vedenjski vzorci in otipljive lastnosti posamezne skupine ljudi, kot npr. jezik, oblikovanje delovnega okolja (npr. ali so pisarne odprtega tipa oz. ali so vrata v pisarne stalno zaprta), interni predpisi, načini oblačenja itd., ter pravzaprav predstavljajo značilnosti organizacijskega življenja, ki jih lahko vsakodnevno opazimo. Drugo raven sestavljajo *vrednote in prepričanja*, ki kot so skupek idealov in teorij lahko usmerjajo oz. ne usmerjajo organizacijsko vedenje. Pri vrednotah ločimo vrednote, ki so skladne s temeljnimi predpostavkami (to lahko pozneje prispeva k identifikaciji skupine in k občutku pripadnosti) in vrednote, ki niso skladne s temeljnimi predpostavkami. Na tej ravni je del vedenja še zmeraj nejasen in nerazumljiv. Tretja raven, *osnovne predpostavke* vključujejo najglobljo in najbolj izčrpno obrazložitev realnosti, saj zajemajo tisto, kar si člani organizacije med sabo delijo in razumejo kot samoumevno. Nanašajo se na odnos do okolja, na naravo človekovega delovanja, na medsebojne odnose, na tiste resnice, o katerih se v organizaciji ne govori na glas, jih pa goji vsak zase (Schein 2004). Pomembno je, da se predpostavke med posamezniki v organizaciji ne razlikujejo preveč, saj je, kot pravi Schein (2004), ravnovesje med prevzetimi prepričanji/vrednotami in temeljnimi predpostavkami ključnega pomena za ciljno orientiranost organizacijske skupine.

**Slika 4.1:** Ravni organizacijske kulture




Vir: Schein (2004,17)

## 4.2 VARNOSTNA KULTURA

Večina avtorjev, ki proučuje segment varnosti v organizacijah, meni, da je zagotavljanje varnosti v osnovi naloga menedžmenta in ne tehnologov, saj tehnična oprema sama ne more zagotoviti visoke varnosti. Brez korenitih sprememb varnostne kulture, ki direktno zadeva varnostne postopke in prakse v organizaciji, sami varnostni instrumenti ne bodo veliko prispevali k varnosti (von Solms in von Solms 2004 v Chang in Lin 2007, 441). V obzir je potrebno vzeti večje število kazalcev uspešnosti, ki so razporejeni na posameznih ravneh organizacije in zajemajo strukturne komponente, operativne dejavnosti, ljudi, varnostno kulturo, organizacijsko kulturo in kulturo okolja. Le-ti lahko pravočasno opozorijo nato, da ločeni procesi ne potekajo tako, kot bi morali in sprožijo ustrezen odziv (Mengoli in Debarberis 2008).

Podobno kot pri organizacijski kulturi se tudi pri poskusih opredeljevanja varnostne kulture srečamo s številnimi definicijami in razlagami. Nekateri so prepričani, da je v vsaki organizaciji prisotna tudi določena stopnja varnostne kulture, ki je lahko šibka ali močna, pozitivna oz. negativna. Medtem ko drugi menijo, da je mogoče reči le za organizacijo, ki je celovito zavezana k zagotavljanju varnosti, da ima kulturo varnosti. Če se strinjamo s slednjimi, bomo verjetno našli zelo malo organizacij z varnostno kulturo, saj si jih večina prizadeva zanjo, a kljub temu redko doseže visoko stopnjo (Hopkins 2006).

Kot sem že omenila, se pojem varnostne kulture prvič pojavi ob nesreči v Černobilu, kjer postane pomanjkljiva varnostna kultura oz. nizka raven varnostnega vedenja, glavni vzrok za nesrečo. Varnostno kulturo se lahko opredeli kot:

> *trajno vrednost in prioriteto, ki se nanaša na varnost delavcev in javnosti, s strani vsakega posameznika v vseh skupinah in na kateri koli stopnji organizacijske hierarhije. Obsega osebno odgovornost posameznikov in skupin za varnost, skrb za ohranjanje, izboljšanje in poročanje varnostnih pomislekov, prizadevanje za aktivno učenje, prilagajanje in spreminjanje vedenj (individualnih in organizacijskih), ki temeljijo na izkušnjah ter nagrajevanju na način, ki je v skladu s temi vrednotami* (Wiegmann in drugi 2002, 8).

Iz definicije je razvidno, da se varnostna kultura nanaša na dokaj splošno področje osebne predanosti in odgovornosti vseh posameznikov (Choudhry in drugi 2007), ki so vključeni v dejavnosti, ki so potencialno nevarne. Oziroma predstavlja pomemben segment pri vzpostavljanju učinkovitih mehanizmov v okoljih, kjer se zaposleni srečujejo z varovanjem in obdelovanjem zaupnih ali občutljivih podatkov (Lobnikar in drugi 2009).

Turner in drugi (1989 v Cooper 2000, 113) definirajo varnostno kulturo kot zbir prepričanj, norm, vedenj, vlog in socialnih ter tehničnih praks, ki so povezane z minimaliziranjem izpostavljenosti (zaposlenih, menedžerjev, strank in družbe) okoliščinam, ki se zdijo nevarne oz. škodljive. Tej definiciji je blizu tudi splošna opredelitev, ki jo navaja Mednarodna organizacija za civilno letalstvo v svojem priročniku iz leta 2005 (ICAO Safety Management Manual 2005, 1–2) in izvira iz predpostavke, da je varnostna kultura naravni produkt organizacijske kulture.

Varnostno kulturo opredeljujejo tri osnovne dimenzije: psihološka, situacijska in vedenjska. Situacijske vidike varnostne kulture je mogoče opaziti v strukturi organizacije, ki zajema politike, delovna pravila, sisteme upravljanja, itd. Vedenjske vidike se meri s pomočjo strokovnega opazovanja, samoporočanja in rezultatov ukrepov, medtem ko je psihološka dimenzija najpogosteje proučevana s pomočjo vprašalnikov, ki merijo posameznikovo dojemanje varnosti (Choudhry in drugi 2007).

Zhang in drugi (2002) so pri pregledu različnih definicij varnostne kulture ugotovili, da je kljub številnim poskusom opredelitve, mogoče izločiti nekaj skupnih značilnosti. Ključne značilnosti so predvsem naslednje:

- varnostna kultura je koncept, ki je definiran na ravni skupine ali višje in se nanaša na skupne vrednote celotne skupine oz. članov organizacije;
- varnostna kultura se ukvarja s formalnimi varnostnimi zadevami v organizaciji in je ozko povezana, a ne omejena, z menedžerskim in nadzorstvenim sistemom;
- varnostna kultura poudarja prispevek vsakogar na vseh ravneh organizacije;
- varnostna kultura organizacije ima vpliv na vedenje ljudi pri delu;
- varnostna kultura se navadno odraža v nepredvidljivostih med sistemom nagrajevanja in varnim postopanjem;
- varnostna kultura se odraža v organizacijski pripravljenosti, da se razvija in uči iz napak, incidentov in nezgod;
- varnostna kultura je relativno trajna, stabilna in odporna na spremembe.

### 4.2.1 Kazalci pozitivne varnostne kulture

Pozitivna varnostna kultura prispeva k učinkovitejšemu sistemu vzdrževanja varnosti in je pokazatelj pokončne in zdrave drže organizacije, torej takšne, ki se zaveda svojih slabosti, jih poskuša neprenehoma odkrivati in z njimi upravljati. Zanjo si morajo organizacije prizadevati in jo postopoma graditi. Njeni značilni kazalci so naslednji:

- višji menedžment močno poudarja varnost kot del strategije za obvladovanje tveganj (npr. minimaliziranje izgub);
- srednji menedžment in operativno osebje ima objektiven pogled na kratko in srednje ročne nevarnosti, ki so povezane z organizacijskimi aktivnostmi;
- tisti, ki so na najvišjih položajih:
  - skrbijo za vzdušje, v katerem je prostor za pozitiven odnos do kritike, komentarjev in povratnih informacij, ki prihajajo s strani nižjih ravni organizacije in so v povezavi z varnostnimi vprašanji,
  - ne uporabljajo svojega vpliva za vsiljevanje lastnih pogledov in

- izvajajo ukrepe s katerimi se poskušajo omejiti posledice ugotovljenih varnostnih pomanjkljivosti;

- višji menedžment spodbuja nekaznovalno delovno okolje. Nekatere organizacije uporabljajo termin »pravična kultura« namesto nekaznovalna, ki pa ne pomeni imunitete pred kaznovanjem;
- na vseh ravneh organizacije (vključno z notranjimi in zunanjimi identitetami) je prisotna zavest o pomembnosti komuniciranja varnostnih informacij;
- obstajajo realni in učinkoviti predpisi, ki se nanašajo na nevarnosti, varnost in potencialno škodo;
- zaposleni so dobro usposobljeni in razumejo posledice nevarnih dejanj;
- pojavnost tveganega vedenja je nizka;
- prisotnost varnostne etike, ki odvrača od tveganega vedenja (International Civil Aviation Organization 2005, 4–18).

V splošnem pa je za organizacijo z učinkovito varnostno kulturo značilno, da ima:

- varen informacijski sistem, ki zbira, analizira in razširja informacije o incidentih ali nezgodah, ki so se ali so se skoraj zgodile, kot tudi o rednih proaktivnih pregledih sistema (t. i. informativna kultura);
- razvito kulturo poročanja, kjer so ljudje pripravljeni priznati svoje napake, zmote in kršitve;
- kulturo zaupanja, kjer se ljudi spodbuja in celo nagradi, da seznanjajo ostale z informacijami, ki so povezane z varnostjo, pri čemer je ločnica med sprejemljivim in nesprejemljivih vedenjem jasna;
- razvito prilagodljivost, ki se kaže v sposobnosti preoblikovati organizacijsko strukturo v skladu z dinamičnimi zahtevami okolja (t. i. fleksibilna kultura) in
- visoko stopnjo pripravljenosti in kompetentnosti za analiziranje varnostnega sistema in izvedbo sprememb, ko je nakazana potreba (t. i. učeča se kultura) (Reason 1997 v Parker, Lawrie in Hudson 2006, 552)

### 4.2.2 Tipologija varnostne kulture

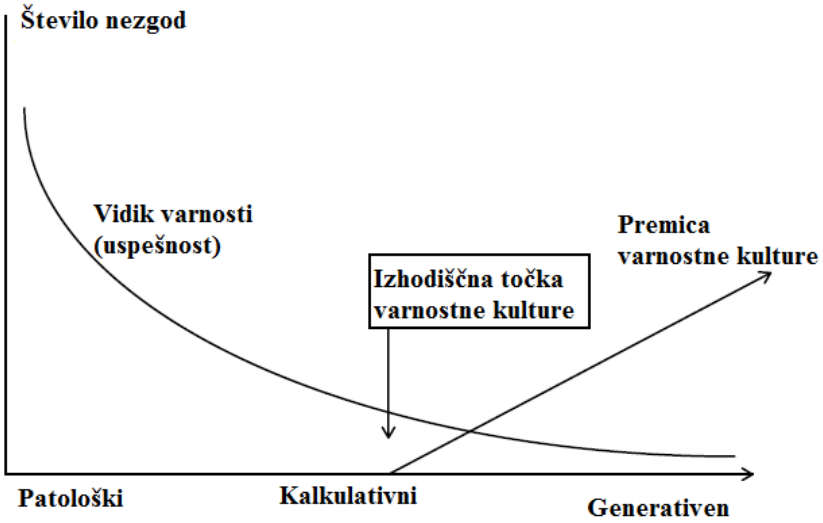
Sociolog Ron Westrum (1993, 1996, 2004 v Parker in drugi 2006, 554–55) predlaga metodo razlikovanja med organizacijskimi kulturami, ki je povezana s tem, kakšen je odnos do občutljivih informacij v organizaciji. Razvil je tipologijo kulture, kjer vsak tip kulture odseva značilnosti upravljanja z informacijami in predstavlja raven večjega napredka od prejšnjega tipa. Patološkemu, birokratičnemu (tudi kalkulativnemu) in generativnemu tipu varnostne kulture sta bila nekoliko kasneje s strani Reasona (1997 v Parker in drugi 2006, 554–555) dodana še dva tipa, in sicer reaktiven in proaktiven. Vseh pet tipov varnostne kulture oz. posameznih razvojnih stopenj, ki predstavljajo rast varnostne kulture v podjetju, lahko opišemo z naslednjimi frazami:

- patološki tip – Kdo bi skrbel za varnost, dokler nas ne ujamejo;
- reaktiven tip – Varnost je pomembna: veliko postorimo vsakokrat, ko se nam zgodi incident;
- birokratičen oz. kalkulativen tip – Imamo sisteme za upravljanje z vsemi nevarnostmi;
- proaktiven tip – Poskušamo predvideti varnostne težave, še preden se pojavijo;
- generativen tip – Zdravje, varnost in okolje so vodilo našega poslovanja (Parker in drugi 2006, 555) (glej Sliko 4.2).

Kot je razvidno iz plastičnega opisa posameznega tipa varnostne kulture, se ti razlikujejo od relativne brezbrižnosti do varnostnih vprašanj, do slepega sledenja nujnim predpisom in vse do visokega zavedanja, zakaj je pomembno upravljati z varnostjo (ko varnostno vedenje postane sestavni del vsega, kar organizacija počne).

Za organizacijo na patološki ravni je značilno, da je varnost ne zanima, in mora najprej napraviti korak v smeri zasnove vrednostnega sistema, ki bo vključeval varnost kot eno izmed najbolj potrebnih vrednot.

**Slika 4.2:** Razvoj varnostne kulture




Vir: Hudson (1999, 5)

Na naslednji, t. i. reaktivni, ravni začno pridobivati varnostna vprašanja na pomenu in pogosto jih usmerjajo notranji in zunanji dejavniki, ki so rezultat številnih incidentov. Na tej prvi fazi razvoja varnostne kulture[4] lahko opazimo počasno sprejemanje vrednot, čeprav so prepričanja, metode in delovne prakse še vedno na zelo »prvinski« ravni. Vodstvo npr. meni, da so incidenti posledica neumnosti, nepazljivosti in celo zlonamernosti s strani zaposlenih. Nasprotno, kalkulativna raven že predstavlja vsebinsko večji odmik od začetnega in precej malomarnega odnosa do varnosti, saj predpostavlja, da je zagotavljanje varnosti potrebno jemati resno. Odnos do varnosti je sicer še vedno precej preračunljiv, ker so kvalitativne ocene tveganj in cena-dobiček analize (ang. cost-benefit analyses) pogosto uporabljene z namenom, da se zadosti samemu pojmu varnosti ter izmeri učinkovitost predlaganih ukrepov. S tem, ko organizacija namerno sprejme delovne postopke lahko sama sebe prisili v resno obravnavo področja varnosti oz. se jo lahko prisili s strani pristojnih služb, čeprav vrednote še vedno niso popolnoma ponotranjene, metode še pretežno nove in individualna prepričanja v zaostanku z organizacijskimi nameni. To pomeni, da lahko o varnostni kulturi pravzaprav govorimo šele na generativni ravni, ko je vrednostni sistem, ki je povezan z varnostjo in varnim delom, popolnoma ponotranjen s prepričanji, ki so že skoraj vidna in ko vse, kar organizacija počne, stoji na temelju varnosti. To tudi pomeni, da mora biti za nastanek pozitivne varnostne kulture izpolnjen pogoj tehničnih okoliščin in postopkov, ki že delujejo, kajti drugače o njej še ne moremo govoriti (glej Sliko 4.2). Za zadnjo stopnjo razvoja je tako

[4] Čeprav o varnostni kulturi kot takšni, ki jo poznamo iz prejšnjih definicij, na tej točki praktično še ne moremo govoriti, jo pa lahko označimo za negativno.

značilno veliko bolj proaktivno zagotavljanje varnosti, kjer je t. i. ponotranjen model dobrih praks njen največji gonilnik (Hudson 1999, 8–3 do 8–6).

## 4.3 INFORMACIJSKA VARNOSTNA KULTURA

Wagner in Brooke (2007) pravita, da sta zaznavanje potencialnih groženj in prepoznavanje lastnih ranljivosti ključna za vsako uspešno organizacijo, saj so dokumenti v smeteh pogosto več vredni, kot isti dokumenti v računalniku. Vloga človeškega dejavnika postaja pri zagotavljanju varnosti vse bolj prepoznavna, poleg tega pa vsaj toliko vredna kot vloga tehnološkega dejavnika. Glede na to, da je delo zaposlenih v obdobju razvitega IKT-ja povezano z visoko stopnjo odgovornosti, integritete, zaupanja in možnostjo razmeroma lahkega dostopanja do informacij, je za organizacijo izredno pomembno, da njeni zaposleni z njo delijo enake poglede na varnost, da razumejo svoje naloge in vlogo, ki jo imajo. Znanje o tem, kakšna je vloga posameznika v organizaciji in kaj se od njega pričakuje, prispeva k zagotavljanju informacijske varnosti ter predstavlja prvo izmed dveh dimenzij človeškega dejavnika pri zagotavljanju varnosti (van Niekerk in von Solms 2006). Poleg znanja vpliva na posameznikovo varno delo z občutljivimi podatki tudi njegovo lastno vedenje. Kajti povsem mogoče je, da zaposleni razumejo svoje vloge in naloge pravilno (imajo primerno znanje), a se kljub temu ne držijo varnostnih pravil, ker ta niso v skladu z njihovimi prepričanji in vrednotami (Schlienger in Teufel 2003 v van Niekerk in von Solms 2006, 2). Zaradi tega je vzpostavitev primerne informacijsko varnostne kulture, ki združuje obe dimenziji, nujna za zagotovitev učinkovite informacijske varnosti (van Niekerk in von Solms 2006).

### 4.3.1 Definicija informacijske varnostne kulture

Informacijska varnostna kultura je v neposredni povezanosti z organizacijsko kulturo, saj slednja predstavlja prevladujočo kulturo v organizacijskem okolju, informacijska kultura pa je neke vrste njena subkultura oziroma komponenta, kar potrjujejo tudi različne raziskave (Borck 2000, Connolly 2000, Le Grand in Ozier 2000 v Da Vaiga in Eloff 2010, 197). Pojem informacijske varnostne kulture se je razvil iz pojma varnostne kulture in pravzaprav nakazuje vrsto varnostne kulture v okolju z določenimi značilnostmi. Na odnos med varnostno in informacijsko varnostno kulturo je mogoče gledati tudi z vidika dopolnitve, saj se značilnosti varnostne kulture odražajo v informacijski varnostni kulturi, le da so te nekoliko bolj

usmerjene v ustvarjanje okoliščin, ki so naklonjene varovanju občutljivih podatkov. Oz. informacijska varnostna kultura se razvije na podlagi informacijsko varnostnega vedenja (torej vedenja, ki je povezano s skrbjo za varovanje informacij) na enak način, kot se razvije organizacijska kultura na podlagi vedenja zaposlenih v organizaciji (ibid, 198).

Informacijsko varnostno kulturo se lahko opredeli kot odnos, predpostavke, prepričanja, vrednote in znanje, ki ga imajo zaposleni v odnosu do organizacijskega sistema in postopkov v vsakem delu dneva. Odnos se kaže v sprejemljivem ali nesprejemljivem vedenju (nastanek napak) v obliki artefaktov (tj. vedenjskih vzorcev in načinov ravnanja) in postopanju, ki postane način za pravilno urejanje stvari v organizaciji z namenom, da se zaščitijo informacijske vrednosti (ibid, 198).

Podobno definirata informacijsko varnostno kulturo tudi Martins in Eloff (2002 v Kuusisto in Ilvonen 2003, 433), ki jo opisujeta kot predpostavko o sprejemljivem vedenju, ki je v skladu s pravili varovanja informacij in vključuje značilnosti, kot so celovitost in razpoložljivost informacij. Po njunem mnenju jo je mogoče oceniti s pomočjo organizacijskih, skupinskih in individualnih ravni.

Načela informacijske varnostne kulture, ki usmerjajo vedenje in mišljenje ljudi lahko strnemo v devet enot. Te so sledeče:

- zavest: Uporabniki se zavedajo potrebe po varovanju informacijskih sistemov in omrežij ter se sprašujejo, kaj lahko storijo za povečanje varnosti.
- odgovornost: Vsi uporabniki so odgovorni za varnost informacijskih sistemov in omrežij.
- dovzetnost: Uporabniki ukrepajo pravočasno in kooperativno na način, da se preprečijo in odkrijejo varnostni incidenti oz. da se nanje primerno odreagira.
- etika: Udeleženci spoštujejo legitimne interese drugih.
- demokracija: Varnost informacijskih sistemov in omrežij je v skladu s ključnimi vrednotami demokratične družbe.
- ocena tveganj: Uporabniki napravijo oceno tveganj, da se ugotovijo grožnje in slabosti, določijo tudi sprejemljivo raven tveganj, preden se vzpostavi nadzor.

- varnostni načrt in implementacija: Uporabniki vključujejo element varnosti kot ključen element informacijskih sistemov in omrežij, tako v tehnične kot netehnične ukrepe in rešitve.
- upravljanje z varnostjo (varnostni menedžment): Udeleženci sprejmejo celovit pristop k upravljanju z varnostjo, vključno z varnostnimi politikami, praksami, ukrepi in postopki, ki so usklajeni in strjeni z namenom, da se ustvari skladen varnostni sistem.
- ponovna ocena: Uporabniki pregledajo in ocenijo varnost informacijskih sistemov in omrežij ter poskrbijo za ustrezne spremembe varnostne politike, praks, ukrepov in postopkov (Organizacija za gospodarsko sodelovanje in razvoj –OECD 2002, 9–12).

Kot sem omenila nekoliko nazaj, ločimo po Scheinu (2004) tri glavne sestavne dele organizacijske kulture: artefakte, sprejete vrednote in temeljne predpostavke. Enake lastnosti so značilne tudi za informacijsko varnostno kulturo, le da je pri njej potrebno dodati še eno raven značilnosti, tj. znanje. Kajti če se v okviru organizacijske kulture pričakuje, da imajo zaposleni dovolj znanja za opravljanje svojih delovnih nalog, v okviru informacijske varnostne kulture tega ni mogoče enostavno pričakovati. Zaposleni namreč lahko kljub slabemu poznavanju informacijske varnosti še vedno opravljajo svoje aktivnosti relativno uspešno. V organizaciji, ki si želi okrepiti področje varovanja informacij, je pomembno pozornost nameniti tudi ustreznemu znanju, ki bo predstavljalo predpogoj za opravljanje običajnih nalog na varen način (van Niekerk in von Solms 2006).

Sestavne dele informacijske varnostne kulture tako gradijo:

- artefakti: so tisto, kar se dejansko dogaja v organizaciji. Za opravljanje vsakodnevnih nalog na varen način morajo imeti zaposleni dovolj znanja o tem, kako opravljati svoje naloge varno.
- sprejete vrednote: da se ustvarijo dokumenti varnostne politike, mora imeti določena oseba ali skupina, ki je odgovorna za pripravo, znanje o tem, kaj se vključi v takšne politike, da bi se te lahko ustrezno odzivale na varnostne potrebe organizacije.
- temeljne predpostavke: zajemajo prepričanja in vrednote zaposlenih. Če so njihova prepričanja v nasprotju s sprejetimi vrednotami organizacije, je znanje o tem, zakaj je

določena varnostna zahteva potrebna, lahko pomembno z vidika spoštovanja predpisov (Schlienger in Teufel 2003 v van Niekerk in von Solms 2010, 478).

- znanje: vključuje nujne informacije v zvezi z zagotavljanjem varnosti (kaj, kako in zakaj) (van Niekerk in von Solms 2010, 478–479).

### 4.3.2 Konceptualni okvir informacijske varnostne kulture

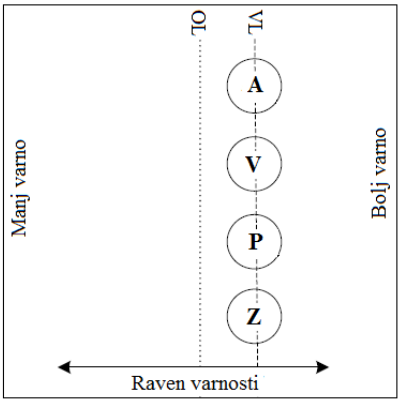
Konceptualni okvir informacijske varnostne kulture se ujema s teorijo konstruktivizma, ki razlikuje med materialno resničnostjo in družbeno realnostjo ter poudarja vrednost ljudi in njihovo občutljivost za raznovrstne vplive. Poleg tega se delno povezuje tudi z liberalistično idejo, ki se fokusira na posameznika. Konceptualno bom informacijsko varnostno kulturo prikazala s pomočjo okvirja, ki ga v svojih delih predstavljata van Niekerk in von Solms (2006, 2010). Avtorja pravita, da je celoten učinek kulture varovanja informacij mogoče razumeti kot rezultat učinkov vseh sestavnih delov ali ravni organizacije (artefaktov, vrednot, predpostavk in znanja), ki bodisi pozitivno bodisi negativno vplivajo na celotno kulturo.

Kot je razvidno iz spodnje Slike 4.3, sestavljajo osnovne elemente konceptualnega okvirja:

- OL: najmanjša sprejemljiva osnovna linija – Ta linija kaže, kaj bi bila sprejemljiva minimalna varnostna linija.
- VL: varnostna linija – Ta linija kaže dejanski vpliv kulture na splošno varnostno stanje. Mogoče jo je razumeti kot kumulativni učinek vseh štirih ravni kulture. Varnostna linija je lahko ali še bolj varna (pomaknjena desno), manj varna (pomaknjena levo) enako varna kot minimalna sprejemljiva linija (prekrivajoča).
- A: artefakti –To vozlišče predstavlja relativno moč artefaktov. Če se nahaja vozlišče levo od najmanjše sprejemljive osnovne linije, kaže na to, da izmerljivi artefakti niso tako varni, kot bi lahko bili. Vozlišče na desni pa kaže na to, da so artefakti celo bolj varni kot je njihov sprejemljiv minimum. Vozlišče, ki leži točno na sprejemljivi osnovni liniji, kaže na to, da so artefakti ravno toliko varni, ko se pričakuje od te linije.
- V: vrednote – To vozlišče predstavlja relativno moč vrednot, ki so sprejete s strani organizacije. Različne politike in postopki, ki so značilni za to raven so lahko bolj, manj ali enako obširni kot tisti, ki so določeni z minimalno sprejemljivo linijo.

- P: predpostavke – To vozlišče predstavlja relativno moč temeljnih predpostavk, ki so skupno sprejete. Vrednote in prepričanja zaposlenih so lahko ali bolj, manj ali enako naklonjeni dobrim varnostnim praksam, kot je določeno z minimalno sprejemljivo linijo.
- Z: znanje – To vozlišče kažem koliko znanja imajo zaposleni o informacijski varnosti. Zaposleni so lahko bolj izobraženi od minimalne predvidene ravni, ki je potrebna za varno delo, lahko so slabše izobraženi, ali pa imajo točno toliko znanja, kot je določeno s stopnjo znanja (van Niekerk in von Solms 2006, 6–7).

**Slika 4.3:** Osnovni elementi konceptualnega okvirja

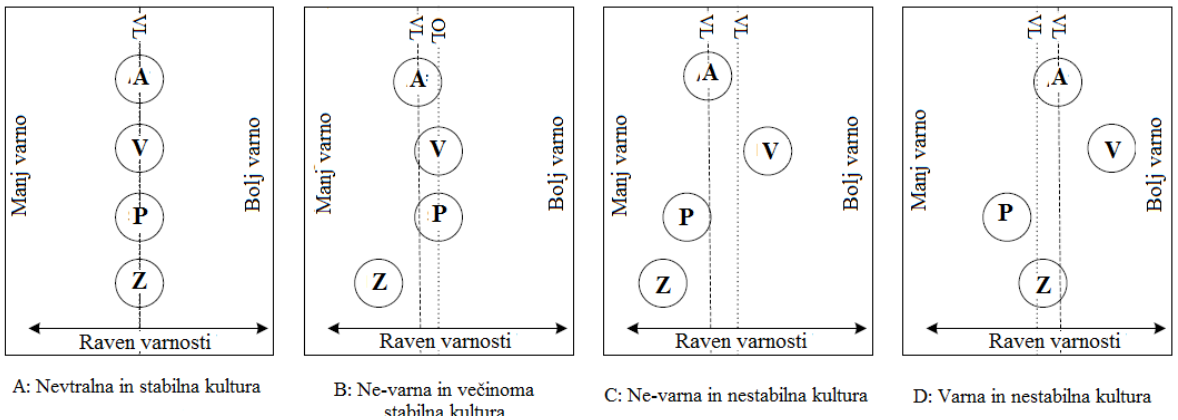



Vir: van Niekerk in von Solms (2006, 6)

Možne interakcije med različni ravnmi informacijske varnostne kulture, ki sem jih nakazala že v okviru njihovega opisa na prejšnji strani, sooblikujejo različne vrste ali tipe kultur. Ločimo med:

- nevtralno in stabilno kulturo:
- ne-varno in večinoma stabilno kulturo
- ne-varno in nestabilno kulturo
- varno in nestabilno kulturo (glej Sliko 4.4) (van Niekerk in von Solms 2006, 8).

**Slika 4.4:** Možne interakcije med različnimi ravnmi informacijske varnostne kulture




Vir: van Niekerk in von Solms (2006, 8)

### 4.3.3 Stopnje informacijske varnostne kulture

Pregled obstoječe literature kaže, da obstajajo v organizacijah različne stopnje povezanosti med organizacijsko kulturo in informacijsko varnostno kulturo. Ločimo med organizacijami 1. tipa: informacijska varnostna kultura je ločena od organizacijske kulture, 2. tipa: informacijska varnostna kultura je subkultura organizacijske kulture in 3. tipa: informacijska varnostna kultura je vključena oziroma je del organizacijske kulture (Lim in drugi 2009, 91).

Za organizacije 1. tipa je značilno, da varovanje informacij še ni sestaven del organizacijske kulture. Večina zaposlenih ni vključena ali pa ima zelo slabo vlogo pri izvajanju varnostnih pravil, kar je povezano z njihovim slabim znanjem in pomanjkanjem odgovornosti za razvijanje informacijske varnosti. Organizacija sama, na drugi strani, gleda na varnost z vidika dodatnega stroška, se izogiba investicijam in je prepričana, da je informacijska varnost izključno naloga IKT- oddelka. Nasprotno se pri organizacijah 2. tipa že kaže večja varnostna osveščenost, saj se občasna usposabljanja s tega področja izvajajo kot upoštevanje navodil menedžmenta. Zaposleni se bolje zavedajo varnostnih zahtev, kljub temu pa je medresorsko (ali med-oddelčno) usklajevanje še vedno nezadovoljivo, saj so vrednote informacijske varnosti pretežno vezane na majhno skupino ljudi (npr. finančni oddelek, kadrovski oddelek) in ne prežemajo celotne organizacije. Najbolj zaželene organizacije so seveda organizacije 3. tipa, kjer so varnostne prakse odgovornost vseh zaposlenih. Organizacija redno posodablja in prilagaja varnostno politiko ter zagovarja visoko stopnjo vključevanja v te procese. To vpliva

na oblikovanje občutka, da so informacije last zaposlenih in povečuje motivacijo za spoštovanje varnostnih predpisov (Lim in drugi 2009, 91–92).

Omenjene oblike povezanosti med organizacijsko in informacijsko varnostno kulturo se ujemajo tudi z organizacijskimi pogledi na varnost, ki jih opisuje Fitzgerald (2007 v Lim in drugi 2009, 92). Loči med organizacijami z:

- visokim poudarkom na varnosti: menedžment razpravlja o informacijski varnosti v okviru novih projektov. Vodstvo je redno obveščeno o stanju informacijske varnosti. Zaposleni se zavedajo pomembnosti informacijske varnosti in vedo, kako in koga obvestiti v primeru, da se zgodi incident. Letni proračun zajema financiranje tekočih programov varnosti. Menedžment gleda na varnost kot na možnost, ki zmanjšuje potencialna poslovna tveganja in si močno prizadeva zagotavljati varnost preko sodelovanja, financiranja in zaupanja;
- zmernim poudarkom na varnosti: zaposleni prejemajo nekaj usposabljanj o tem, kako ravnati z informacijami. Varnostne politike so oblikovane s strani IKT-oddelka, a obstaja verjetnost, da nimajo močne podpore s strani ostalih. Poleg tega zaposleni ne vedo, kje se lahko seznanijo z njimi. Določena oseba je zadolžena za izvajanje informacijske varnosti, ki je pretežno naravnano na operativne dejavnosti kot je sprememba gesla ali oblikovanje dostopa za novega zaposlenega;
- nizkim poudarkom na varnosti: politike informacijske varnosti so lahko oblikovane, a organizacija ni dosledna pri njihovem uveljavljanju. Navadno se organizacija spomni nanje le, ko že pride do incidenta. Čeprav menedžment ve, da je informacijska varnost pomembna, ji ne posveča pozornosti, ki bi bila večja od tega, da računalniki delujejo. Organizacija nima posebnega dela v proračunu, ki bi bil namenjen informacijski varnosti in je ta postavka navadno vključena v postavko za IKT-podporo (Fitzgerald 2007 v Lim in drugi 2009, 92) (glej Tabelo 4.1).

**Tabela 4.1:** Povezanost organizacijske in informacijske varnostne kulture

| Narava povezanosti | Organizacijska kultura (OK) | Informacijska varnostna kultura (IVK) | Verjetne posledice |
|---|---|---|---|
| **3. tip povezanosti:** kjer je IVK del OK (Von Solms 2000, Schlienger, T. IN Teufel 2002, Thomson in drugi 2006)<br><br>**visoki poudarek** (Fitzgerald 2007) | **Vključenost menedžmenta:** Menedžment obravnava varnostne zadeve in strategije na sestankih. Novosti je periodično predstavlja tudi nadzornemu svetu.<br>**Lokus odgovornosti:** Menedžment vključuje vse člane organizacije.<br>**Informacijsko varnostna politika:** Ustvarjena z vidika celovitosti.Obstajajo redne posodobitve.<br>**Izobraževanje/usposabljanje:** Menedžment predpisuje udeležbo na usposabljanju s področja varnostne osveščenosti za obvezno.<br>**Proračun:** Menedžment namenja del letnega proračuna za varnostno dejavnost. | **Odgovornost:** Vedno se je potrebno držati varnostnih pravil in postopkov.<br>**Udeležba:** Zaposleni periodično opravljajo varnostno usposabljanje s področja varnostne osveščenosti.<br>**Predanost:** Zaposleni razvijejo lastniški odnos in se čutijo odgovorne za informacije.<br>**Motivacija:** Motiviranost in predanost zagotavljanju varnosti.<br>**Zavedanje/vedeti kako:** Ve se, kako odreagirati v primeru incidenta in na koga se obrniti. | **Stopnja ranljivosti:** Nizka.<br>**Zavedanje:** Zaposleni se zelo zavedajo in so zaskrbljeni glede varnostnih vprašanj v organizaciji.<br>**Odgovornost:** Varnost zadeva vsakega zaposlenega.<br>**Varnostne prakse:** Celovit pristop. Nezavedno postanejo dnevna rutina.<br>**Naložbe v izvajanje varnostnih praks:** Visoki stroški za implementacijo. |
| **2. tip povezanosti:** kjer je IVK subkultura OK (Dutta in McCrohan 2002, Ramachandran in drugi 2008)<br><br>**zmerni poudarek** (Fitzgerald 2007) | **Vključenost menedžmenta:** Menedžment pripisuje odgovornost za razumevanje informacijske varnost oddelku IKT.<br>**Lokus odgovornosti:** Menedžment pooblašča vodje oddelkov za uveljanje varnostih zadev.<br>**Informacijsko varnostna politika:** Ustvarjena znotraj IKT oddelka in verjetno nima široke podpore, ljudje ne vedo, kje jo najti<br>**Izobraževanje/usposabljanje:** Menedžment začenja posvečati pozornost ozaveščenosti. Ljudje dobijo nekaj usposabljanja s področja informacijske varnosti<br>**Proračun:** Menedžment je pripravljen zagotoviti sredstva za varnostne dejavnosti. | **Odgovornost:** Varnostne zadeve se upošteva zaradi zahtev menedžmenta<br>**Udeležba:** Zaposleni so vključeni v varnostne zadeve v okviru lastnega oddelka. Manj je medresorskega usklajevanja.<br>**Predanost:** Odgovornost in predanost varnostnim stvarem v okviru lastnega oddelka.<br>**Motivacija:** Zaposleni so motivirani na področju varnosti le v okviru lastnega oddelka.<br>**Zavedanje/vedeti kako:** Ve se, kako odreagirati v primeru incidenta v lastnem oddelku in na koga se obrniti. | **Stopnja ranljivosti:** Srednja.<br>**Zavedanje:** Zaposleni se zavedajo varnostnih vprašanj znotraj lastnega oddelka.<br>**Odgovornost:** Zaposleni so odgovorni za varnostne zadeve znotraj svojega oddelka.<br>**Varnostne prakse:** Varnost je rutina posamezniku znotraj lastnega oddelka.<br>**Naložbe v izvajanje varnostnih praks:** Srednji stroški za implementacijo. |
| **3. tip povezanosti:** kjer je IVK ločena od OK (Chia in drugi 2002, Knapp in drugi 20004, Shedden in drugi 2006)<br><br>Dutta in McCrohan | **Vključenost menedžmenta:** Menedžment intuitivno ve, da je informacijska varnost pomembna, a ji pripisuje enako veliko pozornost, kot temu, da računalnik deluje.<br>**Lokus odgovornosti:** Menedžment pripisuje vso odgovornost za avrnsot IKT | **Odgovornost:** Ni skrbi in odgovornosti za varnostne zadeve<br>**Udeležba:** Zaposleni niso vključeni v varnostne zadeve.<br>**Predanost:** Zaposleni jo prepuščajo | **Stopnja ranljivosti:** Visoka.<br>**Zavedanje:** Zavedanja o varnostnih vprašanjih ni.<br>**Odgovornost:** Samo IKT oddelek je odgovoren za varnostne |

| | | | |
|---|---|---|---|
| 2002, Ramachandran in drugi 2008)<br><br>**nizek poudarek** (Fitzgerald 2007) | oddelku.<br>**Informacijsko varnostna politika:**<br>Ustvarjena brez sredstev za uresničitev. Navadno izvira iz memoranduma.<br>**Izobraževanje/usposabljanje:**<br>Nizko zavedanje. Menedžment ne poudarja potrebe po usposabljanju.<br>**Proračun:**<br>Navadno del proračuna, ki je namenjem za IKT podporo. | IKT oddelku. Vedno zaobidi varnostne postopke.<br>**Motivacija:**<br>Zaposleni niso motivirani za ukvarjanje z varnostnimi zadevami.<br>**Zavedanje/vedeti kako:**<br>Ne ve se, kako ukrepati v primeru varnostnega problema. | zadeve.<br>**Varnostne prakse:**<br>Niso dnevna rutina zaposlenih.<br>**Naložbe v izvajanje varnostnih praks:**<br>Nizki stroški za implementacijo. |

Vir: Lim in drugi (2009, 93)

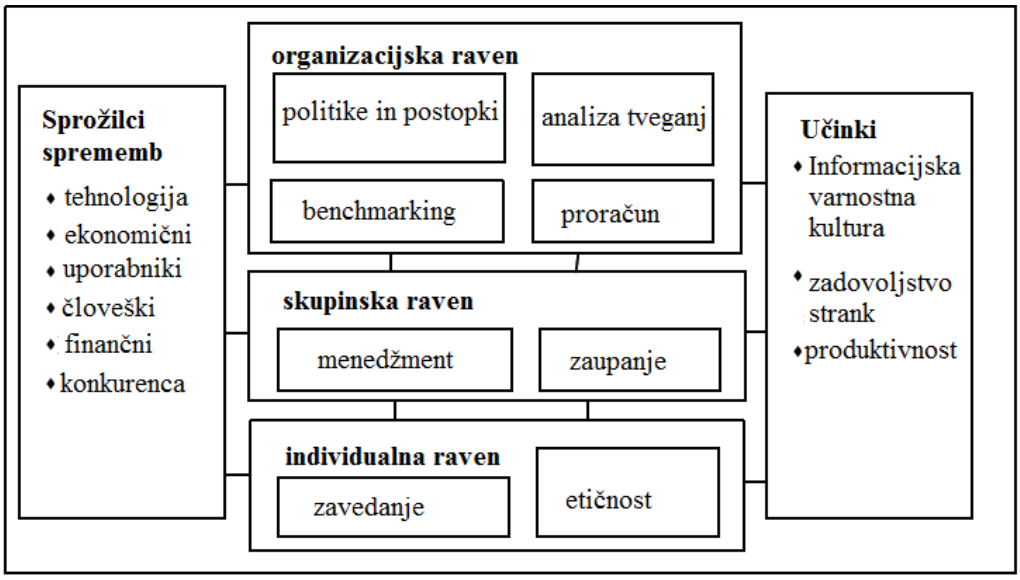
Ko govorimo o različnih stopnjah informacijske varnostne kulture v organizacijah, je potrebno omeniti tudi t. i. valove razvoja informacijske varnosti. Kot pravi von Solms (2000 v Kuusisto in Ilvonen 2003, 432–433) je prvi val informacijske varnosti, ki je trajal približno do začetka 80. let, zaobjel tehnični vidik varnosti in obravnaval varovanje informacij z vidika zmogljivosti IKT-ja (npr. preverjanje pristnosti, storitve nadzora dostopa). Drugi val, t. i. menedžerski val, se je pojavil z začetkom vključevanja organizacij v mrežne aktivnosti, torej s prihodom interneta v zgodnjih 80. letih in zajema pripravo varnostnih politik, postopkov, metod in varnostnega osebja. Tretji val, t. i. institucializacijski pa gradi na informacijski varnosti kulturi na takšen način, da postane informacijska varnost normalen element vsakodnevnih dejavnosti in o njem govorimo v obdobju od zadnjih let 90. let do danes.

### 4.3.4 Ključni indikatorji pozitivne informacijske varnostne kulture

Za ohranjanje sprejemljive ravni informacijske varnosti mora organizacija del svoje pozornosti nameniti tudi implementaciji obširnih in ustreznih indikatorjev, ki so v pomoč pri iskanju odgovorov na številne grožnje, ki ogrožajo varnost posameznikov, delovnih procesov in tehničnih pripomočkov. Indikatorji se odražajo na ravni posameznikov, skupin in celotne organizacije. Individualna raven se nanaša na značilnosti, ki vplivajo na posameznikovo vedenje na delu in vključujejo demografske podatke kot sta starost in stan, osebnostne značilnosti, emocionalne značilnosti, vrednote, prepričanja in osnovne predpostavke (Robbins 2001 v Da Veiga in Eloff 2010, 201). Skupinska raven se povezuje z vedenjem ljudi v skupinah in raziskuje vpliv skupin (skupinsko mišljenje) na vedenje posameznikov. Organizacijska raven pa vpliva na vedenje posameznikov zlasti preko različnih varnostnih politik in pravil (Da Veiga in Eloff 2010, 201).

Na Sliki 4.5 so predstavljene tri ravni organizacijskega vedenja izmed katerih je vsaka raven podlaga drugi. Na ravneh se nahajajo določene postavke, ki morajo biti ustrezno izpolnjene, da lahko spodbujajo krepitev kulture z visoko stopnjo naklonjenosti k udejanjanju informacijske varnosti. Te postavke bodo v nadaljevanju poimenovane indikatorji informacijske varnostne kulture.

**Slika 4.5:** Model informacijske varnostne kulture




Vir: Martins in Eloff (2001, 5)

Nepredvidljiv razvoj IKT-ja pospešuje potrebo po proaktivnemu prilagajanju informacijske varnosti na spremembe, ki jih s sabo prinašajo tehnološke novosti, tekmovalnost med organizacijami, razvoj ekonomije, posledice človeškega dejavnika, pričakovanja uporabnikov (strank) in finančni vložki. T. i. sprožilci sprememb so v okviru proučevanja informacijske varnostne kulture izredno pomemben dejavnik, saj vplivajo na dogajanje znotraj organizacije in se odražajo na spremembah na organizacijski, skupinski in individualni ravni (Martins 2002).

### *4.3.4.1 Organizacijska raven*

Organizacijska raven predstavlja krovno raven v organizaciji, saj kot dežnik zaobjema vse, kar se dogaja na skupinski in individualni ravni. Preko oblikovanja in izvajanja politik in postopkov daje organizaciji značilno strukturo ter vpliva na oblikovanje delovnih procesov in

uporabo tehnologije (Martins 2002). Na organizacijski ravni so pomembni naslednji štirje indikatorji:

- politike in postopki: usmerjajo vedenje ljudi in določajo, kaj se pričakuje od njih. Preko njih se kaže tudi naklonjenost menedžmenta informacijski varnosti, saj ta težko pričakuje, da bodo zaposleni opravljali naloge na določen način, če nimajo na voljo ustreznih sredstev in navodil. Varnostni dokumenti morajo biti pripravljeni na podlagi specifičnih potreb in ciljev organizacije ter morajo obravnavati postavke, ki jih zahteva informacijska varnost;
- benchmarking ali zgledovalno primerjanje: je pomembno z vidika primerjave organizacije z drugimi podobnimi organizacijami in mednarodnimi standardi. Poleg tega prinaša tudi usmeritve, kako primerno ravnati z informacijsko lastnino in jo ob enem varovati pred nevarnostmi. Organizacije lahko npr. napravijo zgledovalno primerjanje s pomočjo standardov družine ISO, ki predstavljajo referenčni dokument z vsemi nadzornimi mehanizmi, ki so potrebni v večini situacij ne glede na velikost organizacije;
- analiza tveganj: služi identifikaciji pomanjkljivosti v organizacijskem sistemu in grožnjam, ki lahko izkoristijo te pomanjkljivosti. V okviru IKT-okolja obstajajo številne priložnosti za računalniški kriminal in zaradi tega je potrebno, da se analizirajo grožnje, ki ogrožajo varnost informacij in posledično implementirajo primerni kontrolni mehanizmi oz. ukrepi;
- proračun: predstavlja del sredstev organizacije, ki so namenjena za zagotavljanje varovanja informacij. Redno načrtovanje stroškov za potrebe informacijske varnosti postane s sčasoma sprejemljivo in ne predstavlja več dodatnega stroška, temveč investicijo oziroma obogatitev organizacije. Poraba sredstev v namene višje informacijske varnosti je tako lahko potencialni generator prihodkov (Martins 2002, 74–80);

#### *4.3.4.2 Skupinska raven*

Na skupinski ravni igra izrazito vlogo menedžment, ki daje pomen varnostnim politikam s predanostjo in rednim vključevanjem v njihove izboljšave. Menedžment ustvarja s

podpiranjem in upoštevanjem varnostnih predpisov okolje v katerem igra zaupanje pomembno vlogo. Na skupinski ravni je pomembna vloga dveh indikatorjev:

- menedžment: menedžment igra ključno vlogo pri procesu udejanjanja informacijske varnosti, saj je odgovoren prepoznati varnostna tveganja in zagotoviti primerne zaščitne ukrepe. Poleg tega se njegova odgovornost povezuje tudi z vsakodnevno predanostjo, usmerjanjem in podporo pri implementaciji informacijske varnosti;
- zaupanje: izvajanje varnostnih predpisov in spreminjanje vedenja zaposlenih v skladu z načeli informacijske varnosti je lažje, če menedžment zaupa svojim zaposlenim in ti zaupajo svojim nadrejenim (Martins 2002, 82–86).

#### *4.3.4.3 Individualna raven*

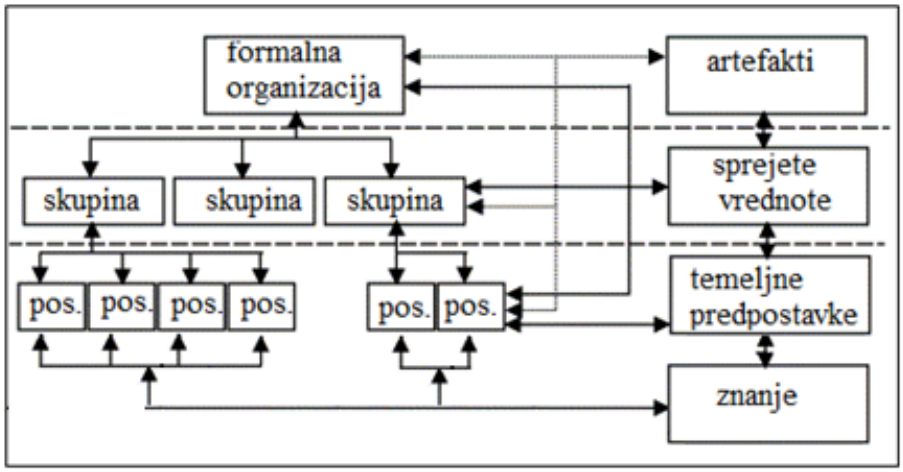
Vsak izmed posameznikov v organizaciji ima svoja prepričanja, ki se odražajo v njegovem vedenju. Ustrezno vedenje je povezano s poznavanjem procesov, ki so definirani na organizacijski ravni, in vpliva na uspešno realizacijo postavk na organizacijski in skupinski ravni. Kajti če se posameznike ne usmerja in opozarja na stvari, se ti ne morejo vesti v skladu s pričakovanji vodstva. Na individualni ravni so pomembni naslednji indikatorji:

- zavedanje: pomeni pritegniti pozornost ljudi, zakaj je področje informacijske varnosti pomembno in poteka preko usposabljanja in izobraževanja na takšen način, da pričakovano vedenje vpliva na gradnjo kulture. V organizaciji, kjer posamezniki ne razumejo in se težko vedejo na način, da ne bi povzročali groženj varnosti, je informacijska varnostna kultura še toliko bolj potrebna;
- etičnost: se povezuje z odnosom do intelektualne lastnine, na katero je potrebno gledati kot na premoženje organizacije in se jo lahko uporablja preudarno ter le v skladu z obstoječimi predpisi. Zaposleni morajo takšen odnos spoštovati in ocenjevati svoje delo kot prispevek k rasti organizacijske intelektualne lastnine. Seveda pa mora tudi organizacija spoštovati pravico zaposlenih do zasebnosti (Martins 2002, 88–93).

Za nekoliko nazornejšo predstavo, kako se omenjene ravni prepletajo in tvorijo informacijsko varnostno kulturo, dodajam Sliko 4.6. Kot je razvidno iz omenjene slike je potrebno pri

obravnavanju kulture v organizaciji, ki je podvržena IKT-ju pristopiti z različnih zornih kotov oziroma pozornost usmeriti na različne nivoje. Ker so ti nivoji, ki značilno gradijo informacijsko varnostno kulturo med sabo dvosmerno povezani, je z vidika upravljanja s kulturo za začetek že dovolj, da se pripravijo ukrepi za izboljšanje stanja na enem nivoju. Zatem pa seveda sledi obravnava drugih nivojev. Npr., proces proučevanja se lahko prične z analiziranjem skupine tako, da se obravnava vsakega izmed kulturnih vplivov posebej. Na skupino namreč vplivajo organizacijski artefakti in tudi skupina vpliva na spreminjanje artefaktov. Podobno tudi sprejete vrednote vplivajo na vedenje skupin, skupine pa dalje vplivajo na vrednostni sistem organizacije. Splošne predpostavke pa prispevajo h gradnji osebnosti posameznika, posamezniki pa neposredno vplivajo na skupino, ki jo sestavljajo.

**Slika 4.6:** Povezanost informacijsko varnostne kulture




Vir: prirejeno po Vroom in von Solms (2004, 197) (dodana je komponenta znanje)

# 5 UPRAVLJANJE INFORMACIJSKE VARNOSTNE KULTURE

Kako se ljudje v organizacijah vedejo, na kakšen način se odzivajo na dogodke in incidente ter kaj se jim zdi pomembno, je odvisno od vpliva treh dejavnikov. Te dejavnike, ki so med sabo dinamično povezani (moč vsakega je povezana z močjo ostalih dveh) in skupaj tvorijo okvir v katerem se oblikuje vedenje, predstavljajo struktura, procesi in kultura[5] (Guldenmund 2007). V nalogi posvečam pozornost dejavniku kulture v organizaciji, ki je izrazito odvisna od IKT infrastrukture. Pojasnila sem razloge, zakaj je področje informacijske varnostne kulture pomembno, nadaljevala s podrobno opredelitvijo pojma, sedaj pa bom nekoliko več prostora namenila odgovoru na vprašanje, zakaj in kako upravljati informacijsko varnostno kulturo.

Raziskave kažejo, da so netehnični vidiki prav tako pomembni kot tehnični vidiki pri varovanju občutljivih ali zaupnih informacij v organizaciji (Dhillon in Torkzadeh 2006, Siponen in Oinas-Kukkonen 2007 v Alfawaz in drugi 2010, 2) oz., da informacijske varnosti ni mogoče doseči le z uporabo tehničnih sredstev in je treba pozornost nameniti tudi ljudem in procesom v organizaciji (Herath in Rao 2009, 154). Kajti še tako izpopolnjena tehnična zaščita ne pomaga, če pozabimo zapreti vrata svoje pisarne in omogočimo prost dostop nezaželeni osebi.

Ob številnih ukrepih in trudu organizacij so zaposleni še vedno tisti, ki zaradi svoje nepazljivosti, prenizke osveščenosti in znanja, povzročajo največ varnostnih incidentov in posledično velike finančne izgube podjetjem. Workman in drugi (2008) ugotavljajo, da kljub številnim ukrepom, kako izboljšati varnostno vedenje ljudi, le ti v praksi niso prinesli pričakovanih uspehov. Analiza obstoječih raziskav, ki so jo opravili, kaže, da so le-te predlagale že celo kopico različnih ukrepov, od kaznovanja, navodil o delovni etiki, višanju varnostne osveščenosti, večanja števila varnostnih postopkov, obravnavanja konkretnih

[5] Organizacijska struktura prikazuje podobo organizacije in porazdelitev centrov moči in odgovornosti (horizontalno in vertikalno razlikovanje) ter mehanizme komunikacije, koordinacije in nadzora (npr. število kontrolorjev dela in njihovo delovno mesto). Kultura zajema osnovne predpostavke, ki oblikujejo prepričanja (npr. »Potrebujemo veliko kontrolorjev dela, ker moramo stalno nadzorovati zaposlene.«). Procesi pa so vsi osnovni in podporni procesi, ki potekajo v celotni organizaciji (npr. proces nadzorovanja, ki stremi k večji predanosti in manjšim napakam pri delu) (Guldenmund 2007, 737).

situacijskih dejavnikov, izboljšanja kvalitete obstoječih politik, izboljšanja povezanosti med organizacijskimi cilji in praksami do izboljšav s strani razvijalcev programske opreme. A vendar se zdi, da teorija vse premalokrat prehaja tudi v prakso. Zaradi tega je vprašanje, kako zmanjšati občutno razliko med osveščenostjo oz. poznavanjem informacijskih groženj in dejanskim ukrepanjem ali spremembo vedenja, vse pogostejša tema razprav o informacijski varnosti. Raziskovalci namreč opažajo, da čeprav se je razumevanje varnostnega vedenja v zadnjih letih izboljšalo, obstaja »vem kako, a ne delam tako« eden izmed temeljnih raziskovalnih in praktičnih vprašanj, ki še niso bili v celoti obravnavani (Workman in drugi (2008, 2800).

Raziskave kažejo, da je kljub razumevanju pomena varnostih groženj in zavedanju, da je potrebno tveganja resno obravnavati, med zaposlenimi pogosto premalo prepoznavanja lastne vloge pri varovanju informacij in prispevanju k varni drži organizacije (SecureInfo Corporation 2007). Na področju varovanja različnih vrst tajnosti se celo dogaja, da zaposleni dejansko predstavljajo večje tveganje, kot pa grožnje izven sistema organizacije (Federal Bureau of Investigation, 2007 v Lobnikar in drugi 2008, 50). Podobno kažejo tudi rezultati raziskave, ki je v vzorec zajela 443 ameriških strokovnjakov s področja informacijske varnosti, saj kar 25 odstotkov vprašanih meni, da je več kot 60 odstotkov finančnih izgub posledica dejanj zaposlenih, ki pa v osnovi niso zlonamerna. Večina vprašanih je tudi menja, da so usposabljanja s področja varnostne ozaveščenosti nezadostna, medtem ko navajajo, da so naložbe v ostala področja zadostne (Computer Security Institute, 2009).

## 5.1 KAKO UPRAVLJATI INFORMACIJSKO VARNOSTNO KULTURO

Informacijska varnostna kultura se nenehno spreminja zaradi številnih dejavnikov, ki vplivajo na njo. To pomeni, da je v organizaciji ni mogoče preprosto ustvariti ter nato pozabiti nanjo. Tako kot splošna organizacijska kultura zahteva konstantno upravljanje oz. vplivanje nanjo, da se ohrani želena stopnja. Zaradi tega lahko proces upravljanja z informacijsko varnostno kulturo poimenujemo tudi kot proces, ki nima konca oz. kot neprekinjen krog analiz in posledičnih sprememb (Schlienger in Teufel 2005). Načela pri obvladovanju tveganj pravijo, da je potrebno razpršiti odgovornost za njeno upravljanje, in sicer tako, da skrb za upravljanje ne zadeva le vodstvenih kadrov, temveč postane naloga vseh zaposlenih v organizaciji,

element vsakodnevnih aktivnosti in praks, tudi tistih, ki se zdijo nepovezane z varnostjo, ter je posledica učenja in prioritetnega položaja, ki ga ima področje varnosti (Chevreau 2006).

Struktura, procesi in ljudje oziroma kultura, ki jo ti ustvarjajo, predstavljajo pomembno postat za varno delovanje IKT-ja oz. poslovanje organizacij nasploh, česar pa se strokovnjaki pogosto premalo zavedajo. Najučinkovitejši pristop k zmanjševanju potencialnih nesreč tako ni povezan z brezhibno delujočo tehnično opremo, ampak z usmerjanjem pozornosti na socialne in organizacijske dejavnike v organizaciji (Fleming in Lardner, 1999).

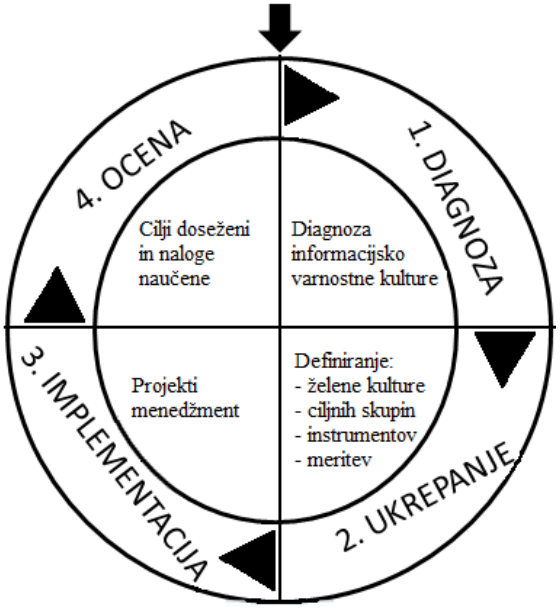
Kot je razvidno iz Slike 5.1, zajema proces upravljanja po Schliengerju in Teufelu (2005, 66–69)[6] štiri različne faze:

- analiza trenutnega stanja ali diagnoza; prikaže dejansko stanje kulture in njene pomanjkljivosti. Najpogosteje vključuje kombinacijo različnih merskih pripomočkov in metod, pogosto je narejena analiza specifičnih dokumentov, anketiranje zaposlenih, intervjuvanje ali anketiranje oseb, ki neposredno skrbijo za varnost, npr. varnostnikov ter metoda opazovanja.
- planiranje ukrepov; je odvisno od rezultatov analize, saj so za ohranjanje določene stopnje kulture potrebni milejši ukrepi kot pri spreminjanju slabe ali nizke kulture. Pri pripravi ukrepov je potrebno upoštevati obstoječe varnostne politike in predpise, ki predstavljajo definicijo kulture. Poleg tega je v pomoč pri določitvi pravilnih ukrepov tudi jasna odločitev o tem, na koga želimo vplivati. Pogosto uporabljen pristop zajema tri ključne skupine ljudi, tj. osebje, ki se ukvarja z IKT-jem, vodstvo in ostale zaposlene ali podporno osebje. Sprejeti ukrepi so različni, vključujejo pa določanje odgovornosti, interno komunikacijo (programe osveščanja), usposabljanje, izobraževanje in poudarek na zglednem vedenju menedžerjev.
- implementacija ali realizacija izbranih ukrepov; vključuje podrobno določitev aktivnosti, odgovornosti, časovno premico in finančna sredstva.
- ocenjevanje: poda dragocene podatke o učinkovitosti uporabljenih ukrepov in morebitnih izboljšavah v prihodnosti. Poleg tega se v tej fazi predvidijo tudi nadaljnji ukrepi, ki vplivajo na planiranje letnih finančnih sredstev in organizacijsko učenje. Zaposleni namreč vidijo, da je bila uvedba ukrepov mišljena resno ter da se njihovi

[6] Proces upravljanja s kulturo sta avtorja večkrat preverila, tudi s pomočjo delovne skupine predstavnikov Information Security Society Switzerland, ki je bila poimenovana »Informacijska varnostna kultura«.

učinki ocenjujejo preko vedenja ljudi, kar posledično prinese tudi hitrejše prilagajanje vedenja.

**Slika 5.1:** Proces upravljanja z informacijsko varnostno kulturo




Vir: Schlienger in Teufel (2005, 67).

### 5.1.1 Vloga vodstvenih struktur

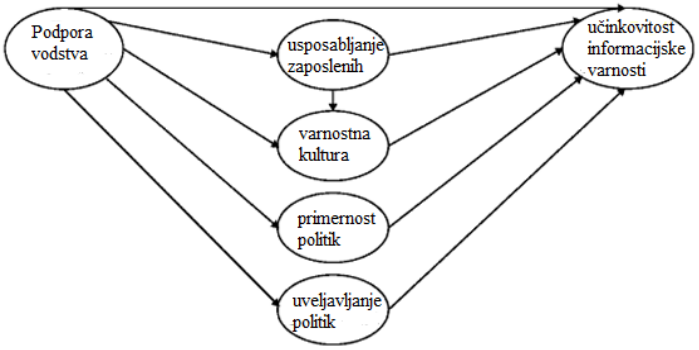
Čeprav magistrska naloga zagovarja stališče, da je skrb za visoko stopnjo informacijske varnostne kulture, naloga celotne organizacije (tako strokovnjakov, ki se neposredno ukvarjajo z IKT-jem, kot vodstva in t. i. »end users« oz. ostalih zaposlenih v organizaciji), se mi zdi potrebno posebej izpostaviti vlogo vodstva oz. menedžmenta in jo nadgraditi s priporočili, kako lahko prispeva k spreminjanju varnostnega vedenja ljudi. Vodstvo je namreč v prvi vrsti odgovorno za delovanje organizacije in zaradi ogromnih zneskov, ki jih lahko povzroči že dokaj nedolžno razkritje zaupnih podatkov, tudi prvo zainteresirano (ali bi vsaj moralo biti) za vlaganje časa, sredstev in dobre volje v izgradnjo informacijske varnosti. Zaradi tega področje informacijske varnosti najprej zadeva vodstveni nivo oz. je v splošnem problem vodstvenih struktur (vodstva in menedžmenta), informacijska varnostna kultura pa je le odsev tega, kako dobro se upravlja s področjem varnosti (Ruighaver, Maynard in Chan 2007). Knapp in drugi (2006 v Ruighaver, Maynard in Chan 2007, 61) celo ugotavljajo, da je podpora najvišjega menedžmenta bistven napovedovalec tako stopnje organizacijske

varnostne kulture, kot tudi stopnje do katere se sprejete varnostne politike še dejansko uresničujejo.

Vloga vodstvenih struktur je pomembna tudi zaradi tega, ker je nemalokrat zanemarjena ali celo podcenjena pri vplivu na varnostno kulturo organizacije. Čeprav je razvoj IKT-ja že sam po sebi prinesel določene spremembe, ki učinkujejo na večje zavedanje ranljivosti informacijsko komunikacijskih sistemov in k osveščenosti močno prispevajo tudi svetovni mediji, raziskave ocenjujejo, da je prispevek vodstva k višji stopnji varnosti še vedno nezadosten. Npr. 874 sodelujočih strokovnjakov s področja informacijske varnosti je v spletni raziskavi iz leta 2004, na prvo mesto izmed 25 najbolj perečih varnostnih vprašanjih s katerimi se srečujejo sodobne organizacije, postavilo prav pomanjkljivo podporo vodstva. Na drugo mesto so uvrstili programe usposabljanj in izobraževanj za osveščanje uporabnikov, na sedmo pa organizacijsko kulturo (Knapp in Marshall 2007).

Vodstvo ima pomembno vlogo pri vplivanju na upravljanje z varnostno kulturo. Seveda pa je potrebno pri tem poudariti, kateri so tisti segmenti organizacijskega življenja, ki so še posebej dojemljivi za vplive s strani vodstva oz. odgovoriti, na kaj se mora vodstvo osredotočiti, če želi izboljšati področje varnosti v organizaciji. Kot je razvidno iz diagrama spodaj (Slika 5.2), vodstvo neposredno vpliva na učinkovitost informacijske varnosti, a samo njegov vpliv ne zadostuje. Avtorja diagrama, Knapp in Marshall (2007), poudarjata, da se dejavnik podpore vodstva povezuje še s štirimi drugimi dejavniki in sicer z dejavnikom usposabljanja zaposlenih, varnostne kulture, primernih politik in dejavnikom udejanjanja teh politik. Osredotočenost na ta področja prinaša največ možnosti za spreminjanje obstoječega stanja.

**Slika 5.2:** Konceptualna povezanost med podporo vodstva in ostalih dejavnikov na učinkovitost informacijske varnosti




Vir: Knapp in Marshall (2007, 54)

Model tako nakazuje, da si je potrebno zastaviti zgolj eno vprašanje, da lahko v splošnem ocenimo »zdravje« organizacije z vidika z varnosti, in sicer, ali vodstvo vidno in aktivno podpira aktivnosti, ki so v povezavi z informacijsko varnostjo oz. s programi, ki so namenjeni njeni krepitvi. Odgovor na vprašanje je namreč močen pokazatelj in napovedovalec varnostnega stanja oz. učinkovitosti zastavljenih programov. In če je odgovor pritrdilen, potem obstaja velika verjetnost, da je organizacija na dobri poti za dosego zastavljenih ciljev. V primeru negativnega odgovora, pa je verjetnost za dosego želenih ciljev sorazmerno manjša. Podpora vodstva je tako v vsaki organizaciji ključna in bistvena za udejanjanje sprememb. Posamezniki bodo sami in brez nje le težko kaj spremenili na bolje oz. bo njihov trud v primerjavi s končnim uspehom nesorazmerno večji (Knapp in Marshall 2007).

### 5.1.2 Priporočila za izboljšanje varnostnega vedenja ljudi

Kot je bilo predstavljeno, učinkovitost informacijske varnosti ni odvisna le od enega, temveč od večjega števila dejavnikov. Kljub temu da so bili vsi omenjeni dejavniki že opisani, bom posebej izpostavila dejavnik, ki ima pomemben delež pri izboljšanju varnostnega vedenja ljudi in vpliva tudi na izgradnjo informacijske varnostne kulture. Čeprav se na usposabljanje pogosto gleda z vidika dodatnega stroška za organizacijo, je investicija v strokovno usmerjanje varnostnega vedenja ljudi, pravzaprav njena dolgoročna prihodnost. Ne glede na to, kako podrobne in natančne so sprejete politike in predpisi, življenje je preveč dinamično, da bi bilo mogoče predvideti vse situacije, ki bodo zahtevale hitro in ustrezno ukrepanje zaposlenih. Poleg tega vodstvo ni sposobno nadzirati vseh delovnih procesov in mora marsikatero odločitev, ki vključuje tudi varnostne dimenzije, prepustiti ostalim zaposlenim.

V nadaljevanju bodo v dveh skupinah predstavljeni dejavniki, ki imajo močan vpliv na varnostno vedenje ljudi, izpostavljeni pa bodo tisti trije, preko katerih lahko organizacija najbolj vpliva na svoje zaposlene.

Prva skupina vključuje dejavnike, ki predstavljajo posameznikovo razumevanje tega, kar organizacija pričakuje od njih, in zajema tisto, kar:

- je posameznikom povedano: sem spadajo vsi t. i. varnostni dokumenti, ki predstavljajo znanje organizacije in so učinkoviti glede na to, kako enostavno se jih

pridobi, kako dovršeni in jasno so ter kako enotne so varnostne vrednote, ki jih sporočajo;

- kar posamezniki vidijo, da počnejo drugi; vedenje drugih, ki ga posamezniki opazujejo okoli sebe, ima nanje močnejši vpliv, kot sama navodila o tem, kako se morajo vesti. Pri tem so posebej izrazite vrednote in odnos do varnosti, ki ga ima vodstvo, konsistentnost med zapisanimi vrednotami in tistimi, ki so vidne iz opazovanega vedenja ter zrcaljenje varnostnih vrednot v vseh organizacijskih dejavnostih;
- se posamezniki naučijo iz svojih preteklih izkušenj: ker je večina varnostnih odločitev, ki jih sprejmejo posamezniki, sprejeta v nekritičnih situacijah in v okviru normalnih okoliščin, so osebne izkušnje bogata zakladnica znanja za učenje kako pravilno ukrepati oz. se vesti (Leach 2003, 586–687).

Druga skupina vključuje dejavnike, ki vplivajo na posameznikovo osebno pripravljenost za upoštevanje predpisanih norm in pravil ter zajemajo:

- osebne vrednote in načine vedenja: večina posameznikov verjame v pomembnost skupnih vrednost in navadno hitro prevzema organizacijski sistem vrednot, saj jim je lažje delati v skladu z dogovornimi pravili kot brez njih. Težje je seveda v primeru, ko se vrednote posameznikov razlikujejo od tistih, ki jih goji organizacija;
- občutek odgovornosti do delodajalca: je posledica psihološkega pritiska, ki ga čutijo posamezniki in zajema prostovoljno upoštevanje pričakovanj organizacije; lahko se ga opiše s pojmom psihološke pogodbe.
- težave, s katerimi se srečujejo pri upoštevanju predpisanih postopkov: v primeru nerazumljivih ali težko izvedljivih varnostnih mehanizmov, kjer njihovo upoštevanje nima vidnih učinkov, imajo zaposleni izredno nizko stopnjo tolerance za vedenje v skladu z njimi (Leach 2003, 588–689).

Leich (2003) pravi, da ima organizacija največ pristojnosti in potenciala za spremembe, ki se nanašajo na vedenje vodstva in ostalih zaposlenih (2. dejavnik 1. skupine), na uporabo znanja, ki izvira iz preteklih izkušenj (3. dejavnik 1. skupine) in na moč psihološke pogodbe (2. dejavnik 2. skupine). Spremembe je mogoče doseči preko procesa povratne komunikacije, kjer zaposleni opozarjajo na pomanjkljivosti v sistemu, preko opozarjanja na napake in

skupnega iskanja boljših rešitev do nagrajevanja dobrih odločitev. Za spodbujanje psihološke pogodbe pa je dobrodošlo vpletanje varnostnih tem v vsakodnevne pogovore in sestanke, ki morajo biti vidno, da postane varnost normalna tema pogovorov.

Odgovor na vprašanje, kako upravljati z organizacijskimi značilnostmi, da postane komponenta varnosti del prepričanj, dejanj in vedenj zaposlenih in kaj je tisto, kar je potrebno dodati številnim predpisom, paleti postopkov evidentiranja in odpravljanja napak, vključno s pravili sankcioniranja kršitev in nenehnega usposabljanja, da bo stopnja informacijske varnosti večja, ni preprost. Zagotovo pa ga lahko iščemo v smeri ponotranjenega zavedanja, kako potrebno je varno vedenje v okviru določene dejavnosti, ki jo posameznik opravlja. Tisto, kar najpogosteje manjka črkam na papirju je izkustvo – najbolj vplivne (ne)formalne norme in pravila je treba čutiti in ponotranjiti, ni jih mogoče enostavno zapakirati v obliko priročnika in servirati kot sredstvo za hitre spremembe (Rao 2007, 731). Ahilovo peto vsake IKT-organizacije tako v največji meri predstavljajo predvsem njeni zaposleni (Gonzales 2002 in Zegers 2000 v Wagnr in Brooke 2007, 118).

# 6 PREGLED STANJA INFORMACIJSKE VARNOSTNE KULTURE V IZBRANIH DIREKTORATIH

V empiričnem delu naloge bom obravnavala informacijsko varnostno kulturo v državni upravi, natančneje v Direktoratu za e-upravo in upravne procese ter v Direktoratu za informacijsko družbo. Direktorata spadata v okvir organov državne uprave in zaradi svojih osrednjih dejavnosti, ki vključujejo ključne informacijsko komunikacijske aktivnosti, pomembno vplivata na oblikovanje informacijske družbe. Kot pravi Brezovšek (2004, 20) je javna (državna) uprava pogosto tudi tisti dejavnik, ki neposredno odloča o stopnji posameznikovih pravic in svoboščin, oziroma o stopnji prisile, ki je potrebna za uveljavitev določenega ukrepa.

V skladu z v 4. poglavju omenjenim pristopom k upravljanju informacijske varnostne kulture bo najprej napravljena analiza informacijske varnostne kulture v okoljih, kjer so zaposleni ključni akterji informacijsko- komunikacijskih sistemov v Sloveniji. Rezultatom analize pa bodo sledila priporočila, kako obstoječo kulturo izboljšati oz. katerim pomanjkljivostim bi bilo potrebno nakloniti večjo pozornost v prihodnosti. Faza implementacije predlaganih priporočil in faza naknadne ocene uspešnosti teh ukrepov v okviru naloge seveda ne bosta predstavljeni, bosta pa morda izvedeni kasneje s strani samih direktoratov.

Direktorat za e-upravo in upravne procese izvaja naloge na naslednjih področjih:

- vodenje in koordinacija strategije razvoja e-poslovanja v javni upravi in priprava ter izvajanje akcijskega načrta;
- spremljanje svetovnega razvoja informacijske infrastrukture in pripravljanje usmeritev in standardov iz svojega področja dela;
- koordinacija državne uprave pri uresničevanju programa za odpravo administrativnih ovir in metodologije za izpolnjevanje in spremljanje izjave o odpravi administrativnih ovir in sodelovanju zainteresirane javnosti;
- prenova upravnih procesov in pospeševanja razvoja e-uprave s ciljem približevanja storitev državljanom in gospodarstvu;
- izboljševanje elektronske podpore med subjekti v javni upravi in izven nje z uporabo sodobne informacijsko-komunikacijske tehnologije;

- zagotavljanje povezljivosti registrov in integracija podatkovnih virov z informacijsko podporo procesom;
- razvoj principov boljše zakonodaje in metodologije za izvajanje presoje učinkov v okviru državne uprave;
- strokovne in svetovalne naloge v zvezi z razvojem sistema učinkovitosti in kakovosti javnega sektorja;
- priprava načrta nabav investicijske opreme;
- izvajanje strokovnih in usklajevalnih nalog pri sodelovanju ministrstva v mednarodnih okvirih;
- spremljanje in analiziranje ter vodenje in koordiniranje mednarodnih aktivnosti z vsebinskih področij ministrstva;
- izvajanje strokovnih in usklajevalnih nalog pri pripravah mednarodnih dokumentov in strategij;
- sodelovanje pri pripravi razpisne dokumentacije za javna naročila s področja dela, sodelovanje v komisijah za javna naročila ter pri javnih razpisih drugih državnih organov;
- skrb za informacijsko in komunikacijsko infrastrukturo ministrstva;
- skrb za razvoj, nemoteno delovanje in vzdrževanje aplikativnih sistemov državnih organov na informacijski in komunikacijski infrastrukturi ministrstva;
- skrb za računalniško infrastrukturo s področja dela in izvajanje podpore uporabnikom (Ministrstvo za javno upravo 2010)

Direktorat za informacijsko družbo pa izvaja naloge koordinacije izvajanja programa na področju informacijske družbe in bistven del svojih aktivnosti namenja aktivnostim pospeševanja razvoja informacijske družbe in usklajevanja dela na tem področju. Direktorat opravlja naloge na naslednjih področjih:

- priprava podzakonskih aktov;
- pomembni projekti, kot so npr. Projekti odprte kode, Indikatorji informacijske družbe, Mreža javno dostopnih točk (JDT): e-šole, e-knjižnice, multimedijski centri (MMC), objava vsebin e-uprave na JDT-ju, vzdrževanje spletišča e-točke, Promocija razvoja informacijske družbe, Spodbujanje uvajanja e-poslovanja, Spodbujanje razvoja IKT sektorja, Spodbujanje razvoja e-vsebin v RS, Slovenščina na daljavo,

Slovenski center za posredovanje ob internetnih incidentih, Preprečevanje nelegalne uporabe programske opreme, Spletna podoba organov državne uprave, Javni razpis Akademska omrežja in vsebine (AOV), Uvajanje e-poslovanja v lokalne skupnosti, Raziskovalni program s področja informacijske družbe – Ciljni raziskovalni program – težišče 9, Strategija Republika Slovenija v informacijski družbi, Priprava in izvedba ter sofinanciranje razpisa računalniško opismenjevanje, Evalvacija regionalnih razvojnih programov in obveznosti z naslova članstva (ERISA), e-GOV Pilot (Vinova) izvajanje programa za Slovenijo;

- sodelovanje pri oblikovanju in spremljanje izvajanja drugih strateških razvojnih dokumentov z vidika informacijske družbe;
- nacionalna koordinacija komunitarnih programov e-VsebinePlus, Varnejši internet plus in e-TEN;
- članstvo v upravnih odborih komunitarnih programov in iniciativ EU;
- sodelovanje v mednarodnih organizacijah in njihovih delovnih skupinah, kot so npr. eAccessibility (EU), High Level Group on Internet Governance (UN/WSIS), e-Governance (OECD), Delovanje in članstvo v ERISA v imenu slovenskih regionalnih razvojnih agensov (RRA), Delovna skupina Sveta EU za telekomunikacije in informacijsko družbo, Delovna skupina EU za strukturno politiko in regionalni razvoj, Sodelovanje pri aktivnostih za pripravo WSIS, Skupina za varna in inteligentna vozila (EU-DG INFSO e-Safety);
- sodelovanje v projektih s področja ID, katerih nosilci so drugi organi, kot so: Register premične kulturne dediščine, Digitalizacija kulturne dediščine, Glasbeno informacijski center, Elektronske volitve, Poslovni načrt sistema za podporo lokacijskim storitvam, Iniciativa "računalnik v vsak dom", Projekt e-VEM (vse na enem mestu), Elektronska izmenjava podatkov v javni upravi, Projekt usposabljanje JU za e-upravo, Projekt Vpogled v CRP za lokalne skupnosti (CRP – Centralni register prebivalstva), Priprava in spremljanje Nacionalnega akcijskega načrta za socialno vključevanje, Priprava in spremljanje Skupnega memoranduma RS in EK o socialnem vključevanju (JIM), Projektni svet IS UNZ, Projektni svet za izvedbo projekta IS nabav, Državni portal e-uprave;
- članstvo v javnih zavodih – ARNES;
- sodelovanje v medresorskih delovnih skupinah;
- priprava stališč v postopku sprejemanja zakonodajnih predlogov in drugih aktov EU;

- mednarodno sodelovanje;
- pomembne tekoče naloge kot so npr. vodenje registra overiteljev, izredna naturalizacija - mnenja, predčasna izdaja dovoljenja za stalno bivanje (Ministrstvo za visoko šolstvo, znanost in tehnologijo 2010).

## 6.1 PODATKI O RAZISKAVI

V raziskavo sta bila vključena Direktorat za e-upravo in upravne procese in Direktorat za informacijsko družbo. Pri obeh direktoratih je bilo iz proučevane populacije izvzeto administrativno osebje ali podporno osebje (večinoma tajnice), ki nima neposrednega opravka s področjem IKT-ja, pri Direktoratu za e-upravo in upravne procese pa tudi zaposleni na Sektorju za boljše predpise in upravne procese. V okviru Direktorata za e-upravo in upravne procese tako populacijo predstavlja 63 oseb (vodstvo: 10 oseb in IKT-strokovnjaki: 53 oseb), v okviru Direktorata za informacijsko družbo pa 31 oseb (vodstvo: 5 oseb in IKT-strokovnjaki: 26 oseb).

Podatki, ki jih predstavljam v empiričnemu delu so bili pridobljeni v mesecu juliju 2010. Anketni vprašalniki so bili razdeljeni s strani direktoratov samih, sodelovanje v raziskavi pa je bilo prostovoljno. Anketirancem je bila zagotovljena anonimnost in povratna informacija o rezultatih v kolikor jih bodo le-ti zanimali.

V raziskavi je bil uporabljen klasičen anketni vprašalnik v katerem so strnjena spoznanja iz teoretičnega dela, upoštevana pa je tudi specifičnost izbranih organizacij. Vprašalnik je bil izdelan na podlagi vprašalnika, ki ga je zasnoval Martins (2002) in nato ustrezno prilagojen ter dopolnjen z dodatnimi vprašanji.

Anketni vprašalnik je razdeljen na dva vsebinska sklopa in zaključni, demografski del. Prvi vsebinski del je sestavljen iz 50 trditev (spremenljivk), ki merijo značilnosti informacijske varnostne kulture po posameznih ravneh organizacije (politike in postopki, benchmarking ali zgledovalno primerjanje, analiza tveganj, proračun, menedžment, zaupanje, zavedanje ali osveščenost, etičnost in pripravljenost za spremembe) s pomočjo petstopenjske lestvice tipa Likert. Lestvica se razteza od stopnje 5 do stopnje 1, pri čemer 5 pomeni, da se anketiranec s trditvijo močno strinja, 1 pa, da se s trditvijo sploh ne strinja. Vmesne vrednosti ustrezajo

vrednosti lestvici in predstavljajo odgovore strinjam se (stopnja 4), niti se strinjam niti se ne strinjam (stopnja 3) in ne strinjam se (stopnja 2). Drugi del vprašalnika sestavlja 8 trditev, ki se nekoliko bolj konkretno nanašajo na organizacijo, v kateri je anketiranec zaposlen, saj je nanje mogoče odgovoriti le z odgovorom da, ne ali ne vem. K tem trditvam sem dodala še trditev na katero je mogoče odgovoriti z eno izmed ponujenih stopenj petstopenjske lestvice. Vprašalnik se zaključuje z vprašanji o demografskih podatkih. V tem delu sem spraševala po spolu, starosti, številu let v trenutni organizaciji, delovnem mestu, izobrazbi in njeni povezanosti s področjem IKT-ja.

### 6.1.1 Urejanje in obdelava podatkov

Zbrani podatki so bili urejeni in obdelani s programom SPSS za statistično obdelavo podatkov. Podatki so bili obdelani s pomočjo opisne statistike, frekvenčne porazdelitve indikatorjev po Likertu in ostalih spremenljivk, analize demografskih podatkov ter korelacijske analize in regresijske analize.

Za vprašalnik sem izvedla tudi analizo notranje konsistentnosti s pomočjo Chronbachovega koeficienta α. Ta znaša 0,920 in zagotavlja dovolj veliko zanesljivost uporabljenega vprašalnika (lastnost, da daje pri ponovljenih merjenih istih lastnosti pri istih osebah enake rezultate).

### 6.1.2 Opis vzorca

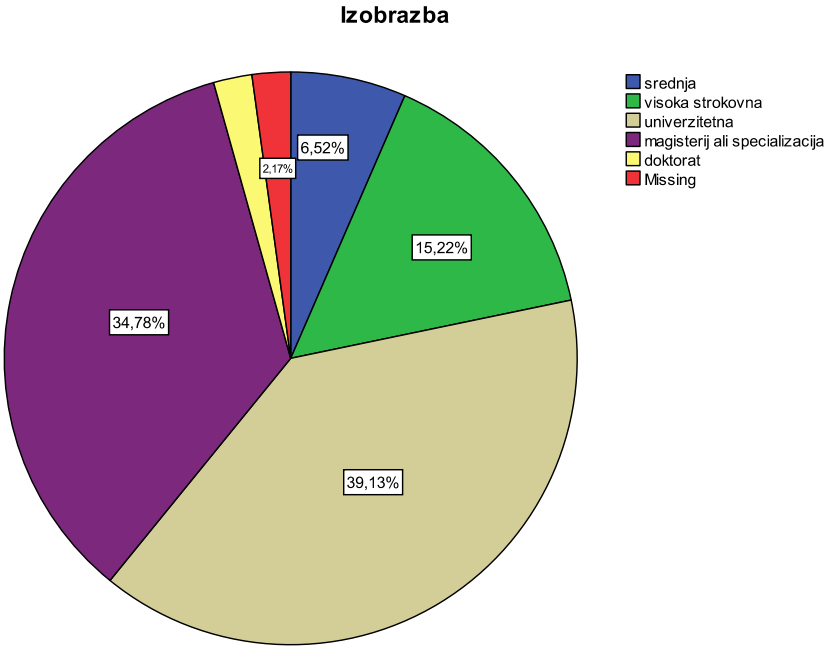
V raziskavi je sodelovalo 46 anketirancev, od katerih jih je bilo 32 zaposlenih na Direktoratu za e-upravo in upravne procese, 13 pa na Direktoratu za informacijsko družbo. Večina anketirancev, 66,7 %, je bila moškega spola. Anketiranci so bili v povprečju stari 40 let (od najmanj 25 do največ 64 let, SD = 7,91), največ pa se jih je nahajalo v starostnem razredu med 41 in 50 letom (Tabela 6.1). Na direktoratu so bili zaposleni povprečno 8,98 let.

**Tabela 6.1:** Starostni razredi v letih

| Starostni razredi | | frekvenca | odstotek | veljaven odstotek | komulativen odstotek |
|---|---|---|---|---|---|
| | od 25 do 30 let | 6 | 13,0 | 14,0 | 14,0 |
| | od 31 do 40 let | 16 | 34,8 | 37,2 | 51,2 |
| | od 41 do 50 let | 18 | 39,1 | 41,9 | 93,0 |
| | od 51 do 64 let | 3 | 6,5 | 7,0 | 100,0 |
| | skupaj | 43 | 93,5 | 100,0 | |
| Manjkajoče | vrednosti | 3 | 6,5 | | |
| skupaj | | 46 | 100,0 | | |

Več kot 90 % anketirancev je visoko izobraženih, od tega jih ima največ 40 % univerzitetno izobrazbo, 35,6 % pa magisterij ali specializacijo (glej Graf 6.1). Več kot polovica, 57,8 % jih je potrdila, da je njihova formalna izobrazba povezana s področjem IKT-ja.

**Graf 6.1:** Izobrazbena struktura anketirancev



## 6.2 PREDSTAVITEV REZULTATOV

V nadaljevanju bodo predstavljeni rezultati analize stanja informacijske varnostne kulture v obeh proučevanih direktoratih. Najprej bodo predstavljeni rezultati, ki so bili pridobljeni z analizo celotnega vzorca, tam kjer so bile izračunane statistično značilne razlike med proučevanima direktoratoma, pa tudi rezultati za posamezen direktorat.

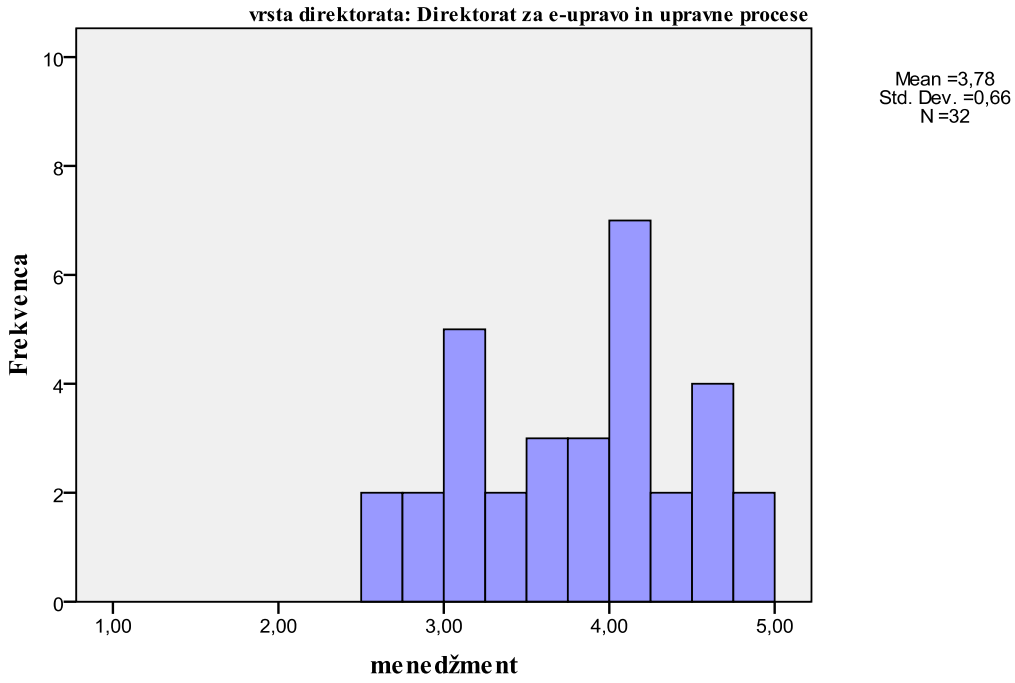
### 6.2.1 Analiza informacijske varnostne kulture v proučevanih direktoratih

Analiza trenutnega stanja informacijske varnostne kulture je bila opravljena s pomočjo opisnih statistik, s katerimi je bilo merjenih devet indikatorjev (zajeti v sklopu petdesetih trditev). Rezultati kažejo, da je informacijsko varnostno kulturo v proučevanih direktoratih mogoče oceniti kot izredno visoko. Zaposleni so namreč vse indikatorje ocenili nadpovprečno, saj so se ocene pri vseh indikatorjih gibale med 3,57 in 4,30. Najbolje ocenjeni indikatorji, ki so jih zaposleni ocenili z oceno 4 in več, so indikator proračuna, zaupanja ter politik in postopkov. Kot je razvidno iz spodnje Tabele 6.2, tem indikatorjem sledijo indikator zavedanja ali osveščenosti, etičnosti, sprememb, benchmarking-a oz. zgledovalnega primerjanja in analize tveganj. Na zadnje mesto se je uvrstil indikator menedžment, pri katerem pa je potrebno razlikovati ocene med direktoratoma, saj se njegova ocena statistično značilno razlikuje glede na direktorat, $t(19,4) = 2,63$; $p = 0,16$. V Direktoratu za e-upravo in upravne procese (v nadaljevanju DEUUP) je povprečna vrednost odgovorov višja kot v Direktoratu za informacijsko družbo (v nadaljevanju DID) in znaša 3,57 ($\delta = 0,66$). V slednjem namreč znaša povprečna vrednost 3,08 (SD = 0,90) (glej Graf 6.2 in Graf 6.3).

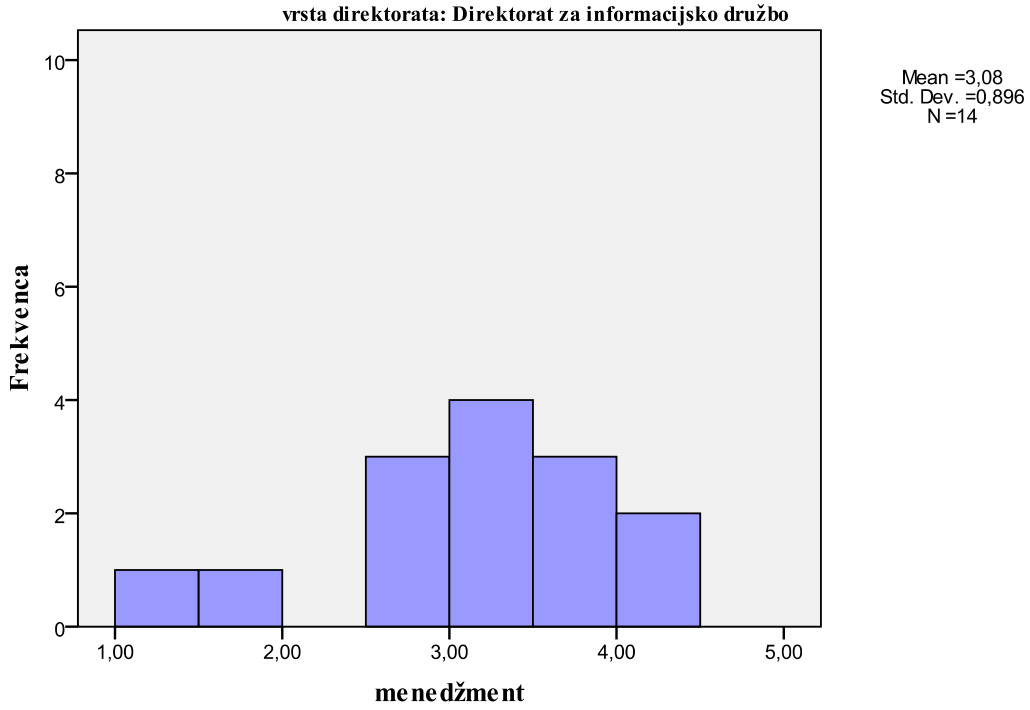
**Tabela 6.2:** Ocene posameznih indikatorjev IVK

| | OCENE POSAMEZNIH INDIKATORJEV IVK | | | | |
|---|---|---|---|---|---|
| **Razporeditev** | **INDIKATOR** | **Povprečna vrednost** | **Standardni odklon** | **Minimalna vrednost** | **Maksimalna vrednost** |
| 1. | PRORAČUN | 4,30 | 0,57 | 3 | 4 |
| 2. | ZAUPANJE | 4,14 | 0,74 | 2,50 | 5 |
| 3. | POLITIKE IN POSTOPKI | 4,09 | 0,58 | 2 | 5 |
| 4. | ZAVEDANJE | 3,95 | 0,43 | 2,80 | 5 |
| 5. | ETIČNOST | 3,92 | 0,46 | 2,78 | 4,78 |
| 5. | PRIPRAVLJENOST NA SPREMEMBE | 3,92 | 0,66 | 2,33 | 5 |
| 6. | ZGLEDOVALNO PRIMERJANJE | 3,80 | 0,61 | 2 | 5 |
| 7. | ANALIZA TVEGANJ | 3,75 | 0,68 | 2 | 5 |
| 8. | MENEDŽMENT:<br>• Direktorat za e-upravo in upravne procese<br>• Direktorat za informacijsko družbo | 3,78<br>3,08 | 0,66<br>0,90 | 2,6<br>1 | 4,90<br>4,10 |

**Graf 6.2:** Gibanje ocen za indikator menedžment (DEUUP)



**Graf 6.3:** Gibanje ocen za indikator menedžment (DID)




- ***Korelacijska analiza med posameznimi indikatorji***

V Tabeli 6.3 so prikazani rezultati korelacijske analize med posameznimi indikatorji s katerimi sem opredelila informacijsko varnostno kulturo. Ugotovim lahko, da se precej indikatorjev med sabo povezuje (statistično značilne povezave so označene s sivo bravo), kar kaže na močno prepletanje in medsebojno odvisnost posameznih kazalcev. Statično značilno se med sabo povezujejo naslednji indikatorji: a) politike in postopki z analizo tveganj, zavedanjem in etičnostjo, b) zgledovalno primerjanje z analizo tveganj, menedžmentom, zaupanjem in etičnostjo, c) analiza tveganj z menedžmentom, zaupanjem, etičnostjo, pripravljenostjo na spremembe, d) proračun z etičnostjo, e) menedžment z zaupanjem, etičnostjo, pripravljenostjo na spremembe, f) zaupanje z etičnostjo, g) zavedanje z etičnostjo in h) etičnost s pripravljenostjo na spremembe.

**Tabela 6.3:** Korelacijska analiza med posameznimi indikatorji

| indikatorji | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| **1 politike in postopki** | r | 1 | | | | | | | | |
| | p | | | | | | | | | |
| | N | 46 | | | | | | | | |
| **2 zgledovalno primerjanje** | r | ,327 | 1 | | | | | | | |
| | p | ,027 | | | | | | | | |
| | N | 46 | 46 | | | | | | | |
| **3 analiza tveganj** | r | ,495 | ,604 | 1 | | | | | | |
| | p | ,000 | ,000 | | | | | | | |
| | N | 46 | 46 | 46 | | | | | | |
| **4 proračun** | r | ,368 | ,367 | -,016 | 1 | | | | | |
| | p | ,012 | ,012 | ,915 | | | | | | |
| | N | 46 | 46 | 46 | 46 | | | | | |
| **5 menedžment** | r | ,165 | ,585 | ,482 | ,239 | 1 | | | | |
| | p | ,274 | ,000 | ,001 | ,109 | | | | | |
| | N | 46 | 46 | 46 | 46 | 46 | | | | |
| **6 zaupanje** | r | ,141 | ,477 | ,520 | ,194 | ,674 | 1 | | | |
| | p | ,355 | ,001 | ,000 | ,202 | ,000 | | | | |
| | N | 45 | 45 | 45 | 45 | 45 | 45 | | | |
| **7 zavedanje** | r | ,688 | ,212 | ,345 | ,443 | ,140 | ,270 | 1 | | |
| | p | ,000 | ,158 | ,019 | ,002 | ,352 | ,073 | | | |
| | N | 46 | 46 | 46 | 46 | 46 | 45 | 46 | | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **8 etičnost** | r | ,456 | ,473 | ,581 | ,468 | ,581 | ,597 | ,484 | 1 | |
| | p | ,001 | ,001 | ,000 | ,001 | ,000 | ,000 | ,001 | | |
| | N | 46 | 46 | 46 | 46 | 46 | 45 | 46 | 46 | |
| **9 pripravljenost na spremembe** | r | ,380 | ,437 | ,674 | ,107 | ,716 | ,408 | ,142 | ,483 | 1 |
| | p | ,011 | ,003 | ,000 | ,488 | ,000 | ,006 | ,359 | ,001 | |
| | N | 44 | 44 | 44 | 44 | 44 | 44 | 44 | 44 | 44 |

Opomba: Zaradi majhnega vzorca sem pri izračunu uporabila Bonferronijev popravek, kjer se zahtevana raven tveganja dobi tako, da se kritična vrednost p=0,05 deli s številom vseh t-testov (Bonferronijev popravek: ac= a/k).

S pomočjo t-testa (upoštevana predpostavka o neobstoju enakih varianc) sem izmerila tudi povezanost med spremenljivkami informacijske varnostne kulture in posameznima direktoratoma. Ugotovila sem, da prihaja do statistično značilnih razlik pri strinjanju s šestimi trditvami, izmed njih se kar tri nanašajo na delo vodstva[7]. Zaposleni na DEUUP-ju se v 84,40 % strinjajo ali močno strinjajo s trditvijo, da poznajo osebo (ali skupino), ki je zadolžena za upravljanje z varovanjem informacij v njihovi organizaciji, zaposleni na DID-u v 28,50 %, t(21,9) = 3,92; p = 0,001. 78,20 % zaposlenih na DEUUP-u je mnenja, da vodstvo pomaga pri izvajanju dejavnosti, ki se nanašajo na informacijsko varnost, medtem ko je na DID-u istega mnenja 50 % zaposlenih, t(20,3) = 2,396; p = 0,026. Podobno je ocenjeno tudi zavedanje vodstva o pomembnosti varovanja informacij, s katerimi ima organizacija opravka, in spoštovanje zasebnosti podatkov, ki se nanašajo na zaposlene. In sicer, 80,7 % zaposlenih na DEUUP-ju in 58,30 % zaposlenih na DID-u je mnenja, da se vodstvo zaveda pomembnosti varovanja informacij (t (23,4) = 2,29; p = 0,032), prav tako jih 84,4 % zaposlenih na DEUUP-ju in 50,00 % na DID-u meni, da vodstvo spoštuje zasebnost njihovih osebnih podatkov (t(25,7) = 2,36; p = 0,026).

Z nadzorom nad ravnanjem z zaupnimi podatki je na DEUUP-ju zadovoljnih 73,30 % zaposlenih (26, 70 jih ni niti zadovoljnih niti nezadovoljnih), na DID-u pa 35,7 % zaposlenih (50,00 % jih ni niti zadovoljnih niti nezadovoljnih, 14,30 % pa jih z nadzorom ni zadovoljnih), t (23,8) = 2,86; p = 0,009. Nekoliko slabše pa je ocenjena trditev, ki se nanaša

[7] Pri izračunu sem upoštevala kritično vrednost p= 0,05 in ne Bonferronijev popravek. Zaradi tega je potrebna previdnost pri interpretaciji rezultatov, saj lahko prihaja zaradi majhnega vzorca do odstopanja med izračunom in realnim stanjem.

na ustrezno prilagojenost informacijsko-komunikacijskih sistemov zahtevnim standardom varovanja zaupnih podatkov, t(17,9) = 3,196; p = 0,005. Na DEUUP-ju ocenjuje 69,00 % zaposlenih ocenjuje, da je prilagajanje informacijsko-komunikacijskih sistemov ustrezno (31,00 % zaposlenih s prilagajanjem ni niti zadovoljna niti nezadovoljna), na DID-u pa precej manj– 25, 00 % (58,30 % zaposlenih s prilagajanjem ni niti zadovoljnih niti nezadovoljnih).

- ***Multipla regresijska analiza***

Zaradi teoretičnih predpostavk, da organizacijske ravni vplivajo obojestransko ena na drugo, (organizacijska raven vpliva na skupinsko in individualno raven, skupinska raven na organizacijsko in individualno raven, individualna raven pa prav tako na organizacijsko in skupinsko) sem želela njihov vpliv izmeriti tudi v okviru raziskave. Zanimalo me je predvsem to, v kolikšni meri indikatorji na organizacijski in skupinski ravni vplivajo na to, kako posameznik razume področje informacijske varnosti. Vpliv organizacijske in skupinske ravni na individualno raven (sestavljata jo indikator etičnost in indikator zavedanje) sem merila s pomočjo multiple regresijske analize.

Najprej sem napravila regresijsko analizo za indikator etičnost. Kot je razvidno iz Tabele 6.4 lahko s pomočjo treh neodvisnih indikatorjev (analiza tveganj, proračun in zaupanje) pojasnimo 61,2 % variance indikatorja etičnosti. Vrednost F (3, 40) za celotni model je 23,58 (p < 0,00). Indikatorji, ki so bili iz modela izključeni imajo seveda lahko na indikator določen vpliv, a ne značilnega.

**Tabela 6.4:** Regresijska analiza indikator etičnost[8]

| SPREJEMLJIVKE | B | β | t | p |
|---|---|---|---|---|
| analiza tveganj | 0,315 | 0,453 | 4,075 | < 0,00 |
| proračun | 0,311 | 0,367 | 3,792 | < 0,00 |
| zaupanje | 0,190 | 0,299 | 2,657 | 0,011 |
| F (3, 40) = 23,58; popravljen $R^2$= 0,612; p < 0,00 | | | | |

Regresijska analiza za indikator zavedanje je pokazala, da lahko s pomočjo le dveh neodvisnih indikatorjev (politike in postopki ter proračun) pojasnimo 52,1 % variance indikatorja. Vrednost F (2, 41) za celotni model je 24,37 (p < 0,00) (glej Tabelo 6.5).

[8] V vseh regresijskih tabelah so prikazane neodvisne spremenljivke po vrstnem redu oz. pojasnjevalni moči v odnosu do odvisne spremenljivke.

**Tabela 6.5:** Regresijska analiza indikator zavedanje

| SPREJEMLJIVKE | B | β | t | p |
|---|---|---|---|---|
| politike in postopki | 0,438 | 0,587 | 5,137 | < 0,00 |
| proračun | 0,219 | 0,091 | 2,397 | 0,021 |
| F (2, 41) = 24,37; popravljen $R^2$ = 0,521; p < 0,00 | | | | |

Opravila sem tudi regresijsko analizo med indikatorjema in demografskimi spremenljivkami. Ta je pokazala, da demografske spremenljivke nimajo vpliva na indikator etičnost, na indikator zavedanje pa statistično značilno vplivata dve spremenljivki, in sicer: čas zaposlitve v sedanji organizaciji in delovno mesto. Čas zaposlitve ima beta 0,026, t = 2,820, p = 0,007, kar pomeni, da dlje časa trajajoča zaposlitev v direktoratu pomembno prispeva k višji stopnji zavedanja razsežnosti informacijske varnosti. Pomemben pa je tudi dejavnik delovno mesto, ki ima beta -0,331, t = -2,113, p = 0,041 in kaže na to, da se posamezniki na vodstvenih[9] položajih bolj zavedajo oz. imajo višjo stopnjo zavedanja kot posamezniki na ostalih delovnih mestih.

- ***Spremenljivke, ki merijo konkretno stanje v organizaciji***

V drugem vsebinskem sklopu so anketiranci odgovarjali na vprašanja v obliki trditev s pomočjo treh ponujenih odgovorov. Ker me je zanimalo, ali so določene stvari v njihovi organizaciji urejene (npr. narejen varnostni načrt, sprejete politike, seznanjenost s tveganji, itd.), so anketiranci na trditev lahko odgovorili le z odgovorom da, ne ali ne vem. Trditve, ki so bile zastavljene v tem delu in odgovori nanje, so prikazani v Tabeli 6.6.

**Tabela 6.6:** Odgovori na trditve o konkretnem stanju v organizaciji

| TRDITEV | DA | NE | NE VEM |
|---|---|---|---|
| 1. V naši organizaciji obstaja utečen postopek, ki zagotavlja, da so vsi zaposleni seznanjeni z določili varovanja zaupnih informacij. | 35,60 % | 22,20 % | 42,20 % |
| 2. V naši organizaciji so predvideni natančni ukrepi za primer nespoštovanja predpisov s področja varovanja zaupnih podatkov. | 22,70 % | 18,20 % | 59,10 % |
| 3. Vsi zaposleni v naši organizaciji so seznanjeni s tveganji, ki so opredeljena za varovanje zaupnih podatkov. | 20,00 % | 22,20 % | 57,8 % |

[9] V okviru statističnih obdelav sem vodstveno delovno mesto ovrednotila s številko 1, nevodstveno delovno mesto pa s številko 2. Negativen predznak se povezuje z nižjo številko spremenljivke, ki je v mojem primeru vodstveno delovno mesto in kaže na to, da višje zavedanje raste sorazmerno s padanjem številke na delovnem mestu.

| | | | |
|---|---|---|---|
| 4. V naši organizaciji imamo izdelan varnostni načrt na področju IKT-ja.<br>$X^2(2) = 16,98; p < 0,00$[10] | | | |
| • Direktorat za e-upravo in upravne procese | 68,8 % | 6,3 % | 25,0% |
| • Direktorat za informacijsko družbo | 7,70 % | 0,00 % | 92,3 % |
| 5. Naša organizacija ima zapisana pravila (politike) informacijske varnosti.<br>$X^2(2) = 9,34; p < 0,00$[11] | | | |
| • Direktorat za e-upravo in upravne procese | 68,75 % | 6,25 % | 25,00 % |
| • Direktorat za informacijsko družbo | 25,00 % | 0,00 % | 75,00 % |
| 6. V naši organizaciji imamo predpisana pravila o tem, kako poročati o nezgodah, ki so v povezavi z informacijsko varnostjo.<br>$X^2(2) = 7,48; p = 0,024$[12] | | | |
| • Direktorat za e-upravo in upravne procese | 53,10 % | 9,40 % | 37,5 % |
| • Direktorat za informacijsko družbo | 16,70 % | 0,00 % | 83,30 % |
| 7. Enostavno lahko pridobim kopijo dokumenta o informacijsko varnostih pravilih, ki obstajajo v naši organizaciji.<br>$X^2(2) = 16,998; p < 0,00$[13] | | | |
| • Direktorat za e-upravo in upravne procese | 53,10 % | 18,80 % | 28,10 % |
| • Direktorat za informacijsko družbo | ni odgovorov = manjkajoče vrednosti | ni odgovorov = manjkajoče vrednosti | 78,60 % |

Kot je razvidno iz Tabele 6.6, večina anketirancev na dane trditve ni znala odgovoriti z odgovorom da ali ne in je največkrat odgovorila z odgovorom ne vem (na pet izmed sedmih trditev), kar pomeni, da je mogoče klepati, da na zastavljeno trditev ne zna ali ve odgovoriti. Zaradi pričakovanj, da lahko med merjenima skupinama prihaja do razlik pri odgovorih, sem frekvenčne porazdelitve odgovorov testirala s pomočjo Hi-kvadrat testa (meri statististično pomenljive razlike med vrednostmi posameznih skupin). Rezultati kažejo, da prihaja do

[10] Potrebno je opozoriti, da imata dve celici od šestih ocenjeno vrednost manjšo od pet.
[11] Potrebno je opozoriti, da imajo tri celice od šestih ocenjeno vrednost manjšo od pet.
[12] Potrebno je opozoriti, da imata dve celici od šestih ocenjeno vrednost manjšo od pet.
[13] Potrebno je opozoriti, da imajo tri celice od šestih ocenjeno vrednost manjšo od pet.

statistično značilnih razlik med direktoratoma pri ocenjevanju štirih trditev (trditve 4, 5, 6 in 7). In sicer, zaposleni na DEUUP-ju odgovarjajo primerjalno z zaposlenimi na MID-u v večjem številu, da ima njihova organizacija izdelan varnostni načrt na področju IKT-ja, da ima predpisana pravila o tem, kako poročati o nezgodah, ki so v povezavi z informacijsko varnostjo, da ima zapisana pravila (politike) informacijske varnosti in da je pri njih razmeroma enostavno pridobiti kopijo dokumenta o informacijsko varnostnih pravilih. Poleg tega se pri njih odgovori razporejajo od strinjanja s trditvijo oz. s tem, da bodisi varnostni načrt, pravila poročanja in politike obstajajo bodisi jih je enostavno pridobiti, do tega, da zaposleni ne vedo ali niso prepričani, če dokumenti obstajajo in kako enostavno jih je pridobiti. Zelo nizek procent odgovorov pa kaže na to, da teh dokumentov v organizaciji ni oz. se jih ne da enostavno pridobiti. Nasprotno, zaposleni na MID-u na trditve največkrat odgovarjajo z odgovorom »ne vem«, ki ga lahko razumemo kot dejanski neobstoj dokumentov ali zgolj slabo poznavanje notranjih predpisov.

- ***Povezanost socialno-demografskih dejavnikov s spremenljivkami informacijske varnostne kulture***

Povezanost med socialno-demografskimi dejavniki in spremenljivkami informacijske varnostne kulture je bila merjena s korelacijsko analizo. Zanimala me je povezanost med spremenljivkami in spolom, starostjo, izobrazbo, številom let v trenutni organizaciji in delovnim mestom. Pri izračunu sem upoštevala kritično vrednost $p = 0,05$. Zaradi tega je potrebna previdnost pri interpretaciji rezultatov, saj lahko prihaja zaradi majhnega vzorca do odstopanja med izračunanim in realnim stanjem.

*a) vpliv spola*

Stopnjo povezanosti med spolom in spremenljivkami informacijske varnostne kulture sem izmerila s pomočjo t-testa. Statistično značilne razlike pri ocenjevanju trditev so se pokazale pri trditvi, ki se nanaša na vključevanje stroškov za zagotavljanje informacijske varnosti v proračun organizacije ($t(21,9) = 2,78$; $p = 0,033$) in trditvi, ki se nanaša primernost upravljanja z zaupnimi dokumenti in informacijami v organizaciji z vidika varnosti ($t(32,8) = -2,43$; $p = 0,025$). S prvo trditvijo se kljub majhni razliki v nekoliko večji meri strinjajo moški ($M = 4,73$; $SD = 0,52$) kot ženske ($M = 4,27$; $SD = 0,70$), medtem ko imajo o primernosti

upravljanja z zaupnimi podatki nekoliko slabše mnenje moški (M = 3,67; SD = 0,80) kot ženske (M = 4,20; SD = 0,68).

Spremenljivka spol se povezuje tudi z indikatorjem zgledovalnega primerjanja, t(40,78) = -2,16; p = 0,037). Ženske ocenjujejo, da je indikator prisoten v organizaciji v večji meri (M = 4,04; SD = 0,4), kot moški (M = 3,70; SD = 0,66).

*b) vpliv starosti*

Stopnjo linearne povezanosti med spremenljivkami in starostjo sem merila s pomočjo Pearsonovega koeficienta korelacije. Ugotovila sem, da anketiranci, ki so starejši, odgovarjajo v primerjavi z mlajšimi sodelavci, na določene trditve z višjo oceno. Statistične značilne razlike glede na starost obstajajo pri naslednjih trditvah:

- Nadzor nad ravnanjem z zaupnimi podatki je v naši organizaciji primeren in primerljiv z ukrepi v podobnih organizacijah (r = 0,31; p = 0,046).
- V naši organizaciji je vzpostavljen takšen pretok informacij, ki zagotavlja ustrezno obveščenost zaposlenih v zvezi z varovanjem informacij (r = 0,34; p = 0,029).
- Organizacija skrbi za to, da spoštujem in upoštevam informacijsko-varnostna pravila (r = 0,35; p = 0,023).
- Menim, da mora proračun organizacije vključevati tudi stroške, ki se nanašajo na zagotavljanje informacijske varnosti v organizaciji (r = 0,33; p = 0,032).
- Vodstvo v naši organizaciji dejansko izvaja ukrepe, predvidene za primer neupoštevanja predpisov s področja varovanja zaupnih podatkov (r = 0,32; p = 0,043).
- Prepričan sem, da moji sodelavci moralno obsojajo zlorabo informacij (r = 0,34; p = 0,028).
- Zaupam vodstvu naše organizacije (r = 0,32; p = 0,038).
- Informacijsko varnost ni potrebno obravnavati kot stvar »tehnične zaščite« (r = 0,43; p = 0,004).

*c) vpliv izobrazbe*

Vpliv izobrazbe anketirancev na ocenjevanje spremenljivk sem merila s pomočjo Spearmanovega koeficienta korelacije. Ugotovila sem, da se med ocenjevanimi parametri pojavlja ena statistično značilna povezanost in sicer, anketiranci z višjo stopnjo izobrazbe se v večjem številu strinjajo s trditvijo, da je informacijsko varnost potrebno obravnavati kot stvar menedžmenta (s = 0,31; p = 0,042), kot anketiranci z nižjo stopnjo izobrazbe.

*d) vpliv števila let v trenutni organizaciji*

Zanimala me je tudi povezanost med številom let v trenutni organizaciji in ocenami trditev, ki sem jo merila s Pearsonovim koeficientom korelacije. Število let v trenutni organizaciji se statistično značilno povezuje z naslednjimi trditvami:

- Vsaka organizacija bi morala imeti izdelan načrt informacijske varnostne zaščite, ki je prilagojen posebnostim delovanja organizacije (r = 0,49; p = 0,001).
- Menim, da je potrebno upoštevati pravila informacijske varnosti v organizaciji (r = 0,357; p = 0,019).
- Poznavanje lastnosti in namena obstoječih varnostnih ukrepov (npr. protivirusni program, enkripcija) v organizaciji je pomembno (r = 0,47; p= 0,001).

*e) vpliv delovnega mesta*

Povezanost med delovnim mestom in ocenami trditev sem merila s pomočjo t-testa. Rezultati kažejo, da se ocene posameznih trditev razlikujejo glede na to, ali je oseba zaposlena na vodstvenem mestu ali dela kot IKT-strokovnjak na nevodstvenem mestu. Kot je razvidno iz Tabele 6.7, prihaja do statistično značilnih razlik pri ocenah devetih trditev. V primeru, da bi uporabila veliko bolj konzervativen Bonferronijev popravek (0,05/50), pa bi do statistično značilne razlike prišlo le v enem primeru št. 5, ki se nanaša na osebno odgovornost za neupoštevanje/zlorabo pravil o varovanju informacij v organizaciji, t(36,0) = 4,74; p< 0,00.

**Tabela 6.7:** Statistično značilna povezanost med delovnim mestom in ocenami trditev

| | Ali naloge opravljate na vodstvenem delovnem mestu? | N | M | SD |
|---|---|---|---|---|
| 1. Osebno me motijo dejanja sodelavcev, ki ne spoštujejo varnostnih določil IKT-ja, predpisanih v organizaciji. | t(18,55) = 3,18; p = 0,005 | | | |
| | da | 7 | 4,43 | ,535 |
| | Ne | 38 | 3,55 | 1,155 |
| 2. Počutim se odgovornega za vzdrževanje visoke stopnje informacijske varnosti v naši organizaciji. | t(17,86) = 2,93; p = 0,009 | | | |
| | da | 7 | 4,43 | ,535 |
| | Ne | 38 | 3,63 | 1,125 |
| 3. Menim, da je potrebno upoštevati pravila informacijske varnosti v organizaciji. | t(19,72) = 2,55; p = 0,019 | | | |
| | da | 7 | 4,29 | ,488 |
| | Ne | 38 | 4,55 | ,686 |
| 4. Organizacijska struktura, odgovornosti in pristojnosti na področju varovanja podatkov so v naši organizaciji jasno opredeljene in opisane. | t(17,03) = 2,91; p = 0,010 | | | |
| | da | 7 | 4,00 | ,577 |
| | Ne | 38 | 3,16 | 1,175 |
| 5. Menim, da bi moral biti vsak posameznik osebno odgovoren za neupoštevanje/zlorabo pravil o varovanju informacij v naši organizaciji. | t(36,00) = 4,74; p = 0,000 | | | |
| | da | 7 | 5,00 | ,000 |
| | Ne | 37 | 4,43 | ,728 |
| 6. V naši organizaciji je vzpostavljen takšen pretok informacij, ki zagotavlja ustrezno osveščenost zaposlenih v zvezi z varovanjem zaupnih podatkov. | t(11,68 )= 3,06; p = 0,010 | | | |
| | da | 7 | 4,14 | ,690 |
| | Ne | 36 | 3,19 | 1,009 |
| 7. Organizacija skrbi za to, da spoštujem in upoštevam informacijsko varnostna pravila. | t(22,65) = 2,63; p = 0,015 | | | |
| | da | 7 | 3,86 | ,378 |
| | Ne | 36 | 3,31 | ,920 |
| 8. Prepričan sem, da moji sodelavci moralno obsojajo zlorabo informacij. | t(22,88) = 3,57; p = 0,002 | | | |
| | da | 7 | 4,86 | ,378 |
| | Ne | 37 | 4,11 | ,936 |
| 9. Informacijsko-komunikacijski sistemi v naši organizaciji se ustrezno prilagajajo zahtevanim standardom varovanja zaupnih podatkov. | t(14,90) = 2,78; p = 0,014 | | | |
| | da | 6 | 4,17 | ,408 |
| | Ne | 35 | 3,54 | ,886 |

Poleg tega se spremenljivka delovno mesto zaposlenih povezuje tudi z indikatorjem analize tveganj, $t(17,8) = 3,04$; $p = 0,007$). Vodstveni kadri ocenjujejo, da je indikator prisoten v organizaciji v večji meri ($M = 4,14$; $SD = 0,33$) kot posamezniki, ki niso na vodstvenih položajih ($M = 3,64$; $SD = 0,68$).

### 6.2.2 Povzetek glavnih ugotovitev

Stopnja obstoječe informacijske varnostne kulture je v izbranih direktoratih ocenjena nadpovprečno visoko, kar kaže na to, da so v zadostni meri vzpostavljeni nujno potrebni ukrepi za zagotavljanje informacijske varnosti. Nekoliko več pozornosti je potrebno nameniti vlogi, ki jo ima vodstveno osebje, saj je njihov prispevek izmed vseh indikatorjev informacijske varnostne kulture ocenjen najslabše. Poleg tega je potrebno več truda vložiti tudi v znanje in varnostno osveščenost zaposlenih. Precejšnja razpršenost odgovorov namreč kaže na izjemno kritičnost nekaterih posameznikov in predstavlja pomemben razlog za uvedbo ukrepov, ki bodo obstoječo informacijsko varnostno kulturo okrepili.

Izmed indikatorjev so najvišje ocenjeni proračun, zaupanje ter politike in postopki. Tem indikatorjem sledi indikator zavedanja, etičnosti, pripravljenosti na spremembe, zgledovalnega primerjanja in analize tveganj. Kot najslabše ocenjen indikator se je uvrstil indikator menedžmenta, pri katerem se ocene statistično značilno razlikujejo glede na vrsto direktorata. Zaposleni na DEUUP-ju ocenjujejo vlogo menedžmenta bolje kot njihovi kolegi, ki so zaposleni na DID-u. Do statističnih razlik med direktoratoma prihaja tudi pri mnenju o tem, koliko vodstvo pomaga pri izvajanju dejavnosti, ki se nanašajo na informacijsko varnost (po ocenah sodeč je vodstvo DEUUP-ja bolj aktivno kot vodstvo DID-a), in koliko se vodstvo zaveda pomembnosti varovanja splošnih informacij, kot tudi tistih, ki se nanašajo na zaposlene (v obeh primerih prednjači vodstvo DEUUP-ja, saj se zaposleni strinjajo s trditvijo v več kot 80 %). Ugotovitve so zanimive, saj odgovori nakazujejo, da je vloga menedžmenta na DEUUP-ju večja kot na DID-u oz., da je menedžment DEUUP-ja bolj aktiven pri vzdrževanju informacijske varnosti. Slabše ocenjena vloga vodstva na DID-u se zrcali tudi v nižjem strinjanju zaposlenih s predpostavko, da ima organizacija izdelan varnostni načrt na področju IKT-ja, zapisana pravila (politike) informacijske varnosti in predpisana pravila o tem, kako poročati v primeru nezgod. Čeprav so merjene spremenljivke v splošnem ocenjene nadpovprečno, je potrebno poudariti, da je v primerih, ko prihaja do razlik med ocenami enega in drugega direktorata, stanje boljše v okolju DEUUP-ja, kot DID-a. Vzroke za razlike

med direktoratoma je potrebno iskati v organizaciji sami in za bolj jasno sliko še podrobneje analizirati obstoječe stanje. V okviru svojih raziskovalnih zmožnosti lahko namreč izpostavim le določene dejavnike, ki bi potencialno imeli moč vplivanja na točnost rezultatov. Te vidim zlasti v času, ko je bila raziskava izvedena, saj je potekala v poletnem času[14], ko so ljudje morda nekoliko manj razpoloženi za sodelovanje v raziskavah in posledično tudi manj natančno odgovarjajo na dana vprašanja[15]. Poleg tega so se za sodelovanje v raziskavi morda odločili predvsem tisti posamezniki, ki so do obstoječe ureditve bolj kritični, kot bi bilo realno potrebno. Primerjalno gledano so namreč zaposleni na DID-u v večji meri pripisovali komentarje oz. dajali pripombe na sam vprašalnik kot zaposleni na DEUUP-ju, kar je seveda lahko svojevrsten indic, da so zaposleni na DID-u bolj kritični, lahko pa tudi indic za večjo občutljivost za odgovarjanje na vprašanja v povezavi z občutljivim področjem zagotavljanja informacijske varnosti.

Izsledki raziskave kažejo, da so organizacijski in skupinski dejavniki močni napovedovalci varnostnega vedenja oz. osveščenosti in etičnosti posameznikov. 61,2 % variacij znotraj posameznikove etičnosti je pojasnjenih z indikatorji: analiza tveganj, proračun in zaupanje. Medtem ko 52,1 % variacij posameznikovega varnostnega zavedanja pojasnjujejo politike in postopki ter proračun. Rezultati kažejo, da je mogoče spremembe pri vedenju posameznikov izzvati s pomočjo povečane osredotočenosti na to, kako jasno so zapisane in kaj vse določajo politike in pravila v organizaciji. Pri tem pa je seveda pomembno, da se o njih govori vsakodnevno (varnost tako postane normalna tema pogovorov) in je do njih enostavno tudi priti oz. jih pridobiti v obliki kopije. Na individualno raven informacijske varnostne kulture vpliva tudi analiziranje potencialnih tveganj, ki omogoča seznanitev z varnostno šibkimi ali ogroženimi področji dela in vpliva na to, da so posamezniki pri določenih segmentih dela bolj previdni. Zanimivo je v regresijski analizi izpostavljen tudi dejavnik proračuna, kar kaže na to, da finančna sredstva, ki so namenjena višanju stopnje varnosti, vplivajo na to, kako zaposleni dojemajo svoj del odgovornosti in skrb za informacijsko varnost. Omeniti je potrebno še dejavnik zaupanja med zaposlenimi in vodstvom, ki ima pomembno vlogo pri tem v kolikšni meri bodo zaposleni spoštovali etična načela in težili k visoki stopnji

[14] Na tem mestu bi želela opozoriti na to, da so imeli anketiranci ravno zaradi poletnega meseca in časa dopustov za sodelovanje v raziskavi na voljo štiri tedne. Zaradi relativno nizke udeležbe so bili tudi večkrat zaprošeni za sodelovanje, a se nekateri vseeno niso odločili za sodelovanje.

[15] Čeprav bi sama od IKT-strokovnjakov vseeno pričakovala, da jih v primerjavi z ostali poklici še bolj zanima, kako sodelavci ocenjujejo lastno kulturo, kot tudi to, da so v večji meri pripravljeni potrditi za zboljšanje pomanjkljivosti. V spremni besedi vprašalnika je bilo namreč zapisano, da se bodo zaposleni lahko seznanili z rezultati v kolikor bodo to želeli.

integritete. Posamezniki, ki so že dlje časa zaposleni na direktoratu se v večji meri zavedajo informacijske-varnostne problematike, kot posamezniki, ki so na direktoratu zaposleni krajši čas. Poleg tega je razsežnost njihovega varnostnega zavedanja odvisna tudi od tega, ali so zaposleni na vodstvenem delovnem mestu ali na ostalih delovnih mestih. Vodstveni kadri se namreč v večji meri zavedajo problemov, kot njihovi sodelavci, ki so v podrejenem odnosu.

Pri glavnih ugotovitvah je potrebno omeniti tudi to, da zaposleni niso v zadostni meri seznanjeni s tem, kakšni ukrepi obstajajo v njihovi organizaciji za primer kršitev varnostnih predpisov in ne morejo potrditi, da so vsi zaposleni dovolj dobro seznanjeni s tveganji zaradi katerih je varovanje zaupnih podatkov potrebno.

## 6.3 OBRAVNAVA HIPOTEZ IN UGOTOVITVE

V nalogi sem si zastavila dve hipotezi, ki sem ju preverjala z empirično raziskavo med zaposlenimi v državni upravi, natančneje med zaposlenimi na DEUUP-ju in DIF-u. Na podlagi rezultatov raziskave lahko ugotovim sledeče:

***Hipoteza št.1: Informacijska varnostna kultura je v izbranih organih državne uprave na zadovoljivi ravni – to pomeni, da se uslužbenci zavedajo problemov varnosti.***

***Ugotovitev:***

Hipotezo sem preverjala z devetimi komponentami oz. indikatorji informacijske varnostne kulture, ki se razvrščajo na treh organizacijskih ravneh. Rezultati kažejo, da so vsi indikatorji ocenjeni nadpovprečno visoko, saj povprečne vrednosti vseh indikatorjev presegajo oceno 3. Zaradi tega lahko hipotezo št. 1 sprejmem in ugotovim, da je informacijska varnostna kultura v izbranih organih državne uprave na več kot zadovoljivi ravni, pravzaprav celo na nadpovprečno visoki ravni. Je pa pri potrditvi hipoteze potrebno omeniti relativno razpršenost odgovorov (standardni odklon se giblje od 0,43 do 0,90), kar pomeni, da so bili nekateri izmed anketirancev, kljub dobri povprečni oceni, precej kritični do posameznih kazalcev.

Rezultati niso nepričakovani, saj se v organizaciji, ki skrbi za razvoj temeljnih informacijsko-komunikacijskih sistemov, že v osnovi zahteva visoka stopnja odgovornosti pri varovanju

občutljivih informacij. Ta se mora kazati tako na organizacijski ravni (v obliki predpisanih politik in predpisov, konstantnih primerjav delovnih procesov s podobnimi organizacijami, proučevanj potencialnih tveganj in razporejanj proračunskih sredstev v luči podpore IKT-procesom), kot na skupinski (preko vedenja, odločitev in aktivnosti menedžmenta ter ustvarjanja zaupanja) in individualni ravni (v obliki posameznikove osveščenosti, razumevanja etičnih razsežnosti uporabe IKT-ja in pripravljenosti ali prilagodljivosti na spremembe).

***Hipoteza št. 2*: *Pozitivno ocenjeni indikatorji informacijske varnostne kulture na organizacijski in skupinski ravni vplivajo na pozitivno oceno indikatorjev na individualni ravni.***

***Ugotovitev:***

Hipotezo sem preverjala s korelacijsko analizo povezanosti posameznih indikatorjev, ki je odgovorila, kako močno se indikatorji med sabo povezujejo in z multiplo regresijsko analizo, s katero sem določala vpliv posameznih indikatorjev na druge. Rezultati kažejo, da se indikatorji med sabo relativno močno povezujejo (izmed 36 izračunanih povezav, jih je 26 statistično značilnih), kar kaže na to, da so med sabo močno prepleteni in jih ni mogoče opredeliti kot relativne samostojne gradnike informacijske varnostne kulture.

Hipotezo lahko delno potrdim, saj na individualno raven statistično značilno vplivajo štirje indikatorji, trije iz organizacijske in eden iz skupinske ravni. Pri ostalih indikatorjih namreč ni zaznati pomembnega vpliva. Individualno raven sestavljata indikatorja etičnosti in zavedanja. Na indikator etičnost statistično značilno vplivajo trije indikatorji, in sicer: analiza tveganj, proračun in zaupanje ter ga pojasnjujejo v več kor 60 %. Na indikator zavedanje pa vplivata indikatorja politike in postopki ter proračuna, ki pojasnjujeta več kot 50 % variance indikatorja. Poleg tega na posameznikovo zavedanje razsežnosti informacijske varnosti vplivata tudi čas zaposlitve v sedanji organizaciji in delovno mesto. Posamezniki, ki so že dlje časa zaposleni na direktoratu, se v večji meri zavedajo informacijske-varnostne problematike, kot posamezniki, ki so na direktoratu zaposleni krajši čas. Poleg tega je razsežnost njihovega zavedanja odvisna tudi od tega, ali so zaposleni na vodstvenem delovnem mestu ali na ostalih delovnih mestih. Vodstveni kadri se namreč v večji meri zavedajo problemov kot njihovi sodelavci, ki so v podrejenem odnosu.

Ob delni potrditvi hipoteze lahko ugotovimo, da je na vedenje posameznika v veliki meri mogoče vplivati s pomočjo sprememb na organizacijski in skupinski ravni. Direktorata bosta največ sprememb pri vedenju zaposlenih dosegla preko uvajanja sprememb, ki se nanašajo na področje urejenosti, vidnosti in dostopnosti politik in postopkov, s pomočjo vidnega in jasnega opredeljevanja tveganj, proračunskih postavk, ki bodo namenjene krepitvi informacijske varnostne kulture, in preko višanja medsebojnega zaupanja.

## 6.4 PRIPOROČILA ZA SPREMINJANJE IN IZBOLJŠANJE INFORMACIJSKE VARNOSTNE KULTURE

V tem delu bi želela podati priporočila, ki so usmerjena k izboljšanju informacijske varnostne kulture v reprezentativnih organih državne uprave. Na osnovi rezultatov statističnih obdelav zbranih podatkov predlagam naslednja priporočila:

***1. Priporočam, da vodstvo nameni več pozornosti temu, kako voditi z zgledom.***

Vloga vodstva je v splošnem dobro ocenjena in zaposleni poročajo o visoki stopnji obojestranskega zaupanja. Več kot 80 % zaposlenih namreč poroča, da zaupajo svojemu neposredno nadrejenemu vodji oz. da jim tudi neposredno nadrejeni vodja zaupa. Zaupanje do višjega vodstva oz. menedžmenta je ocenjeno nekoliko nižje, a je še vedno v visokem povprečju. Zaupanje vodstvu tako predstavlja kakovostno osnovo za uvajanje sprememb, saj lahko pripomore k hitrejšemu sprejemanju oz. posnemanju ravnanj brez pomislekov o njihovi dejanski smotrnosti. Kljub temu pa je potrebno to zaupanje, ki si ga vodstvo in zaposleni izkazujejo, nadgraditi še s poudarjenim pristopom k vodenju, ki mu pravimo vodenje z zgledom. Voditi s svojim zgledom pomeni voditi, spodbujati in podpirati zaposlene z dobrim delom, namenjati jim pozornost in vzeti si čas zanje, imeti odgovoren odnos do delovnih nalog v vsakem delu dneva ne glede na njihovo zahtevnost, hkrati pa zasledovati visoko stopnjo lastne integritete ter si prizadevati za visoko stopnjo integritete drugih. Vodenje z zgledom je potrebno okrepiti, saj komaj nekaj več kot 50 % zaposlenih meni, da daje vodstvo s svojim ravnanjem ustrezen zgled ostalim za varovanje zaupnih podatkov in da organizacija skrbi dovolj dobro za to, da zaposleni spoštujejo in upoštevajo informacijsko-varnostna pravila. Slabo je ocenjena tudi ažurnost odzivanja na pobude, ki prihajajo s strani zaposlenih in so namenjene izboljšanju varovanja zaupnih podatkov – z dobro ažurnostjo vodstva se namreč strinja le 40 % anketirancev.

***2. Priporočam spodbujanje zaposlenih k redni udeležbi na seminarjih, ki so namenjeni usposabljanju in izobraževanju s področju krepitve informacijske varnostne kulture.***

Zaposleni se načeloma čutijo osebno odgovorne za vzdrževanje visoke stopnje informacijske varnosti, a zanimivo niso popolnoma prepričani, da mora vsak posameznik tudi dejansko odgovarjati za neupoštevanje oz. zlorabo pravil o varovanju občutljivih informacij. Če se vodstveni kadri v celoti strinjajo, da je neupoštevanje pravil potrebno kaznovati, je pri ostalih mogoče zaznati, sicer majhno, a vseeno opazno negotovost. To bi se lahko glede na ocene zaposlenih verjetno dalo povezovati z relativno nizkim trudom vodstva po spodbujanju spoštovanja in upoštevanja predpisov, kar sem ugotovila v okviru prvega priporočila. Zato priporočam, da organizacija svoje zaposlene v prihodnje pogosteje vključuje v programe, seminarje in podobne oblike usposabljanj, ki krepijo informacijsko-varnostno osveščenost. Zaposleni so se ob primerni spodbudi verjetno pripravljeni redno udeleževati tovrstnih oblik izobraževanj, saj jih je več kot 80 % mnenja, da je izobraževanje s področja informacijske varnosti za zaposlene potrebno ter da je za dvig ravni pomembno predvsem periodično usposabljanje.

***3. Priporočam temeljitejše seznanjanje zaposlenih z varnostnimi politikami in pravili, ki so sprejeta in veljajo v organizaciji.***

V prvo skupino dejavnikov, ki imajo močan vpliv na vedenje ljudi, spada primerno in učinkovito posredovanje dogovorjenih varnostnih pravil. Ta omogočajo, da se posamezniki vedejo v skladu s pričakovanji organizacije in se znajo ob slučaju incidenta tudi primerno odzvati. V kolikor zaposleni niso seznanjeni s temi pravili oz. niso niti prepričani, da le ta v organizaciji tudi obstajajo, lahko takšno stanje predstavlja resno grožnjo vzdrževanju informacijske varnosti. Rezultati namreč kažejo na to, da zaposleni veliko prepogosto kot bi še bilo sprejemljivo, ne vedo odgovora na nato, ali ima njihova organizacija izdelan varnostni načrt na področju informacijske varnosti, ali ima zapisana pravila (politike) informacijske varnosti in kje najti pravila o tem, kako ustrezno poročati o nezgodah, ki so v povezavi z informacijsko varnostjo. Odgovor, kako doseči izboljšanje na tem področju, je mogoče razbrati že iz samih rezultatov raziskave, tj. s temeljitejšim seznanjenjem zaposlenih in zlasti z enostavnejših dostopom do kopij dokumentov, ki obstajajo v njihovi organizaciji.

***4. Priporočam več interne komunikacije in individualnega osredotočanja na zaposlene.***

Intenzivnejša komunikacija bo odpravila nejasnosti pri razumevanju internih predpisov, individualno osredotočanje na posameznike (posameznik kot dragocen intelektualni kapital)

pa pripomoglo k manjši razpršenosti odgovorov, ki se nanašajo na obstoječe stanje informacijske varnostne kulture. Kljub načeloma spodbudnim rezultatom je namreč potrebno izpostaviti precejšno kritičnost nekaterih posameznikov do posameznih področij varovanja informacij. To pa seveda lahko otežuje usklajenost individualnih ciljev in vrednot s cilji in vrednotami organizacije ter zahteva pripravo ukrepov, ki bodo informacijsko varnostno kulturo okrepili sorazmerno med vsemi zaposlenimi. Načinov za to je več, nekateri izmed njih so omenjeni v prejšnjih priporočilih, drugi pa v teoretičnem delu naloge.

# 7 ZAKLJUČEK

V magistrski nalogi sem proučevala informacijsko varnostno kulturo v državni upravi, natančneje v okviru dveh direktoratov, Direktorata za e-upravo in upravne procese in Direktorata za informacijsko družbo. Kot sem omenila že v uvodu naloge, sem direktorata izbrala zaradi njune neposredne povezanosti z informacijsko-komunikacijskimi procesi, hkrati pa tudi zaradi tega, ker preko svojih osrednjih dejavnosti močno prispeta k razvijanju informacijske družbe. V proučevano populacijo sem zajela primarni segment zaposlenih, torej tiste posameznike, ki se vsakodnevno ukvarjajo z IKT področjem (v proučevano populacijo nisem zajela oseb, ki nimajo neposrednega opravka z IKT-jem, večinoma je bilo to administrativno osebje) in dejansko predstavljajo tisti del ljudi v državi, ki bi morali biti z vidiki zagotavljanja informacijske varnosti najbolj seznanjeni. Razlog, da sem se odločila za proučevanje informacijske varnostne kulture na populaciji strokovnjakov za IKT, leži tudi v predpostavki, da je večina IKT-strokovnjakov že po naravi bolj tehnično usmerjena in da jih ima veliko izmed njih tudi tehnično izobrazbo. To pomeni, da zaradi svoje tehnične usmerjenosti, če se izrazim metaforično, pogosto med posameznimi drevesi ne vidijo gozda. Spregledajo pomembnost organizacijskih elementov na podlagi katerih in zaradi katerih tehnologija sploh deluje oz. je ustvarjena. Poleg IKT-strokovnjakov so proučevano populacijo predstavljali tudi vodstveni kadri. Ti so bili v populacijo zajeti zaradi osrednje in pomembne vloge, ki jo imajo v direktoratih, pa tudi zaradi osebnega mnenja, da se skrb za varnost v organizacijah prične na ravni vodstva. Kajti, če se zdi področje informacijske varnostne kulture nepomembno vodstvenim kadrom, je težko pričakovati, da bodo imeli nižji kadri drugačen odnos. Temu pritrjujejo tudi izsledki literature, ki ugotavljajo, da je najpomembnejše prepričanje v organizaciji, prepričanost zaposlenih in organizacije same, da je varnost pomembna (Connolly 2000 v Ruighaver, Maynard in Chang 2007, 57).

Rezultati raziskave kažejo, da zaposleni ocenjujejo vsebinske sklope informacijske varnostne kulture v izbranih direktoratih nadpovprečno visoko. Na podlagi tega lahko sklepam, da so ukrepi, ki so nujno potrebni za zagotavljanje informacijske varnosti, vzpostavljeni v zadostni meri in v organizaciji načeloma naj ne bi bilo institucionalno-normativnih ovir, ki bi oteževale implementacijo varnostnih načel. Nekoliko več pozornosti pa bi bilo potrebno nameniti odgovoru na vprašanje, kakšna je vloga vodstva pri upravljanju z informacijsko varnostno kulturo, saj je izmed vseh indikatorjev njegova vloga najslabše ocenjena. Kljub temu, da se

odgovornost za razvoj kulture nahaja na različnih organizacijskih ravneh, tako na ravni celotne organizacije, kot na ravni skupin in posameznikov, je pomembno izpostaviti predvsem naloge, ki so v domeni vodenja in upravljanja. Menim, da si mora vodstvo v večji meri prizadevati za povečanje znanja in varnostne osveščenosti svojih zaposlenih, tako preko lastnega zgleda, odkrite komunikacije, kot tudi preko ciljno usmerjene razporeditve finančnih sredstev. Večina zaposlenih na direktoratih je visoko izobražena in bi morala že s strokovnega vidika poznati vsaj najbolj ključna varnostna tveganja v organizaciji. Zaradi tega predvidevam, da je tisto, kar manjka zapisanim pravilom, predvsem njihova ponotranjenost in vedenje v skladu z njimi. Če v času post-fordistične družbe veliko beremo o integriteti, si upam trditi, da je vsaj toliko primanjkuje tudi v praksi. Varnostna pravila ni mogoče enostavno zapakirati v obliko dokumenta, nanj gledati kot na sredstvo za hitre spremembe in ga servirati z namenom vsestranskega upoštevanja in spoštovanja. Menim, da je tisto, kar manjka črkam na papirju predvsem izkustvo in skladnost misli z dejanji. Tega primanjkuje tako zaposlenim, kot tudi vodstvu. In neodgovorno ter neetično bi bilo reči, da spremenjene oblike varnostih groženj zahtevajo nove ljudi na odgovornih delovnih mestih (te uslužbenci državne uprave zagotovo zasedajo), saj je ravno nasprotno: sodobne oblike ogrožanj varnosti pogojujejo le intenziviranje postopkov za upravljanje z informacijsko varnostno kulturo. Vse kar potrebujemo za učinkovit boj, ob predpostavki nenehnega tehnološkega razvoja, že imamo, premalo izurjeni so le naši bojevniki. Raje kot špartanske vzgoje, bi jim bilo potrebno vliti več samurajskega duha, kjer velja, da se tisto, kar se nosi za pasom, nosi tudi v srcu.

# 8 LITERATURA


**A**

1. Albright, David. 1999. *What happened in Japan: The Tokaimura Criticality Event. ISIS Reports*. Dostopno prek: http://isis-online.org/isis-reports/detail/what-happened-in-japan-the-criticality-event/ (24. februar 2010).
2. Alfawaz, Salahuddin, Nelson Karen in Mohannak Kavoos. 2010. *Information security culture: a behaviour compliance conceptual framework.* Prispevek predstavljen na Australasian Information Security Conference, 18.-21. januarja, v Brisbane, Avstralija.
3. Antonsen, Stian. 2009. *Safety culture: theory, method and improvement*. FARNHAM, Burlington (VT): Ashgate company.

**B**

4. Bajpai, Kanti. 2000. *Human Security: Concept and Measurement*. Knoc Institute Occasional Paper (Number 19). University of Notre Dame, Indiana. Dostopno prek http://www.hegoa.ehu.es/dossierra/seguridad/Human_security_concept_and_measurement.pdf (24. 5. 2010).
5. Bakhshi, Taimur, Maria Papadaki in Steven Furnell. 2009- Social engineering: assessing vulnerabilities in practice. *Information Management & Computer Security*, 17 (1), 53-63.
6. Benson, Christipher, Denis Bensch, Dawie Human, Louis De Klerk in Johan Grobler. 2010. *Security Threats. Microsoft Corporation.* Dostopno prek: http://technet.microsoft.com/en-us/library/cc723507.aspx#XSLTsection124121120120 (15. maj 2010).
7. Brezovšek, Marjan. 2004. Različni pristopi k proučevanju upravne kulture in vrednot v javni upravi. V *Upravna kultura*, ur. Marjan Brezovšek in Miro Haček, 11-39. Ljubljana: Fakulteta za družbene vede.

**C**

8. Chang, Shurchih Ernest in Lin Chin-Shien. 2007. Exploring organizational culture for information security management. *Industrial Management & Data Systems*, 107 (3), 438-458.
9. Chevreau, François-Régis. 2006. Dafety culture as a rational myth: why developing safety culture implies engineering resilience? V *Proceedings of the second resilience engineering symposium*, ur. Erik Hollnagel in Eric Rigaud, 63-73. Antibes, Juan-les-

Pins, Paris: Mines Paris, Les Presses. Dostopno prek: http://www.resilience-engineering.org/REPapers/Chevreau_R.pdf (10. junij 2010).

10. Choudhry, Rafiq M., Dongping Fang in Sherif Mohamed. 2007. The nature of safety culture: A survey of the state-of-the-art. *Safety Science*, 45 (10), 993-1012.
11. Computer Security Institute. 2009. *CSI Computer Crime and Security Survey*. Dostopno prek: http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey09_Executive-Summary.pdf (21. januar 2010).
12. Cooper, M. Dominic. 2000. Towards a model of safety culture. *Safety Science*, 36 (2): 111-136.

**D**

13. Da Veiga, Adele in Jan H. P. Eloff. 2010. A framework and assessment instrument for information security culture. *Computers & Security*, 29 (2), 196-207.
14. Dhillon, Gurpreet in Backhouse, James. 2001. Current directions in IS security research: towards soxio-organizational perspectives. *Info Systems* 11(2): 127-153.
15. Dlamini, M.T., Jan H.P. Eloff in Mariki M. Eloff. 2009. Information security: The moving target. *Computers & Security 28 (3-4): 189-198.*
16. Dvoršak, Andrej in Bojan Dobovšek. 2009. Pojavne oblike kriminalitete v informacijsko komunikacijski tehnologiji – računalniška in internetna kriminaliteta. V *Transnacionalna kriminaliteta*, ur. Bojan Dobovšek, 433-495. Ljubljana: Fakulteta za varnostne vede.

**E**

17. ENISA, European Network and Information Security Agency. 2007. *Pobude za ozaveščanje o varnosti informacij: Sedanja praksa in merjenje uspeha*. Heraklion: ENISA, European Network and Information Security Agency. Dostopno prek: http://www.enisa.europa.eu/act/ar/deliverables/2007 (19. januar 2010).
18. Eriksson, Johan in Giampiero Giacomello. 2006. The Information Revolution, Security, and International Relations: (IR)relevant Theory? *International Political Science Review* 27(3): 221-244.
19. Eurostat, European Commisson. 2009. *European business - Facts and figures*. Dostopno prek: http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/KS-BW-09-001/EN/KS-BW-09-001-EN.PDF (19. januar 2010).

**F**

20. Fleming, Mark in Ronny Lardner. 1999. Safety culture – the way forward. *The Chemical Engineer*. Dostopno prek: /www.keilcentre.co.uk/Data/Sites/1/Culture.pdf (1. januar 2010).

**G**

21. Guldenmund, Frank W. 2000. The nature of safety culture: a review of theory and research. *Safety Science* 34(1-3): 215-257.
22. Guldenmund, Frank W. 2007. The use of questionnaires in safety culture research – an evaluation. *Safety Science*, 45 (6), 723-743.
23. Grizold, Anton. 2005. *Slovenija v spremenjenem varnostnem okolju: k razvoju obrambno-zaščitnega sistema: izzivi in spodbude*. Ljubljana: Fakulteta za družbene vede.
24. Grošelj, Klemen. 2007. *Slovenija v svetu mirovnih operacij*. Ljubljana: Fakulteta za družbene vede.

**H**

25. Herath, Tejaswini in H. Raghav Rao. 2009. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision support systems*, 47 (2), 154-165.
26. Hertsgaar, Mark. 2004. *Three Mile Island. The Notion*. Dostopno prek: http://www.thenation.com/doc/20040405/hertsgaard (23. februar 2010).
27. Hopkins, Andrew. (2006). Studying organisational cultures and their effects on safety. *Safety Science*, 44 (10): 875-889.
28. Howard, Brett, Oliver Paridaens in Bernhard Gamm. 2009. Information security: threats and protection mechanisms. *Alcatel Telecommunications Review* - 2nd Quarter, 117-121. Dostopno prek: http://lt.fe.uni-lj.si/gradiva/kos/clanki_pdf/28-information%20security%20-%20threats%20and%20protection%20mechanisms.pdf (15. maj 2010).
29. Hudson, Patrick. 1999. *Safety Culture-Theory and Practice. RTO HFM.* Workshop on »The Human Factor in System Reability- Is Human PERFORMANCE Predictable?« Dostopno prek:: http://ftp.rta.nato.int/public//PubFulltext/RTO/MP/RTO-MP-032///MP-032-$$TOC.pdf (21. januar 2010).

**I**

30. International Civil Aviation Organization (2005). *ICAO Safety Management Manual.* Dostopno prek: http://www.cao.ir/farsi/sms/Document/9859.pdf. (25. januar 2010)

31. International Civil Aviation Organization (2009). *ICAO State Safety Programme (SSP) Implementation Course. Module N° 2 Basic safety management concepts*. PowerPoint predstavitev dobljena 25. 2. 2010 na: http://www2.icao.int/en/acip/Documents/Safety%20Management/2008/SMS%20Workshop/Modules/ICAO%20SMS%20Module%20N%C2%B0%202%20%E2%80%93%20Basic%20safety%20concepts%202008-11%20%28E%29.pdf.
32. International Telecommunication Union. 2010. *Measuring the Information Society*. Geneva: International Telecommunication Union. Dostopno prek: http://www.itu.int/ITU-D/ict/publications/idi/2010/Material/MIS_2010_without%20annex%204-e.pdf (15. maj 2010).

**J**

33. Jackson, Robert in Georg Sørenses. 2007. *Introduction to international relations: theories and approaches.* Third Edition. Oxford, New York: Oxford University Press.

**K**

34. Kletz, Trevor. 2001. *Learnings from Accidents*. Third Edition. Oxford: Gulf Professional Publishing.
35. Knapp, Kenneth J. in Thomas E. Marshall.2007. Top management support Essential for effective information security. V *Information Security Management Handbook, Sixth Edition*, ur. Harold F. Tipton Micki Krause, 51-58. Boca Raton: Auerbach Publications.
36. Košmrlj, Rudi. 1982. *Varnostna kultura v sistemu družbene samozaščite*. Diplomska naloga. Ljubljana: Fakulteta za družbene vede.
37. Kraemer, Sara, Pascale Carayon in John Clem. 2009. Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computers & Security* 28 (7), 509-520.
38. Kuusisto, Tuija in Ilona Ilvonen. 2003. Information security culture in small and medium size enterprises. *Frontiers of e-business research*, 431-439. Dostopno prek: http://www.ebrc.info/kuvat/431-439.pdf (25. 5. 2010).

**L**

39. Lamy, Steven L. 2007. Sodobni večinski pristopi: neorealizem in neliberalizem. V *Globalizacija svetovne politike: uvod v mednarodne odnose*, ur. John Baylis in Steve Smith, 263-290. Ljubljana: Fakulteta za družbene vede.

40. Leach, John. 2003. Improving user security behaviour. *Computers & Security*, 22 (8), 685-692.
41. Lim, Joo Soon, Shanton Chang, Sean Maynard in Atif Ahmad. 2009. *Exploring the Relationship between Organizational Culture and Information Security Culture*. Prispevek predstavljen na 7th Australian Information Security Management Conference, 1.-3. decembra, v Perthu, Zahodna Avstralija.
42. Lobnikar, Branko, Denis Čaleta, Miroslav Žaberl, Andrej Anžič in Katja Rančigaj. 2009. *Varnostna in organizacijska kultura v Slovenski vojski z vidika upravljanja s tajnimi podatki : končno poročilo raziskovalne skupine Fakultete za varnostne vede*. Ljubljana: Fakulteta za varnostne vede.

**M**

43. Mackenzie, Kate. 2006. Employees may be opening the door to criminals. Financial Times Limited. Dostopno prek: http://www.ft.com/cms/s/458807fe-efec-11da-b80e-0000779e2340.html (20. 5. 2010)
44. Malešič, Marjan. 1994. Tri teoretične perspektive sodobne varnosti. *Javnost* 1(4): 97-104.
45. Marinšek, Damijan. 2009. Informacijska varnostna politika javne uprave. Prispevek predstavljen na Informatika v javni upravi, 7.-8. decembra, v Brdu pri Kranju, Ljubljana.
46. Martins, Adéle. 2002. *Information Security Culture*. Master's dissertation. Johannesburg: Rand Afrikaans University.
47. Mengoli, Anna in Luigi Debarberis. 2007. Effectiveness evaluation methodology for safety processes to enhance organisational culture in hazardous installations. *Journal of Hazardous Materials*, 155 (1-2), 243-252.
48. Mesner-Andoljšek, Dana. 1995. *Organizacijska kultura.* Ljubljana: Gospodarski vestnik.
49. Ministrstvo za javno upravo. 2010. Dostopno prek: http://www.mju.gov.si/index.php?id=132 (30. junij 2010).
50. Ministrstvo za visoko šolstvo, znanost in tehnologijo. 2010. Dostopno prek: http://www.mvzt.gov.si/si/delovna_podrocja/informacijska_druzba/ (30. junij 2010).
51. Moravcsik, Andrew. 1997. Talking Preferences Seriously: A Liberal Theory of International Politics. *International Organisation* 51(4): 513-553.

**O**

52. Organizacija za gospodarsko sodelovanje in razvoj. 2002. *OECD Guidelines for the Security of Information Systems and Networks*. Dostopno prek: http://www.oecd.org/dataoecd/16/22/15582260.pdf (30. maj 2010).

**P**

53. Pagon, Milan. 2004. Razvoj organizacijske kulture v javnem sektorju. *HRM*. 2(3), 50-54.
54. Parker, Dianne, Lawrie Matthew in Patrick Hudson. 2006. A framework for understanding the development of organisational safety culture. *Safety Science*, 44 (6), 551-562.
55. Prezelj, Iztok. (2001). Grožnje varnosti, varnostna tveganja in izzivi v sodobni družbi. *Teorija in praksa*, 38, (1): 127-141.
56. Prezelj, Iztok (2002). Konceptualizacija nacionalnih varnostnih interesov. *Teorija in praksa*, 39 (4): 621-637.
57. Prezelj, Iztok. 2005. *Nacionalni sistemi kriznega menedžmenta*. Ljubljana: Fakulteta za družbene vede.

**R**

58. Rao, Suman. 2007. Safety culture and accident analysis - A socio-manage,ent approac based on organizational safety social capital. *Journal of Hazardous Materials* 142 (3), 730- 740.
59. Rheea, Hyeun-Suk, Cheongtag Kimb inYoung U. Ryuc. 2009**.** Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security*, 28 (8), 816-826.
60. Rizman, Rudi. 1992. Intelektualni temelji liberalizma. V *Zbornik – Sodobni liberalizem,* ur. Rudi Rizman,15-29 Ljubljana: Knjižna zbirka Krt.
61. Ruighaver, Antonie B., Sean B. Maynard in Shanton Chang. 2007. Organisational security culture: Extending the end-user perspective. *Computers & Security*, 26 (1), 56-62.

**S**

62. Schein, Edgar H. 2004. *Organizational Culture and Leadership* (3rd ed.), San Francisco, Jossey: Bass Publishers.
63. Schlienger, Thomas in Stephanie Teufel. 2005. Tool supported management of information security culture. V *Security and Privacy in the Age of Ubiquitous*

*Computing*, ur. Ryoichi Sasaki, Sihan Qing in Hiroshi Yoshiura, 65-77. Boston: Springer.

64. SecureInfo Corporation. 2007. *Information Security Awareness Report. The Government Workers' perspective*. Dostopno prek: http://www.secureinfo.com/downloads/reports/SecureInfo-InfoSec-Report-Dec-2007.pdf (15. julij 2010)
65. Shaluf, Ibrahim Mohamed. 2008. Technological disaster stages and management. *Disaster Prevention and Management*, 17 (1), 114-126.
66. Shaw**,** Ruey Shiang, Charlie Charlie C. Chen, Albert L. Harris in Hui-Jou HUang. 20009. The impact of information richness on information security awareness training effectiveness. *Computers & Education*, 52 (1), 92-100.
67. Smith, Tomas. A. 2009. *Culture, Teams and Safety Management: Preparing for the NewManagement Model*. Dostopno prek: http://www.mocalinc.com/sitebuildercontent/sitebuilderfiles/cultureeamssafety.pdf. (18. januar 2010).
68. Svete, Uroš. 2005. *Varnost v informacijski družbi*. Ljubljana: Fakulteta za varnostne vede.
69. Svete, Uroš. 2006. Informacijsko-komunikacijska tehnologija in sodobne varnostne teorije. V *Varnost v postmoderni družbi*, ur. Marjan Malešič, 47-67. Ljubljana: Fakulteta za družbene vede.

**T**

70. Treven, Sonja. 2001. *Mednarodno organizacijsko vedenje.* Ljubljana: GV Založba.

**U**

71. Ullman, Richard. 1983. Redefining security. *International Security* 8(1): 129-153.
72. United Nations. 2004. *A More Secure World: Our Shared Responsibility: Report of the Secretary-General's High-level Panel on Threats, Challenges and Change.* New York: United Nations.

**V**

73. van Niekerk, Johan in Rossouw von Solms. 2006. Understanding information security culture. a conceptual framework. Johanesburg: Information Security South Africa (ISSA). Dostopno prek: *icsa.cs.up.ac.za/issa/2006/Proceedings/Full/21_Paper.pdf (25. 5. 2010).*
74. van Niekerk, Johan in Rossouw von Solms. 2010. Information security culture: A management perspective. *Computers & Security*, 29 (4), 476-486.

75. van Vuuren, Wim. 2000. Cultural influences on risks and risk management: six case studies. *Safety Science*, 34(1-3), 31-45.

76. Vroom, Cheryl in Rossouw von Solms. 2004. Towards information security behavioural compliance. *Computers & Security*, 23 (3), 191-198.

**W**

77. Wagner, Andreas in Carole Brooke.2007. Wasting Time: The Mission Impossible with Respect to Technology-Oriented Security Approaches. *The Electronic Journal of Business Research Methods*, 5 (2), 117-124.

78. Wiegmann, Douglas A., Hui Zhang, Terry von Thaden, Gunjan Sharma in Alyssa Mitchell. 2002. *A Synthesis of Safety Culture and Safety Climate Research*. *Technical Report ARL-02-3/FAA-02-2*. Savoy, Illinois: University of Illinois at Urbana-Champaign. Dostopnp prek: http://www.humanfactors.uiuc.edu/Reports&PapersPDFs/TechReport/02-03.pdf (20. januar 2010).

79. Workman, Michael. 2008. A test of interventions for security threats from social engineering. *Information Management & Computer Security*, 16 (5), 463-483.

80. Workman Michael, William H. Bommer in Detmar Straub. 2008. Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers and Human Behavior*, 24 (6), 2799-2816.

**Z**

81. Zakaria, Omar. 2006. Employee Security Perception in Cultivating Information Security Culture. V *Security Management, Integrity, and International Control in Information Systems*, ur. Steve Furnell, Bhavani Thuraisingham, X. Sean Wang in Paul Dowland, 83-92. Boston: Springer.

82. Zhang, Hui, Wiegmann, Douglas A., Terry L. von Thaden, Gurjan Sharma in Alyssa A. Mitchell. 2002. *Safety culture: a concept in chaos*? The Proceedings of the 46th Annual Meeting of the Human Factors and Ergonomics Society. Dostopno prek:http://www.humanfactors.illinois.edu/Reports&PapersPDFs/humfac02/zhawiegvonshamithf02.pdf. (25. februar 2010).

**PRILOGA A: Vprašalnik o informacijski varnostni kulturi**

Spoštovani,

Sem študentka Fakultete za družbene vede v Ljubljani in asistentka na Fakulteti za varnostne vede Univerze v Mariboru in pripravljam magistrsko nalogo o informacijskI varnostni kulturi. Za uspešno izvedbo magistrske naloge potrebujem vaše sodelovanje. Prosim vas, da izpolnite vprašalnik, ki je priložen v nadaljevanju.

Z vprašalnikom vas sprašujem po vašem ***mnenju***, ne pa o stvareh, s katerimi se srečujete pri svojem delu. V vzorec anketiranih ste bili uvrščeni zato, ker ste strokovnjak s področja, ki ga analiziram v svoji magistrski nalogi.

Za izpolnitev vprašalnika boste potrebovali približno 10 minut.

Vaše sodelovanje je prostovoljno in anonimno. Vsi vaši odgovori so zaupne narave, in bodo prikazani le v zbirni obliki, tako da ne bo mogoče ugotoviti odgovore, ki so jih na zastavljena vprašanja dajali posamezniki. Podatke bom uporabila za pripravo magistrske naloge.

Če imate kakršna koli dodatna vprašanja, ali pa če bi vas zanimali rezultati mojega dela, mi lahko pišete na moj elektronski naslov katja.rancigaj@fvv.uni-mb.si.

Za vaše sodelovanje se vam že vnaprej najlepše zahvaljujem.

Katja Rančigaj

**Navodila za izpolnjevanje vprašalnika**

Naslednje trditve se nanašajo informacijsko-varnostno kulturo. Vsako od njih pozorno preberite in se odločite, v kolikšni meri se z njo strinjate. Svoje mnenje označite tako, da obkrožite ustrezno vrednost ob posamezni trditvi. Pri tem 1 pomeni, da se s trditvijo sploh ne strinjate, 5 pa, da se s trditvijo močno strinjate. Ko odgovarjate, imejte v mislih direktorat, v katerem ste trenutno zaposleni.

sploh se ne strinjam 1 2 3 4 5 močno se strinjam

| | | |
|---|---|---|
| 1. | Menim, da je pomembno, da so standardi informacijske varnosti zapisani. | 1 2 3 4 5 |
| 2. | Informacijsko varnost je potrebno obravnavati kot stvar »tehnične zaščite«. | 1 2 3 4 5 |
| 3. | Informacijsko varnost je potrebno obravnavati kot stvar menedžmenta. | 1 2 3 4 5 |
| 4. | Informacijska varnost se v splošnem ukvarja z varovanjem informacij ne glede na obliko: elektronska, papirna ali druga oblika. | 1 2 3 4 5 |
| 5. | Menim, da je izobraževanje s področja informacijske varnosti za zaposlene potrebno. | 1 2 3 4 5 |
| 6. | Osebno me motijo dejanja sodelavcev, ki ne spoštujejo IKT varnostnih določil, predpisanih v organizaciji. | 1 2 3 4 5 |
| 7. | Da bi lahko bili uspešni, je osnovno znanje s področja informacijske varnosti nujno potrebno za vse uslužbence. | 1 2 3 4 5 |
| 8. | Počutim se odgovornega za vzdrževanje visoke stopnje informacijske varnosti v naši organizaciji. | 1 2 3 4 5 |
| 9. | Poznam posameznika (ali skupino) ki je zadolžen za upravljanje z varovanjem informacij v naši organizaciji. | 1 2 3 4 5 |
| 10. | Vodstvo pomaga pri izvajanju dejavnosti, ki se nanašajo na informacijsko varnost v naši organizaciji. | 1 2 3 4 5 |
| 11. | Vsaka organizacija bi morala imeti izdelan načrt informacijske zaščite, ki je prilagojen posebnostim delovanja organizacije. | 1 2 3 4 5 |
| 12. | Za dvig informacijske varnostne kulture je pomembno, da v naši organizaciji organiziramo periodično usposabljanje s tega področja. | 1 2 3 4 5 |
| 13. | V vsaki organizaciji bi morali imeti zapisana pravila o tem, kako poročati o nezgodah, ki so v povezavi z informacijsko varnostjo. | 1 2 3 4 5 |
| 14. | Upravljanje z zaupnimi dokumenti in informacijami je v naši organizaciji primerno z vidika varnosti. | 1 2 3 4 5 |
| 15. | Varnostni ukrepi v naši organizaciji ustrezajo mednarodnim standardom. | 1 2 3 4 5 |
| 16. | Nadzor nad ravnanjem z zaupnimi podatki je v naši organizaciji primeren in primerljiv z ukrepi v podobnih organizacijah. | 1 2 3 4 5 |

| | | | | | | |
|---|---|---|---|---|---|---|
| 17. | V vsaki organizaciji bi morali imeti natančne ukrepe za primer nespoštovanja predpisov s področja varovanja zaupnih podatkov. | 1 | 2 | 3 | 4 | 5 |
| 18. | Vsi zaposleni v organizaciji bi morali biti seznanjeni s tveganji, ki so opredeljena za področje varovanje zaupnih podatkov. | 1 | 2 | 3 | 4 | 5 |
| 19. | V vsaki organizaciji bi moral obstajati utečen postopek, ki zagotavlja, da so vsi zaposleni seznanjeni z določili varovanja zaupnih informacij. | 1 | 2 | 3 | 4 | 5 |
| 20. | Menim, da je potrebno upoštevati pravila informacijske varnosti v organizaciji. | 1 | 2 | 3 | 4 | 5 |
| 21. | Investicije, ki pripomorejo k izboljšanju varovanja informacij, predstavljajo naložbo v prihodnost. | 1 | 2 | 3 | 4 | 5 |
| 22. | Vodstvo spoštuje zasebnost podatkov, ki se nanašajo na zaposlene. | 1 | 2 | 3 | 4 | 5 |
| 23. | Menim, da je potrebno ocenjevati delo, ki ga opravljam, kot del intelektualne lastnine organizacije. | 1 | 2 | 3 | 4 | 5 |
| 24. | Organizacijska struktura, odgovornosti in pristojnosti na področju varovanja podatkov so v naši organizaciji jasno opredeljene in opisane. | 1 | 2 | 3 | 4 | 5 |
| 25. | Verjamem, da med zaposlenimi v naši organizaciji obstajajo posamezniki, ki so pripravljeni za določeno uslugo nepooblaščeno razkriti podatke zaupne narave. | 1 | 2 | 3 | 4 | 5 |
| 26. | Menim, da bi moral biti vsak posameznik osebno odgovoren za neupoštevanje/zlorabo pravil o varovanju informacij v naši organizaciji. | 1 | 2 | 3 | 4 | 5 |
| 27. | V naši organizaciji so tveganja za varovanje zaupnih podatkov zadosti dobro opredeljena. | 1 | 2 | 3 | 4 | 5 |
| 28. | V naši organizaciji je vzpostavljen takšen pretok informacij, ki zagotavlja ustrezno osveščenost zaposlenih v zvezi z varovanjem zaupnih podatkov. | 1 | 2 | 3 | 4 | 5 |
| 29. | Organizacija skrbi za to, da spoštujem in upoštevam informacijsko-varnostna pravila. | 1 | 2 | 3 | 4 | 5 |
| 30. | Menim, da mora proračun organizacije vključevati tudi stroške, ki se nanašajo na zagotavljanje informacijske varnosti v organizaciji. | 1 | 2 | 3 | 4 | 5 |
| 31. | Pripravljen/a sem spremeniti svoje delovne navade, če bi se s tem zagotovila večja varnost informacij s katerimi imamo opravka v organizaciji. | 1 | 2 | 3 | 4 | 5 |
| 32. | Vodstvo se zaveda pomembnosti varovanja informacij s katerimi imamo opravka v organizaciji. | 1 | 2 | 3 | 4 | 5 |
| 33. | Spremembe, ki poskušajo izboljšati informacijsko varnost, so znotraj organizacije sprejete pozitivno (npr. urejeno delovno okolje, uporaba enkripcije, vsakodnevno ustvarjanje varnostnih kopij, itd.) | 1 | 2 | 3 | 4 | 5 |
| 34. | Vodstvo daje s svojim ravnanjem ustrezen zgled zaposlenim za varovanje zaupnih podatkov. | 1 | 2 | 3 | 4 | 5 |

| | | | | | | |
|---|---|---|---|---|---|---|
| 35. | Vodstvo v naši organizaciji dejansko izvaja ukrepe, predvidene za primer neupoštevanja predpisov s področja varovanja zaupnih podatkov. | 1 | 2 | 3 | 4 | 5 |
| 36. | Vodstvo se v naši organizaciji ažurno odziva na pobude podrejenih za izboljšanje varovanja zaupnih podatkov. | 1 | 2 | 3 | 4 | 5 |
| 37. | Zaupam svojemu neposredno nadrejenemu vodji. | 1 | 2 | 3 | 4 | 5 |
| 38. | Moj neposredno nadrejeni vodja mi zaupa. | 1 | 2 | 3 | 4 | 5 |
| 39. | Naša organizacija ščiti avtorske pravice na primeren način. | 1 | 2 | 3 | 4 | 5 |
| 40. | Prepričan sem, da vodstvo zaupa zaposlenim. | 1 | 2 | 3 | 4 | 5 |
| 41. | Vodja me vključuje v sprejemanje odločitev, ki zadevajo moje delovne obveznosti. | 1 | 2 | 3 | 4 | 5 |
| 42. | Prepričan sem, da moji sodelavci moralno obsojajo zlorabo informacij. | 1 | 2 | 3 | 4 | 5 |
| 43. | Na novo sprejeti delavci v naši organizaciji so, po mojem mnenju, dovolj varnostno osveščeni. | 1 | 2 | 3 | 4 | 5 |
| 44. | V naši organizaciji je na voljo dovolj možnosti za dodatna usposabljanja s področja informacijsko-komunikacijske tehnologije (IKT). | 1 | 2 | 3 | 4 | 5 |
| 45. | Informacijsko-komunikacijski sistemi v naši organizaciji se ustrezno prilagajajo zahtevanim standardom varovanja zaupnih podatkov. | 1 | 2 | 3 | 4 | 5 |
| 46. | Naša organizacija spoštuje pravice intelektualne lastnine. | 1 | 2 | 3 | 4 | 5 |
| 47. | Zaupam vodstvu naše organizacije. | 1 | 2 | 3 | 4 | 5 |
| 48. | Pri svojem delu upoštevam načela kodeksov etičnega ravnanja. | 1 | 2 | 3 | 4 | 5 |
| 49. | Menim, da je pomembno upoštevati pravila, ki se nanašajo na prenos informacij z interneta, npr. priponke v e-pošti, sofware, itd. | 1 | 2 | 3 | 4 | 5 |
| 50. | Poznavanje lastnosti in namena obstoječih varnostnih ukrepov (npr. protivirusni program, enkripcija) v organizaciji je pomembno. | 1 | 2 | 3 | 4 | 5 |

51. Za vašo organizacijo na spodnji lestvici ocenite, kakšna je stopnja odvisnosti od IKT procesov (*obkrožite*):

nizka 1 2 3 4 5 zelo visoka

52. Ali je v vaši organizaciji, po vaši vednosti, v zadnjih 12 mesecih prišlo do katerega od naslednjih dogodkov

| | | | |
|---|---|---|---|
| a) notranjega napada (s strani zaposlenega) | DA | NE | NE VEM |
| b) zunanjega napada (s strani nekoga zunaj organizacije) | DA | NE | NE VEM |
| 53. V naši organizaciji imamo izdelan varnostni načrt na področju IKT | DA | NE | NE VEM |
| 54. V naši organizaciji imamo predpisana pravila o tem, kako poročati o nezgodah, ki so v povezavi z informacijsko varnostjo. | DA | NE | NE VEM |
| 55. Naša organizacija ima zapisana pravila (politike) informacijske varnosti. | DA | NE | NE VEM |
| 56. V naši organizaciji so predvideni natančni ukrepi za primer nespoštovanja predpisov s področja varovanja zaupnih podatkov. | DA | NE | NE VEM |
| 57. V naši organizaciji obstaja utečen postopek, ki zagotavlja, da so vsi zaposleni seznanjeni z določili varovanja zaupnih informacij. | DA | NE | NE VEM |
| 58. Enostavno lahko pridobim kopijo dokumenta o informacijsko varnostih pravilih, ki obstajajo v naši organizaciji. | DA | NE | NE VEM |
| 59. Vsi zaposleni v naši organizaciji so seznanjeni s tveganji, ki so opredeljena za varovanje zaupnih podatkov. | DA | NE | NE VEM |

***Za potrebe statistične analize bi potrebovala še nekaj dodatnih socio-demografskih podatkov.***

60. Spol (*obkrožite*): a) moški b) ženski

61. Starost (*napišite dopolnjena leta*): _____

62. Koliko časa delate v organizaciji *(napišite dopolnjena leta*)? _____

63. Ali naloge opravljate na vodstvenem delovnem mestu (*obkrožite*)?

a) da b) ne

64. Izobrazba (*obkrožite najvišjo dokončano stopnjo izobrazbe*):

a) srednja b) višja c) visoka strokovna d) univerzitetna

e) magisterij ali specializacija f) doktorat

65. Ali je vaša formalna izobrazba povezana s področjem IKT (*obkrožite*)?

a) da b) ne

**KOMENTAR**

……

……

……

……

**Najlepša hvala za sodelovanje!**