UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

# MERJENJE ZAVEDANJA ČLOVEŠKEGA VPLIVA NA VAROVANJE INFORMACIJ V IZBRANEM PODJETJU

Ljubljana, september 2023 MATIC KOSMAČ

# IZJAVA O AVTORSTVU

Podpisani(-a) Matic Kosmač, študent/-ka Ekonomske fakultete Univerze v Ljubljani, avtor/-ica predloženega dela z naslovom Merjenje zavedanja človeškega vpliva na varovanje informacij v izbranem podjetju, pripravljenega v sodelovanju s svetovalcem/svetovalko red. prof. dr. Tomažem Turkom

I Z J A V L J A M

1. da sem predloženo delo pripravil/-a samostojno;

2. da je tiskana oblika predloženega dela istovetna njegovi elektronski obliki;

3. da je besedilo predloženega dela jezikovno korektno in tehnično pripravljeno v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani, kar pomeni, da sem poskrbel/-a, da so dela in mnenja drugih avtorjev oziroma avtoric, ki jih uporabljam oziroma navajam v besedilu, citirana oziroma povzeta v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani;

4. da se zavedam, da je plagiatorstvo – predstavljanje tujih del (v pisni ali grafični obliki) kot mojih lastnih – kaznivo po Kazenskem zakoniku Republike Slovenije;

5. da se zavedam posledic, ki bi jih na osnovi predloženega dela dokazano plagiatorstvo lahko predstavljalo za moj status na Ekonomski fakulteti Univerze v Ljubljani v skladu z relevantnim pravilnikom;

6. da sem pridobil/-a vsa potrebna dovoljenja za uporabo podatkov in avtorskih del v predloženem delu in jih v njem jasno označil/-a;

7. da sem pri pripravi predloženega dela ravnal/-a v skladu z etičnimi načeli in, kjer je to potrebno, za raziskavo pridobil/-a soglasje etične komisije;

8. da soglašam, da se elektronska oblika predloženega dela uporabi za preverjanje podobnosti vsebine z drugimi deli s programsko opremo za preverjanje podobnosti vsebine, ki je povezana s študijskim informacijskim sistemom članice;

9. da na Univerzo v Ljubljani neodplačno, neizključno, prostorsko in časovno neomejeno prenašam pravico shranitve predloženega dela v elektronski obliki, pravico reproduciranja ter pravico dajanja predloženega dela na voljo javnosti na svetovnem spletu preko Repozitorija Univerze v Ljubljani;

10. da hkrati z objavo predloženega dela dovoljujem objavo svojih osebnih podatkov, ki so navedeni v njem in v tej izjavi.

11. da sem preveril verodostojnost informacij, ki izhajajo iz zapisov na podlagi uporabe orodij umetne inteligence.

V Ljubljani, dne 05.09.2023 Podpis študenta(-ke): _____

# KAZALO

# KAZALO TABEL

# KAZALO SLIK



# KAZALO PRILOG

# SEZNAM KRATIC

angl. – angleško
**ACMP** – (angl. Association of Change Management Professionals); združenje strokovnjakov za upravljanje sprememb
**AES** – (angl. Advanced Encryption Standard); standard naprednega šifriranja
**AI** – (angl. Artificial Intelligence); umetna inteligenca
**ATP** – (angl. Advanced Persistent Threat); napredna trajna grožnja
**BCM** – (angl. Business Continuity Management); neprekinjenost poslovanja
**BCP** – (angl. Business Continuity Planning); načrt neprekinjenega poslovanja
**BIA** – (angl. Business Impact Analysis); analiza vpliva na poslovanje
**CERT** – (angl. Computer Emergency Response Team); nacionalna skupina za odzivanje na računalniško varnostne incidente
**CIA** – (angl. Confidentiality, Integrity, Availability); triada zaupnosti, celovitost in razpoložljivost
**COBIT 5** – (angl. Control Objectives for Information and Related Technology); okvir za upravljanje informacijske varnosti
**COVID-19** – (angl. coronavirus disease 2019); koronavirusna bolezen 2019
**CSIRT** – (angl. Computer Security Incident Response Team); skupina za odzivanje na računalniške incidente
**CSV** – (angl. Comma-Separated Values); datoteka z vrednostmi, ločenimi z vejicami
**DDoS** – (angl. Distributed Denial of Service); porazdeljeni napad z zavrnitvijo storitve
**DoS** – (angl. Denial of Service); zavrnitev storitve
**DPIA** – (angl. Data Protection Impact Assessment); ocena učinka na varstvo osebnih podatkov
**EFA** – (angl. Exploratory Factor Analysis); eksploratorna faktorska analiza
**ESCO** – (angl. European Cyber Security Organisation); Evropska organizacija za kibernetsko varnost
**EU** – (angl. European Union); Evropska unija
**FA** – (angl. Factor analysis); faktorska analiza
**GDPR** – (angl. General Data Protection Regulation); Splošna uredba o varstvu osebnih podatkov
**HAIS-Q** – (angl. Human Aspect of Information Security Questionnaire); vprašalnik o človeških vidikih informacijske varnosti
**HMAC** – (angl. Hash-Based Message Authentication Code); posebna vrsta kode za preverjanje pristnosti sporočila, z vključeno kriptografsko zgoščevalno funkcijo in skrivnim kriptografskim ključem
**HTTP** – (angl. Hyper Text Transfer Protocol); niz pravil za prenos datotek in promet na svetovnem internetu

**HTTPS** – (angl. Hypertext Transfer Protocol Secure); niz pravil za prenos datotek in promet na svetovnem internetu v povezavi s protokolom za preverjanje pristnosti in varnosti
**ICS** – (angl. Information Security Culture); informacijska varnostna kultura
**IKT** – (angl. Information and Communication Technology); informacijska komunikacijska tehnologija
**IMF** – (angl. International Monetary Found); Mednarodni denarni sklad
**IoT** – (angl. Internet of Things); internet stvari
**IP** – (angl. Internet Protocol); edinstveno ime s svetovnim spletom povezane elektronske naprave
**IS** – (angl. Information System); informacijski sistem
**ISA** – (angl. Information Security Awereness); zavedanje o informacijski varnosti
**IT** – (angl. Information Technology); informacijska tehnologija
**ITIL** – (angl. Information Technology Infrastructure Library); infrastrukturna knjižnica informacijske tehnologije
**KAB** – (angl. Knowledge, Attitude, Behaviour); znanje, odnos, vedenje
**KMO** – (angl. Keiser-Meyer-Olkin Test); Kaiser-Meyer-Olkin test za ustreznost vzorčenja
**ML** – (angl. Machine Learning); strojno učenje
**NIS** – (angl. Network and Information Security); vseevropska zakonodaja o kibernetski varnosti
**NIST** – (angl. National Institute of Standards and Technology); ameriški nacionalni inštitut za standarde in tehnologijo
**P2P** – (angl. Peer To Peer); protokol enakovrednemu
**PAF** – (angl. Principal Axis Factoring); metoda glavne osi ekstrakcije faktorjev
**PDCA** – (angl. Plan, Do, Check, Act); cikel načrtuj, izvedi, preveri, ukrepaj
**PIAF** – (angl. Privacy Impact Assessment Framework); okvir ocene vpliva na zasebnost
**SHA** – (angl. Secure Hash Algorith); algoritem varnega zgoščevanja
**SMART** – (angl. Specific, Measurable, Attainable, Relevant, Time-Bound); Metoda za postavljanje ciljev – Specifično, merljivo, dosegljivo, realistično in časovno omejeno
**SoA** – (angl. Statement of Applicability); izjava o uporabnosti
**SSL** – (angl. Secure Sockets Layer); varnost transportnega sloja
**SUIV** – (angl. Information Security Management System); sistem za upravljanje informacijske varnosti
**VPN** – (angl. Virtual Private Network); navidezno zasebno omrežje
**ZinfV** – Zakon o informacijski varnosti
**ZVOP-2** – Zakon o varstvu osebnih podatkov 2

# UVOD

Tehnološki napredek in digitalizacija poslovanja ne prinašata vedno varnejšega okolja, zato je informacijska varnost sestavni del digitalne preobrazbe (Soltanmohammadi, Asadi & Ithnin, 2013, str. 329). Zdravstvena pandemija je organizacije še dodatno ozavestila, da je nemoteno delovanje poslovanja odvisno predvsem od informacijske tehnologije (angl. Information technology, v nadaljevanju IT) in je zato informacijska varnost ključnega pomena. Vse vrste človeških dejavnikov lahko močno vplivajo na upravljanje informacijske varnosti (angl. Managing Information Security) v organizaciji in ogrozijo vse vrste procesov, zato informacijska varnost in pomen varnosti v splošnem ni izključno tehnični problem (Ashenden, 2008, str. 198). Za doseganje učinkovite prakse varnosti informacijskih sistemov in varnosti informacij mora vodstvo poznati, razumeti ter obvladovati tudi človeške dejavnike, ki vplivajo na varnostne incidente. Kljub tem dejstvom in trendom se podjetja srečujejo s pomanjkanjem strokovnjakov, ki bi bili ustrezno usposobljeni obvladovati te grožnje, ki pretijo informacijskem sistemu (angl. Information system, v nadaljevanju IS). Za doseganje ustrezne ravni zaščite je potrebno vlagati v namenske ukrepe in imeti visoko usposobljene strokovnjake, ki te iste ukrepe učinkovito izvajajo. Poleg omejitev, povezanih s proračunskimi vprašanji, se vse prevečkrat pojavlja tudi težava usposobljenosti zaposlenih. Ti izzivi predstavljajo glavne pomisleke glede upravljanja informacijske varnosti in lahko nekako pojasnijo, zakaj napake zaposlenih povzročajo več kot polovico vseh varnostnih incidentov (Rožanc & Lahajnar, 2017, str. 93; Marble in drugi, 2015).

Človeške dejavnike se težko obvladuje, ker so medsebojno povezani ter vplivajo na delo v informacijsko tehnološkem okolju, zato je takšno okolje potrebno ustrezno zaščititi pred nezaželenimi vplivi (Herzog, 2010). Človeški dejavniki so različnih dimenzij, so edinstveno prepleteni z organizacijsko kulturo in so skupek različnih individualnih zaznav ter značilnosti. Znanstvena literatura človeški dejavnik definira kot zapleten, dinamičen, matematično nekoliko nelinearen in stohastičen. To pomeni, da ni sorazmeren, ampak odvisen tudi od drugih vplivov ter se obnaša kaotično in negotovo (Proctor & Van Zandt, 2018; Alavi, Islam, Jahankhani & Al-Nemrat, 2013, str. 51).

Posledično zagotavljanje globalnih rešitev informacijske varnosti predstavlja velik izziv v organizacijskem kontekstu na ravni države oz. celotnega globalnega gospodarskega okolja, saj se IS podjetja nahajajo v istem globalnem kibernetskem prostoru (Tipton & Krause, 2008). Človeški dejavniki so glavni povzročitelj varnostnih incidentov, povezanih z varnostjo IS, posledica tega pa so tudi vprašanja, kako obvladovati te dejavnike, kot so napake, neustrezne veščine, pomanjkljive varnostne politike, varnostno zavedanje ali apatija (Werlinger, Hawkey & Beznosov, 2009, str. 5–9).

Zagotavljanje zanesljivega in skladnega IS zahteva trden varnostni okvir, ki zagotavlja zaupnost (angl. Confidentiality), celovitost (angl. Integrity) in razpoložljivost (angl. Availability) kritičnih informacijskih sredstev. Sistem upravljanja informacijske varnosti (angl. Information Security Management System, v nadaljevanju SUIV) določa vzpostavitev trdnega varnostnega okvirja in sistematično ureja rabo informacijsko-komunikacijske tehnologije (angl. Information and Communication Technology, v nadaljevanju IKT). Tehnološke nadgradnje sistema informacijske varnosti ne zagotavljajo vedno varnost celotnega organizacijskega okolja, saj človeški dejavniki igrajo pomembno vlogo pri varnosti informacij in gre zato za ranljivejši element v verigi informacijske varnosti (Alavi, Islam, Jahankhani & Al-Nemrat, 2013). Ker imajo ljudje različni kontekst dojemanja varnosti, so reakcije na postopke in ukrepe informacijske varnosti lahko zelo raznolike in predstavljajo nenadzorovane sile. Vsak posameznik ima pomisleke, lastne vrednote, kulturo, veščine, znanja, stališča in vedenje (Karjalainen, Siponen & Sarker, 2020, str. 4). Našteti dejavniki so zelo subjektivni in jih je težko meriti, kaj šele izračunati v procesih informacijskega varnostnega sistema. Te sile medsebojno vplivajo na varnost tehnoloških elementov v medsebojno povezanem IS (Herzog, 2010).

Naloga razumevanja človeških dejavnikov je zahtevna, saj je njihova domena zelo subjektivne narave in so zato težko neposredno merljiva (Alavi, Islam, Jahankhani & Al-Nemrat, 2013). Veliko je področij, pri katerih postane presoja izjemno težka in subjektivna, saj je vsak človek svoj boem, prav tako pa je tudi področje definiranja dejavnikov lahko zelo osebno in subjektivno. Za primer vzemimo, da je skoraj nemogoče oceniti oz. presojati apatijo ljudi in odnosa do informacijske varnosti. Umetna inteligenca (angl. Artificial intelligence, v nadaljevanju AI) in strojno učenje (angl. Machine learning, v nadaljevanju ML) predstavljata temeljno tehniko povezovanja in obdelave velikih količin podatkov ter predstavljata dobro pot učenja v poslovnem svetu, da bi lažje razumeli in skozi še neprepoznane vzorce lažje obvladovali tveganja, ki jih predstavljajo človeški dejavniki. Na nivoju skupine je zelo pomembno zaupanje med zaposlenimi in vodstvom, ker ima vodstvo ključno vlogo pri udejanjanju informacijske varnosti, zato mora skozi svoja dejanja odražati zavezanost in vključenost ter biti zgled vsem zaposlenim pri spoštovanju varnostne politike in varnostnih protokolov. Na nivoju posameznika je potrebno nenehno spodbujanje k dvigu zavedanja varovanja informacij. Prav tako je pomembna etičnost pri ravnanju z intelektualno lastnino organizacije ter etičnost pri rokovanju z IKT (Mittu & Lawless, 2015; Redmill, 2002, str. 172–173).

Strategije informacijske varnosti bi bilo mogoče nadgraditi in izboljšati, da ugotovimo kritične človeške dejavnike ter raven zavedanja do varovanja informacij in podatkov ter poskušamo oceniti, kje je tveganje večje, saj s tem lažje predvidimo in minimiziramo tveganje za nastanek prekinitve poslovanja in nedovoljenih posegov v IS organizacije. Večina vprašanj informacijske varnosti ima največkrat skupni imenovalec – ljudi. Prioriteta zaključnega dela je prepoznanje ključnih človeških dejavnikov, ki predstavljajo tveganje za IS. S prepoznavo tveganja z vidika človeških dejavnikov in njegovih povezav

na informacijsko varnost lahko uspešno spreminjamo strategijo informacijske varnosti ter lažje predvidimo ranljivosti pri upravljanju informacijske varnosti, ki jo predstavljajo ljudje (Parsons, McCorman, Butavicius, Pattinson & Jerram, 2014, str. 166–167).

Namen magistrskega dela je na podlagi primarnih podatkov, pridobljenih z anketnim vprašalnikom, analizirati zavedanje zaposlenih in podati predloge ukrepov za izboljšanje znanja, ki bi se odražalo v boljšem odnosu in varnostnem vedenju, torej zavedanju do informacijske varnosti.

Cilji magistrskega dela so s sistematičnim pregledom strokovne in znanstvene literature opredeliti upravljanje informacijske varnosti z vidika človeških dejavnikov, opredeliti tveganja posrednih in neposrednih človeških dejavnikov, preveriti ustreznost ozaveščenosti zaposlenih o informacijski varnosti, ugotoviti, katera dimenzija po oceni zavedanja najbolj ogroža sistem upravljanja informacijske varnosti, ter prenesti spoznanja iz realno obravnavanega primera merjenja zavedanja informacijske varnosti v poslovno prakso. Glavna cilja dela sta z uporabo multivariatnih metod faktorske analize preveriti veljavnost prevedenega vprašalnika, zaradi terminoloških in leksikalnih razlik med angleškim in slovenskim jezikom ter z regresijskima analizama opisati naravo odnosa ter napovedati vrednost odvisne spremenljivke vedenja na podlagi vrednosti neodvisnih spremenljivk znanja in odnosa.

Delo je razdeljeno na tri poglavja. Prvo in drugo poglavje vsebujeta teoretična izhodišča upravljanja informacijske varnosti ter opredelitev vpliva človeških dejavnikov na upravljanje varnosti informacij. Tretje poglavje je namenjeno empiričnemu delu in preverjanju veljavnosti vprašalnika, izračunu medsebojnega vpliva po treh dimenzijah po okvirju vprašalnika ter oceni zavedanja informacijske varnosti zaposlenih s predlogi za izboljšavo.

# 1 UPRAVLJANJE INFORMACIJSKE VARNOSTI

Cilji upravljanja informacijske varnosti so zaščititi sisteme, ki so kritični za izvajanje poslanstva organizacije (Soltanmohammadi, Asadi & Ithnin, 2013, str. 331). Danes so računalniški sistemi v organizaciji močno povezani z notranjim (angl. Intranet) ter zunanjim (angl. Internet) omrežjem za namen lažjega dostopa do vseh vrst informacij, zato potrebujemo protokole, ki jih mora organizacija izvesti, da zagotovi zaupnost, celovitost in razpoložljivost informacijskih sredstev. Vendar se še vedno vsakodnevno postavljajo vprašanja o informacijski varnosti, kako čim bolj učinkovito zaščititi informacijska sredstva pred nepooblaščenimi dostopi, razkritjem, spreminjanjem in uničevanjem (Samonas & Coss, 2014, str. 23). Internet predstavlja ranljivo vstopno točko za kibernetske napade, vključno z lažnim predstavljanjem, virusi in uhajanjem podatkov (Kritzinger, da Veiga & van Staden, 2022).

Upravljanje informacijske varnosti vključuje tudi obvladovanje informacijskih tveganj, s katerimi se organizacija sooča pri upravljanju in zaščiti informacijskega premoženja. Obstaja veliko tehničnih rešitev, ki pomagajo zaščititi informacijsko premoženje organizacije, da se prepreči nevarnost uhajanja poslovnih informacij, njihovo spreminjanje ali uničenje, vendar se tveganju popolnoma ne moremo izogniti. Za bolj učinkovito zagotavljanje informacijske varnosti ni dovolj, da se izključno zanašamo na tehnološke rešitve, saj s tehnologijo upravljamo ljudje in največkrat lahko človeški dejavniki močno ogrozijo informacijsko varnost (Soltanmohammadi, Asadi & Ithnin, 2013, str. 331–333). Še tako napredni in tehnično dovršeni varnostni sistemi imajo pomanjkljivosti, ki jih spletni kriminal poskuša učinkovito preskočiti s pomočjo človeške interakcije, ko postanemo nepozorni. Raziskave o upravljanju informacijske varnosti definirajo, da je informacijska varnost sestavljena iz tehničnih konceptov v razmerju 20 : 80 v razmerju s človeškim vedenjem. Nekatere študije celo navajajo, da je to razmerje 90 : 10 v prid vedenja zaposlenih (Fertig & Schütz, 2020; Samonas & Coss, 2014, str. 23).

## 1.1 Informacijska sredstva

Na področju informacijske varnosti in IT so sredstva (angl. Asset) vse, kar prinaša organizaciji koristi pri poslovanju in je povezano z informacijskimi storitvami ter predstavlja vrednostno postavko (Shedden, Ahmad, Smith, Tscherning & Scheepers, 2016, str. 15). Standard ISO 27001 navaja sredstva kot naprave, programske sisteme, podatke in informacije ter nenazadnje tudi ljudi ter ostala korporacijska sredstva, ki za organizacijo predstavljajo določeno vrednost. Torej lahko kot sredstvo označimo vse, kar ima vrednost ter podpira delovanje podjetja, ne glede na obliko vrednosti. Poznavanje sredstev v organizaciji je pomemben element informacijske varnosti, saj pomagajo razumeti, kako občutljivi so podatki in informacije, kdo lahko do njih dostopa ter kakšno raven zaščite jim moramo zagotoviti (Culot, Nassimbeni, Podrecca & Sartor, 2021, str. 77–78).

Informacijsko sredstvo je mogoče opisati kot nabor urejenih podatkov, ki predstavljajo dragoceno enotno entiteto. Torej je informacijsko sredstvo vsak podatek oz. znanje, ki ima za organizacijo določeno vrednost. Zaradi tega se vrednost informacij obravnava enako kot katero koli drugo korporativno sredstvo. Informacijska sredstva imajo za organizacije tako finančno, informacijsko kot strateško vrednost, ker so pomembna za nemoteno učinkovito poslovanje organizacije (Bojanc, Jerman-Blažič & Tekavčič, 2014, str. 11–14).

Pomembno je razumeti, katere so potencialne nevarnosti v poslovnem okolju za organizacijska poslovna sredstva, da jih lahko učinkovito zaščitimo. Niso vse grožnje namerne, saj lahko uporabnik nehote razkrije občutljive in zaupne podatke osebi, kateri jih ne bi smel, in tako ogrozi informacijsko varnost organizacije. V izogib temu moramo podobno kot za vsa ostala sredstva tudi za ljudi prepoznati ustrezne vzorce vodenja, da se

zagotovi ustrezno raven informacijske varnosti, ki za organizacijo predstavlja poslovno vrednost in je težko nadomestljiva (Bojanc, Jerman-Blažič & Tekavčič, 2014, str. 21). Da ljudje v organizaciji upravljajo z vsemi sredstvi, je potrebno spremljati njihove odzive, saj pomembno vplivajo na (ne)varnost sredstev. Poslovanje, ki sledi zastavljenim ciljem, terja tudi, da morajo imeti zaposleni dostop do ustreznih sredstev in z njimi povezanih informacij, ki jih morajo znati učinkovito uporabljati in hkrati varovati. Že iz tega vidika vidimo, da ima vodstvo ključno vlogo pri ozaveščanju pomena informacijske varnosti v organizacijah, saj so nenazadnje tudi posredni lastnik sredstev (angl. Asset owner), z njimi upravljajo ter so odgovorni za to, kako skrbniki informacijskih sredstev (zaposleni) z njimi upravljajo in operirajo. Lastnik informacijskih sredstev mora oceniti tveganja in zagotoviti, da so ta primerno zaščitena. Uporabnik podatkov je vsak zaposleni, ki ga je imetnik podatkov pooblastil za dostop do informacijskih sredstev, zato imajo ključno vlogo pri varovanju in vzdrževanju IS organizacije ter morajo biti ustrezno usposobljeni, da lahko prepoznajo in poročajo o morebitnih incidentih oz. zlonamernih dejavnostih, ki ogrožajo vrednost informacijskega sredstva (Samonas & Coss, 2014, str. 27; Bojanc, Jerman-Blažič & Tekavčič, 2014, str. 19).

## 1.2 Informacijske grožnje

Grožnja (angl. Threat) je v informacijski varnosti potencialno nezaželeno dejanje ali pojav, ki lahko negativno vpliva na zaupnost, razpoložljivost in celovitost informacijskih sredstev. Grožnje lahko izvirajo znotraj organizacije ali iz zunanjega okolja, kar je tudi najpogostejši način segmentiranja informacijskih groženj. Akterji informacijskih groženj so največkrat finančno ali družbeno in socialno motivirani hekerji, nezadovoljni zaposleni ali pa delujejo kot organizirani spletni kriminal (Samonas & Coss, 2014).

Bojanc, Jerman-Blažič in Tekavčič (2014) grožnje razvrščajo glede na usmeritev in vpliv na informacijska sredstva, in sicer na:

- uničenje informacijskih sredstev;
- spreminjanje informacijskih sredstev;
- krajo informacijskih sredstev;
- razkritje zaupnih informacij;
- prekinitev delovanja storitev.

Talabis in Martin (2012) poudarjata, da je pomembno razločevanje med virom grožnje in grožnjo. Primer hekerskega napada na sistem predstavlja vir grožnje – heker, grožnja pa predstavlja nepooblaščeni dostop do sistema s strani hekerja. Napadi navadno nimajo za cilj zgolj dostop, temveč je namen nepooblaščenega dostopa tudi grožnja izbrisa, zlorabe ali prekinitve dostopa storitev. Določanje nevarnosti groženj je največkrat zelo subjektivna presoja, zato si strokovnjaki za informacijsko varnost pomagajo s smernicami

iz katalogov ali referenčnimi modeli, ki pomagajo prepoznati potencial nevarnosti preteče grožnje na informacijska sredstva ter kakšno škodo lahko povzročijo.

Človeške grožnje razdelimo na namerne in nenamerne. Namerne grožnje lahko izhajajo iz zunanjega okolja poslovanja ali od notranjega uporabnika, katerega namen je škodovati organizaciji. Najpogosteje se pojavljajo v obliki sprememb podatkov, vdorov v sistem, kraje podatkov, kraje identitete ter v obliki zlonamernih kod. Nenamerne grožnje v obliki napak izvirajo iz vedenja zaposlenih, kot je brisanje datotek, nepravilno ravnanje s sredstvi, fizične nesreče ali drugih oblik vedenj. Dosedanje študije kažejo, da več kot 80 % povzročenih varnostnih incidentov v poslovnem okolju izvira iz notranjih groženj – odnosa in vedenja zaposlenih (Conwill, 2010, str. 3).

## 1.3 Model informacijske varnosti

Model informacijske varnosti prikazan na sliki 1 – triada zaupnosti, celovitost in razpoložljivost (angl. Confidentiality, Integrity, Availability – CIA) je pravzaprav varnostni model, ki je bil razvit, da bi ljudem pomagal razviti holističen pristop do varnosti v IT okolju. Cilji informacijske varnosti so zaščita zaupnosti informacij, zaščita celovitosti ter zagotavljanje pravočasne razpoložljivosti informacij izključno avtoriziranim uporabnikom. Tri načela skupaj tvorijo temelj varnostne infrastrukture katere koli organizacije ter bi morala delovati kot temeljni cilj vsakega varnostnega programa v organizaciji (Bojanc, Jerman-Blažič & Tekavčič, 2014, str. 20).

*Slika 1: Model informacijske varnosti*


*Prirejeno po Samonas & Coss (2014).*

Podjetja za posamezne cilje informacijske varnosti določijo želeno stopnjo na način, da podjetje za vsak poslovni proces določi zahteve zaupnosti, celovitosti in razpoložljivosti sistema oz. podatkov. Ko pride do varnostnega incidenta, krizna ekipa najprej oceni kršenje navedenih treh temeljnih varnostnih načel. Varnostni strokovnjaki torej ocenijo

grožnje na podlagi morebitnega vpliva, ki ga ima incident na zaupnost, celovitost in razpoložljivost sredstev organizacije. Na podlagi ocene tveganja strokovnjaki izvajajo nabor varnostnih kontrol, da zmanjšajo tveganje v okolju poslovanja organizacije. Torej je v tem okviru zaupnost niz pravil, ki omejujejo dostop do informacij, celovitost je zagotovilo, da so informacije zanesljive in točne, razpoložljivost pa je jamstvo za zanesljiv dostop do informacij s strani pooblaščenih oseb (Bojanc, Jerman-Blažič & Tekavčič, 2014, str. 22–23).

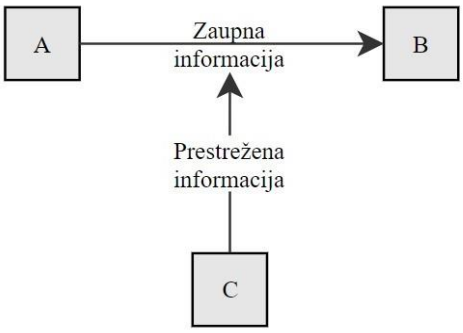
V poslovni praksi je zelo pomembno šifriranje podatkov in sporočil (angl. Encryption), tj. ena od metod za zagotavljanje zaupnosti, tako da nepooblaščeni uporabniki ne morejo pridobiti ali dostopati do podatkov, do katerih nimajo pravice. Nadzor dostopa je tudi bistveni del ohranjanja zaupnosti, saj določa, kateri uporabniki imajo pravico do dostopa. Ko pride do varnostnega incidenta, je zelo pomembno, da imamo revizijsko sled oz. dnevnik dogodkov znotraj SUIV, saj to zagotavlja celovitost podatkov. Uveljavljanje nadzora in revizijskih sledi v IS organizacije zagotavlja, da so podatki točni in celoviti, kar je bistvo vrednosti podatkov in informacij organizacije, ki zasleduje skladnost poslovanja. Razpoložljivost v praksi organizacije največkrat dosegajo z uporabo IT rešitev v oblaku, kot so Google Cloud, AWS, Microsoft Azure idr. ponudniki (Nieles, Dempsey & Yan Pillitteri, 2017).

### 1.3.1 Zaupnost

Zaupnost (angl. Confidentiality) je zasebnost in avtorizacija. Razkrivanje občutljivih podatkov nepooblaščenim osebam predstavlja izgubo zaupnosti. Zaupnost je pogosto jedro vseh varnostnih politik v podjetju, ki določa, kateri posameznik ima dostop do določenih informacij ter za kakšne namene jih lahko uporablja pri svojem delu (Bojanc, Jerman-Blažič & Tekavčič, 2014, str. 20).

Slika 2 plastično ponazarja primer, ko sta zasebnost in avtorizacija kršeni. Ustrezna zaščita pred izgubo zaupnosti je nadzor dostopa in šifriranje podatkov ter podatkovnih baz. Sodobni algoritmi za šifriranje so relativno zelo varni in so sestavni del programske in strojne opreme. Najbolj razširjen in poznan je napredni šifrirni standard (angl. Advanced Encryption Standard – AES), ki spada med simetrične bločne šifre. Z naprednim šifrirnim standardom lahko uporabljamo krajše bitne ključe, kot sta 128- in 192-bitna, vendar je priporočljivo uporabljati 256-bitnega. Daljša kot je dolžina bitov ključa, težje je dešifriranje, kar pomeni, da je težje dostopati do samih podatkov in informacij v berljivi obliki brez ključev za dešifriranje. Ko je uporabnik identificiran in je avtorizacija končana, dobi pravico do dostopa v sistem ali pa se uporabniku onemogoči dostop do sistema na podlagi dodeljenih pravic dostopa (Nieles, Dempsey & Yan Pillitteri, 2017).

*Slika 2: Izguba zaupnosti*




A: Zaupna informacija
B: Pooblaščeni uporabnik
C: Nepooblaščeni uporabnik

*Vir: lastno delo.*

Zaupnost je pri prenosu podatkov bistvenega pomena. Navidezno zasebno omrežje (angl. Virtual Private Network – VPN) je ustrezna rešitev za zagotavljanje komunikacije med uporabniki in ciljnim omrežjem ali komunikacijo med omrežji (angl. Peer to Peer – P2P) preko interneta, kar povečuje zaupnost. Toda rešitev VPN ni mogoče uporabljati povsod, zato je potrebno spletna brskanja, plačilne transakcije ter vse vrste občutljivih podatkov obravnavati z uporabo šifriranega prometa s kriptografskim protokolom. Komunikacijski protokol med odjemalci in strežniki (angl. Hyper Text Transfer Protocol – HTTP) preko kriptografskega protokola SSL (angl. Secure Sockets Layer – SSL), omogoča varno komunikacijo na internetu – HTTPS, zaradi česar je uporaba internetnih virov varnejša, povečujeta se tudi zaupnost in zasebnost podatkov, kar je pri današnjem digitalnem poslovanju bistveno za ohranjanje poslovne vrednosti ter konkurenčnih prednosti. Obstaja veliko spletnih strani, ki še ne uporabljajo protokola HTTPS. Če naletimo na spletno mesto, ki ne uporablja šifriranega prometa, bi morali biti kot uporabnik previdnejši, še posebej, če pri storitvi operiramo z zaupnimi podatki ali plačilnimi transakcijami. Zato ne smemo na spletna mesta brez ustreznega šifriranja nikoli vnašati zaupnih podatkov in informacij, čeprav od nas spletno mesto to zahteva, saj je namen v veliki verjetnosti zlonameren. Zavedati, se je potrebno, da še tako napredna tehnologija nima odgovorov na vsa varnostna vprašanja, zato je uporaba različnih standardov in algoritmov ter šifriranje samo del reševanja varnostnega problema, ki opravlja ključno komponento informacijske varnosti (Nieles, Dempsey & Yan Pillitteri, 2017; Bojanc, Jerman-Blažič & Tekavčič, 2014, str. 23).

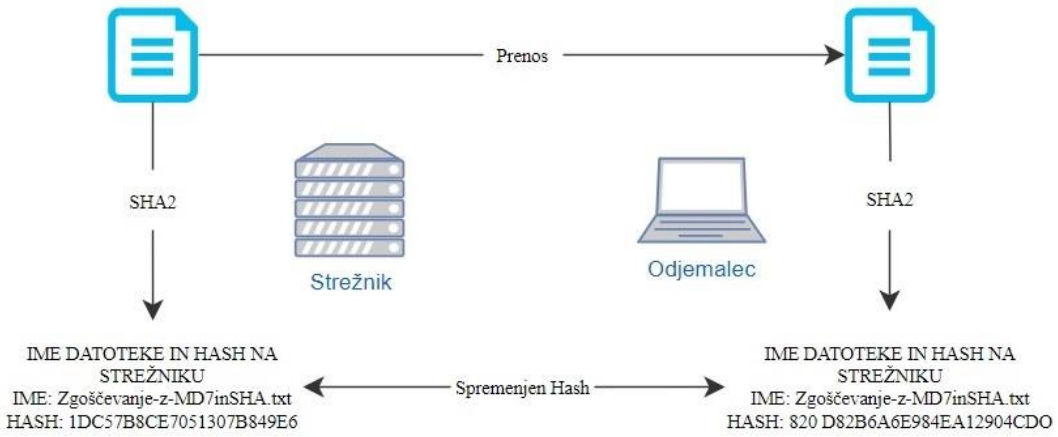
### 1.3.2 Celovitost

Celovitost (angl. Integrity) vključuje ohranjanje doslednosti, natančnosti in zanesljivosti podatkov ter informacij celotnem življenjskem ciklu. Izguba celovitosti pomeni, da je podatke nepooblaščen posameznik spremenil oz. uničil ali da je bila spremenjena

sistemska konfiguracija, zaradi česar uporabniki trpijo škodo (Qadir & Quadri, 2016, str. 191).

Varnostni mehanizmi za zagotavljanje celovitosti delujejo tako, da blokirajo vse nepooblaščene poskuse spreminjanja in preverjajo celovitost informacij. Mehanizmi sami po sebi ne preprečujejo zlorab. V kolikor zaznajo, da je bil nepooblaščen poskus spreminjanja uspešen, sporočijo, da informacija ni več vredna zaupanja in je s tem kršena celovitost ter sprožijo signal za varnostni incident. Zagotavljanje celovitosti v elektronski obliki se izvaja s kontrolnimi podatki oz. zgoščevalnimi algoritmi (angl. Hash), ki delujejo na principu izgube informacij in zagotavljajo, da je izvleček za poljubno dolg niz informacije vedno enako dolg v enakih vrednostih. Čeprav se informacijo spremeni minimalno, to pomeni popolnoma drugačno vrednost izvlečka. Celovitost se zagotovi tako, da se pri pošiljanju ali shranjevanju informacije izračuna izvleček z algoritmi in se izvleček shrani skupaj z informacijo. Pri prejemu informacije se izvleček ponovno izračuna ter primerja s prejetim izvlečkom. Če sta rezultata enaka, to pomeni, da se informacija v procesu pošiljanja oz. prejemanja ni spremenila. Teoretično lahko obstaja več različnih datotek, ki imajo enak izvleček, vendar je matematično nemogoče najti dve datoteki, ki podata enak rezultat, saj z matematičnimi algoritmi vsaki datoteki izračunamo unikatno zgoščevalno vrednost (Bojanc, Jerman-Blažič & Tekavčič, 2014, str. 23–24). Poznamo več vrst standardiziranih enosmernih zgoščevalnih algoritmov, kot sta SHA (angl. Secure Hash Algorith, v nadaljevanju SHA) ali MD (angl. Message Digest, v nadaljevanju MD). Kompleksnost obeh algoritmov je približno enaka, vendar je odzivni čas MD hitrejši od SHA algoritmov. MD uporablja 128-bitno dolžino šifriranja in je bolj ranljiv za napade kot SHA, ki ima dolžino možnosti zgoščevanja v 160-bitov (Preethi & Parameshvar, 2022, str. 4362). Slika 3 je nazorni primer izgube celovitosti, ko uporabnik prenese datoteko s strežnika, kjer je bil spremenjen »Hash« iz prvotne vrednosti, kar pomeni, da je bil izveden poseg v datotečni sistem.

*Slika 3: Sprememba celovitosti datoteke*




*Vir: lastno delo.*

Problem enosmernih zgoščevalnih funkcij oz. algoritmov je, da lahko tisti, ki spreminjajo informacijo, ponaredijo tudi izvleček, saj ga ponovno izračunajo na podlagi spremenjene informacije ter tako zamenjajo prvotni izvleček. Tega se lahko uspešno ubranimo na način, da izvleček dodatno šifriramo in uporabimo zgoščevalni algoritem s ključem (angl. Hash-based Message Authentication Code, v nadaljevanju HMAC). HMAC je podoben digitalnemu podpisu, saj oba uveljavljata celovitost oz. integriteto in pristnost ter uporabljata kriptografske ključe, s to razliko, da digitalni podpis uporablja asimetrične ključe, medtem ko HMAC uporablja simetrične ključe brez uporabe javnega ključa (Bojanc, Jerman-Blažič & Tekavčič, 2014, str. 24).

### 1.3.3 Razpoložljivost

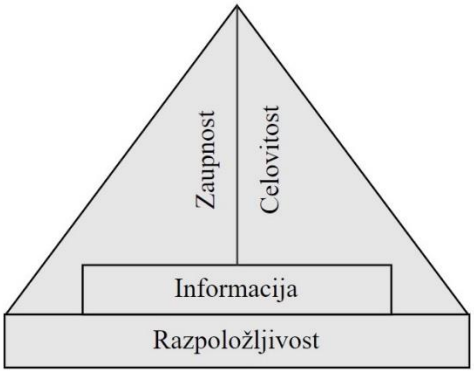
Koncept razpoložljivosti (angl. Availability) pomeni zagotavljanje pravilnosti in razpoložljivosti informacij, ko so te potrebne pooblaščenim uporabnikom ter za vzdrževanje nemotenega dostopa. Nasprotje razpoložljivosti je zavrnitev storitve (angl. Denial of Service – DoS). Povzročiteljev namen je doseči ohromitev storitve ali storitev z napadom računalniškega črva, da ta postane nedosegljiva uporabniku. Največkrat napadalec uporabi omrežja "*okuženih*" računalnikov oz. drugih ranljivih naprav, nad katerimi so predhodno pridobili nadzor (angl. Botnet). Napad se torej izvaja iz več deset ali sto različnih naprav hkrati. Zloraba razpoložljivosti se lahko zgodi tudi nenamerno, ko recimo pride do prekinitve storitve z električno energijo ali prekinitve telekomunikacijskih storitev zaradi napak na strani ponudnika storitev ali napak zaposlenih. Ukrepe za ublažitev groženj razpoložljivosti je mogoče zaslediti pod pojmom upravljanje neprekinjenega poslovanja (angl. Business Continuity Management – BCM), ki vključuje priporočila in dobre prakse po standardu ISO 22301 (Bojanc, Jerman-Blažič & Tekavčič, 2014, str. 24).

Vsaka zaustavitev procesa se meri v stroških, ki se kažejo kot stroški zaustavitve, čakanja, ponovnega zagona, stroški zakasnjenih dobav, izguba posla ali celo ugleda in dobrega imena, zato je rešitev za preprečitev razpršenega izvajanja storitev na več geografsko ločenih lokacijah. ISO 22301 je prvi svetovni mednarodni standard upravljanja neprekinjenega poslovanja. Standard je razdeljen na deset glavnih klavzul, ki opredeljuje področja uporabe, normative, izraze ter definicije. Sledijo zahteve standarda s proaktivnim pristopom za zmanjševanje učinka incidenta, opredeljene so tudi kritične funkcije, ki jih je potrebno vzdrževati v času kriznega dogodka in so osnova za neprekinjeno poslovanje, zmanjševanje izpada med dogodkom in učenja iz napak ter nadgrajevanja odpornosti sistema za uspešno nadaljnjo odpornost na podobne izpade storitev. Za učinkovitejše izvajanje neprekinjenega poslovanja je priporočena tudi souporaba standardov ISO 27031, ISO 24762, ISO 22399, ISO 27001, PAS 200, PD 25666 in PD 25111, ki se osredotočajo na človeške vidike neprekinjenega poslovanja v fazi načrtovanja (Bojanc, Jerman-Blažič & Tekavčič, 2014, str. 24; Samonas & Coss. 2014).

Qadir in Quadri (2016) izpostavljata, da klasična triada CIA, kot je prikazana na sliki 1 obravnava vse tri atribute varnosti enakovredno, medtem ko v praksi obstaja odvisnost. Ta odvisnost prikazana na sliki 4 je, da imamo lahko razpoložljivost, tudi če nimamo zaupnosti in celovitosti, vendar ne moremo imeti zaupnosti in celovitosti, če nimamo razpoložljivih informacij, kadar jih potrebujemo. Poudarjata, da je v praksi informacijske varnosti razpoložljivost ključnega pomena in predstavlja temelj varovanja informacij.

Za primer vzemimo, da pooblaščeni uporabnik nima dostopa do informacij, ko jih potrebuje. Če temeljna predpostavka razpoložljivosti ni izpolnjena, potem v praksi ne potrebujemo ne celovitosti in ne zaupnosti. Če nimamo zagotovljenega dostopa, ne moremo uporabiti naprednih metod šifriranja podatkov ali načina nadzora nad informacijami. Vsi varnostni mehanizmi dobijo svoj pomen ter vrednost, ko imajo pooblaščeni uporabniki dostop do informacij in virov, ko jih potrebujejo v obliki, ki ohranja vrednost in izpolnjuje njihov namen (Qadir & Quadri, 2016 str. 186).

*Slika 4: Spremenjen in realističen model prakse informacijske varnosti*




*Prirejeno po Qadir & Quadri (2016).*

## 1.4 Izzivi varovanja informacij in stroški informacijske varnosti

Na informacijsko varnost ne moremo gledati kot na samostojno entiteto, saj gre za celo vrsto varnostnih ukrepov, zato jo je potrebno obravnavati kot neprekinjen proces. Informacijska varnost združuje številne različne vidike in pristope, pri čemer nobenega ni mogoče šteti za bolj ali manj pomembnega. To pomeni, da nobenega vidika ali pristopa ne smemo zanemariti. Če je eno področje ali del sistema varovanja prezrto, sistem ne bo deloval pravilno, kar predstavlja ranljivost. Vpliv ljudi oz. človeških dejavnikov bo vedno najranljivejši del informacijske varnosti katere koli organizacije, ker ljudje delamo napake in ljudje tudi programiramo algoritme. Pomanjkanje zavedanja in razumevanje tveganja v informacijski varnosti je eden največjih izzivov za učinkovito varovanje informacij v dobi digitalnega poslovanja. Iz dneva v dan je na voljo več varnostne

programske opreme, ki je zasnovana za izvajanje zelo specifičnih funkcij in uporaba te tehnologije pomaga zaščititi IS. Vendar tudi najbolj dovršena programska oprema, ki uporablja najnaprednejšo tehnologijo in tehnološko izpopolnjene algoritme, ne more zagotoviti 100-odstotno varnega okolja IS. Razlog je v temu, ker so ljudje vključeni v razvoj in izvajanje programske opreme, ljudje pa delamo napake. Človeški dejavniki so glavni razlog, zakaj so številni napadi na računalniške sisteme uspešni, saj človeška interakcija povzroči incident. Napaka po incidentu pa predstavlja za organizacijo tudi neko vrednost, saj se iz njih lahko marsičesa naučimo, če jih uspešno upravljamo v povezavi z managementom znanja (angl. Knowledge management) (Arachchilage & Love, 2014, str. 305–306).

Digitalna doba poleg izziva človeškega zavedanja in vpliva na varnost informacij prinaša tudi tehnološke izzive, zlasti vzpon uporabe tehnologije, ki temelji na internetu stvari (angl. Internet of things, v nadaljevanju IoT). V IoT obstajajo ranljivosti v komunikacijskih protokolih, ki med seboj povezujejo naprave z omrežjem in različnimi vrstami vmesnikov za prenos podatkov, v in iz virov v oblaku ter strojne in programske opreme naprav IoT. Nedvomno sta varnost in zasebnost IoT tehnologije kot celote ter tudi občutljivi podatki, s katerimi operira v IS in ki morajo neprekinjeno zagotavljati storitev, resnično zahteven varnostni izziv za uporabnike in ponudnike IKT v času digitalizacije (Hughes-Lartey, Li, Botchey & Qin, 2021, str. 2).

Platforma 5G je nova in zapletena tehnologija, ki zahteva večjo varnost kot omrežja prejšnjih generacij. 5G omrežje močno vpliva ne samo na telekomunikacije, temveč tudi na zagotavljanje tehnoloških platform za razvijanje pametnih mest (angl. Smart City), robnega računalništva (angl. Edge Computing), avtonomnih avtomobilov (angl. Autonomy Vehicles) in inteligentnih električnih omrežij (angl. Smart Grid). Če samo karikiramo, lahko z DoS napadom iz več sistemov sprožimo porazdeljeno ohromitev storitve (angl. Distributed Denial of Service – DDoS). Tak napad ne vpliva samo na prekinitev storitev omrežij zgolj z ogrožanjem ene same naprave znotraj IS, temveč ogroža celotno sistemsko omrežje z vsemi povezanimi napravami v sistem. Takšen napad lahko enačimo s terorističnim dejanjem (Petrov & Janevski, 2020, str. 1329).

Obdobje med globalno zdravstveno krizo, pri čemer so v številnih državah in institucijah opravljali delo na daljavo, se je v skladu s tem dejstvom število napadov močno povečalo. Analitiki Evropske organizacije za kibernetsko varnost (angl. The European Cyber Security Organisation – ECSO) navajajo, da se je v času samoizolacije in karanten pričakovano dvignil trend napadov v primerjavi z leti poprej. Kot razlog za to navajajo eksponentno rast vrednosti kripto valut (angl. Cryptocurrency), ki so napadalce motivirale, da se osredotočijo na uporabnike tehnologije rudarjenja. K temu je pripomogel tudi vzpon uporabe IoT naprav, ki so postale tarče DDoS napadov. Kot glavni razlog pa navajajo finančno negotovost, ki jo je povzročila pandemija, saj je poglavitni namen takšnih napadov finančna korist. V bodoče bodo z razvojem novih naprednih in

pametnih tehnologij nedvomno svoj davek terjala tudi varnostna vprašanja in z njimi povezani izzivi v sistemih. Tehnološki napredek izpopolnjuje tudi napadalce, ki postajajo glede na vire močnejši in spretnejši pri izrabi zaznanih varnostnih ranljivosti v sistemih in protokolih. V prihodnje bo bistvenega pomena učinkovito ozaveščanje zaposlenih o varnosti informacij ter vseh novitetah pri zaznavi kibernetskih napadov in informacijskih incidentov, ki so postali del vsakdana v globalnem okolju razvoja novih tehnologij (Kappel, 2020).

Po navedbah italijanskega podjetja na področju varnosti IS – Leonardo, je kibernetski kriminal leta 2021 stal več kot 6000 milijard dolarjev (5700 milijard evrov). Od širjenja pandemije koronavirusne bolezni 2019 (angl. Coronavirus disease 2019 – COVID-19) in vojne v Ukrajini so kibernetski napadi postali številčnejši in bolj sofisticirani ter so povzročili več škode kot leta poprej. Skoraj petina napadov je bila usmerjenih v Evropo. S tem informacijski in kibernetski kriminal postaja vse obsežnejša globalna grožnja. Evropska komisija in države članice Evropske unije (angl. European Union, v nadaljevanju EU), morajo gledati na informacijsko varnost kot na ključni dejavnik, da bi zagotovili svojo digitalno suverenost in strateško avtonomijo. Sistem informacijske varnosti je še vedno preveč birokratiziran in samo prostoru EU primanjkuje 200.000 strokovnjakov, da bi pokrili trenutne potrebe povpraševanja po strokovnjakih informacijske varnosti. Mednarodni denarni sklad (angl. The International Monetary Fund – IMF) izraža zaskrbljenost, da je vojna v Ukrajini povzročila resno globalno nevarnost glede kibernetskih napadov, ki so usmerjeni predvsem v sistemsko pomembne finančne institucije. Če bi bili ti napadi uspešni, bi lahko povzročili izgubo zaupanja v širši finančni sistem, kar bi negativno vplivalo na globalno finančno stabilnost, posledice bi pa nosilo celotno globalno gospodarstvo (News in France, 2022).

Morgan (2020) napoveduje, da bodo svetovni stroški kibernetskega kriminala v naslednjih petih letih narasli za 15 % na letni ravni. Leta 2025 naj bi dosegli 9.550 milijarde EUR (10.500 milijard USD), v primerjavi z 2730 milijardi EUR (3000 milijardami USD) v letu 2015. To napovedovanje predstavlja največji prenos gospodarskega bogastva v zgodovini, tvega globalne spodbude inovacij ter naložb, predstavlja eksponentno večjo škodo, kot so jo povzročile naravne nesreče v enem letu, in bo donosnejši od celotne svetovne trgovine z vsemi prepovedanimi drogami. Najnevarnejši in stroškovno najdražji so dolgotrajni napadi oz. napredna trajna grožnja (angl. Advanced Persistent Threat – APT). Njihovo odkrivanje je zelo težko, saj napadalci uporabljajo prefinjene tehnike in orodja, da se izognejo varnostnim kontrolam napadenega sistema, v katerega se infiltrirajo.

## 1.5 Pravna podlaga varovanja informacij

Informacijska varnost pomeni varstvo podatkov in informacijskih sistemov pred nezakonitim dostopom, nezakonito uporabo, razkritjem, odtujitvijo, spremembo ali

uničenjem. Ogrodje informacijske varnosti predstavlja zaupnost, celovitost in razpoložljivost podatkov ter informacij ne glede na obliko. Organizacije kopičijo velike količine zaupnih informacij o zaposlenih, strankah, poslovnih partnerjih, proizvodih, raziskavah, finančnem položaju idr. Večina teh informacij je zbrana, obdelana in shranjena v IS ter prenesena skozi mreže na druge računalnike in strežnike. Zaupni podatki o strankah ali poslovnemu modelu bi lahko padli v neprave roke. Posledica bi lahko vodila v izgubo posla, ugleda ali izgubo dobrega imena. Varovanje zaupnih podatkov je tako poslovna, kot v mnogih primerih tudi etična in pravna zahteva. V ta namen poznamo pravno ureditev informacijske varnosti na več ravneh, od regionalne do lokalne z vidika zakonov, uredb in direktiv (Talimonchik, 2019, str. 2–4).

### 1.5.1 Direktiva EU 2016/1148

Vzporedno s Splošno uredbo o varstvu osebnih podatkov, ki je opisana v poglavju 1.5.3, je nastajala tudi direktiva EU 2016/1148 (angl. Network and Information Security, v nadaljevanju NIS). Cilj direktive NIS je zagotoviti visoko enotno evropsko harmonizirano raven varnosti omrežij in informacij z razširitvijo predpisanih varnostnih ukrepov na širši nabor subjektov. Namen te direktive je spodbujati razvito kulturo obvladovanja tveganj in obvladovanja incidentov v zasebnem in javnem sektorju. Cilj direktive je tudi zapolnitev vrzeli skupne ravni omrežne in informacijske varnosti, ki bi zagotovila enotni digitalni trg in nemoteno delovanje notranjega evropskega trga, saj so vprašanja kibernetske in informacijske varnosti v javnih omrežjih najpomembnejši cilj iskanja rešitev za boj proti digitaliziranemu kriminalu (European Commission, 2021).

Za zagotovitev visoke skupne ravni varnosti omrežij in informacij v EU imajo države članice teritorialno in zunanjo teritorialno pristojnost. Ta direktiva zajema ponudnike digitalnih storitev s sedežem v EU in tudi ponudnike digitalnih storitev s sedežem zunaj EU, vendar omogoča storitve prenosa znotraj EU. Če ima ponudnik digitalnih storitev sedež v številnih državah članicah, velja zakonodaja, kjer je sedež organizacije. Če ponudnik storitev nima sedeža v EU, ampak svoje storitve opravlja samo v EU, mora ponudnik storitev imenovati predstavnika v državi članici, kjer ponuja storitve. Zastopnik mora imeti sedež v eni od držav članic EU, kjer se ponujajo storitve, in šteje se, da je ponudnik v pristojnosti države članice, kjer je zastopstvo pravno ustanovljeno. Cilj direktive EU 2016/1148 je doseči splošno visoko raven varnosti omrežij ter IS po vseh državah članicah EU. Direktiva se osredotoča na javno-zasebno sodelovanje in državam članicam postavlja zahtevo, da vzpostavijo strategijo informacijske varnosti. Glavna skrb je dokumentiranje informacijsko-varnostih incidentov ter njihov jasen pregled. Vsaka država članica mora imeti organ, ki upravlja incidente na področju informacijske varnosti (angl. Computer Emergency Response Team, v nadaljevanju CERT). Za doseg splošne visoke ravni varnosti direktiva NIS določa obveznosti poročanja državam članicam in organom CERT-a ter Komisiji EU (angl. The European Commission) o stanju napada na IS in povzročenih incidentih. Komisija vsaki dve leti oceni izvajanje direktive. Poleg

CERT-ov vsaka država članica imenuje en organ, ki je kontaktna točka s Komisijo EU z namenom pridobivanja informacij o incidentih na IS v državi. Od začetka veljave direktive so se obveznosti poročanja razširile na vsakega ponudnika storitev, tako javnega kot zasebnega, ki delujejo pod kritično infrastrukturo in mednarodno pomembnimi storitvami. Direktiva NIS opozarja na potrebo po skupnih točkah in razumevanju varnosti IS, kar velja za temelj pridobitve enako visoke ravni varnosti za vse IS (European Commission, 2021; European Parliament & Council of the European Union, 2016a).

### 1.5.2 Zakon o informacijski varnosti

Slovenija je z implementacijo Zakona o informacijski varnosti (ZinfV), Ur. L. RS, št. 30/2018, 95/2021, 130/2022 – ZEKom-2 in 18/2023 – ZDU-1O, v svoj pravni red prenesla evropsko direktivo NIS, katere namen je zagotoviti visoko raven varnosti omrežij in IS v EU, ki so bistvenega pomena za nemoteno delovanje države v vseh varnostnih razmerah ter zagotavljajo bistvene storitve za ohranitev ključnih družbenih in gospodarskih dejavnosti. Zakon je pričel veljati 11. maja 2018 ter določa minimalne varnostne zahteve in zahteve za priglasitev incidentov zavezancev zakona. Predstavlja tudi konkretno zakonsko podlago in pomembnost zavedanja informacijske in kibernetske varnosti. Zakon o informacijski varnosti morajo spoštovati institucije, organizacije, ustanove ter podjetja, ki so bistvene za nemoteno delovanje države in izvajanje storitev v vseh razmerah. Zakon zavezance deli v tri glavne kategorije: ponudnike digitalnih storitev, organe državne uprave in izvajalce kritičnih storitev, ki jih določa vlada z naslednjimi merili (ZinfV):

- subjekt zagotavlja storitev, ki je bistvena za ohranjanje ključnih gospodarskih in družbenih dejavnosti;
- subjekt zagotavlja storitve, ki je odvisna od omrežij in IS;
- varnostni incident oz. kibernetski napad bi imel pomembno negativni vpliv na zagotavljanje teh storitev.

ZinfV zavezancem narekuje, da morajo imenovati kontaktno osebo za informacijsko varnost ter njenega namestnika, ki sta pristojna za komunikacijo in poročanje o incidentih organu za odzivanje na varnostne dogodke (angl. Computer Security Incident Response Team – CSIRT); v Sloveniji je to institucija SI-CERT, ki je pristojna za odzive na incidente s področja informacijske varnosti. Zavezanci morajo v svojo varnostno organizacijsko politiko in infrastrukturo implementirati konkretne tehnične in organizacijske ukrepe za ustrezno prepoznavanje, obvladovanje, preprečevanje in zmanjšanje vpliva varnostnih incidentov. V kolikor se varnostni incident zgodi, ga morajo zavezanci, ki so zakonsko primorani spoštovati zahteve zakona, nemudoma prijaviti brez odlašanja. Zakon med drugim nalaga transparenten sistem upravljanja varovanja informacij in sistem upravljanja neprekinjenega poslovanja, ki mora vsebovati najmanj analizo tveganja, politiko neprekinjenega poslovanja, načrt obnove delovanja ključnih

sistemov ter seznam sistemov in načrta odzivanja na incidente z jasnim protokolom obveščanja pristojnemu organu CSIRT oz. SI-CERT-u (28. člen ZInfV).

Zakon sam po sebi ne zagotavlja višje stopnje informacijske varnosti, je pa pomemben napredek pri zavedanju o potencialni poslovni škodi v primeru incidenta na IS ali kibernetskemu napadu. Zgolj učinkovita obramba ni samo domena tehnologije in procesov, temveč je bistveni del tudi organizacijska kultura ter zavedanje zaposlenih o informacijski varnosti.

### 1.5.3 Uredba EU 2016/679

Namen splošne uredbe o varstvu osebnih podatkov (angl. General Data Protection Regulation, v nadaljevanju GDPR), da evropskim državljanom »*vrne*« nadzor nad osebnimi podatki ter tako okrepi zasebnost kot eno od temeljnih človekovih pravic. Da bi to dosegli, uredba vodi načela, iz katerih izhajajo posamezne zahteve, ki jih je treba izvajati v organizacijah, ki obdelujejo osebne podatke vseh državljanov EU. Uredba je še posebej pomemba v času hitro razvijajoče se IT ter njene vsesplošne uporabe. Vendar lahko ta načela pomagajo tudi podjetjem pri usmerjanju k večji skladnosti IS. V smislu informacijske varnosti osebne podatke obravnavamo kot ključne informacije, ki jih imajo vse organizacije, in jih morajo ustrezno zaščititi. Zaradi tega sta varstvo osebnih podatkov in informacijska varnost medsebojno tesno povezani kategoriji. Številne zahteve GDPR so podobne ali celo zajete v standardu ISO 27001. Standard ISO 27018 prispeva h konkretizaciji načel varstva osebnih podatkov in GDPR obveznosti ter načela ISO 29100 (Barolli, Hyra & Tomco, 2022, str. 2). Z direktivo je bilo razvitih šest načel zasebnosti, ki so opredeljene v 5. členu GDPR uredbe (European Parliament & Council of the European Union, 2016b):

- Zakonitost, poštenost in preglednost (angl. Lawfulness, fairness and transparency)

Načelo je sestavljeno iz treh delov, od katerih je najpomembnejša presoja zakonitosti, ki zahteva, da je obdelava podatkov v skladu s 5. členom uredbe, ki določa, da je potrebno podati soglasje. Upravljalec podatkov mora opisati proces obdelave oz. t.i. tokokrog podatkov, ki se mora ujemati s tem, kar se je oz. se bo v resnici izvedlo s podatki – preglednost (angl. Transparency), in ne sme odstopati iz obsega primarnega soglasja – načelo poštenosti (angl. Fairness). Če je potrebna nadaljnja obdelava podatkov, je potrebno najprej pridobiti novo soglasje.

- Omejitev namena (angl. Purpose limitations)

Posamezniku, na katerega se nanašajo osebni podatki, mora biti naveden jasen namen dejavnosti za zbiranje podatkov v obvestilu o zasebnosti. Tega namena ni mogoče razširiti brez nove privolitve. V skladu s 5. členom je zbiranje podatkov dovoljeno le za izrecne

oz. določene in zakonite namene. To v praksi pomeni, da je prodaja ali prenos zbirke osebnih podatkov na tretje osebe nezakonita ter velja za hudo kršitev, kot tudi če njihova uporaba podatkov presega obseg iz prvotnega obvestila o zasebnosti, ki je bila izražena v soglasju.

- Minimizacija podatkov (angl. Data minimisation)

Za vsako zbiranje podatkov je obvezno zbrati le tiste vrste podatkov, ki so dejansko potrebni za izpolnitev namena. V 5. členu je določeno, da bi morali biti osebni podatki ustrezni in omejeni na tisto, kar je potrebno glede na namen, za katerega se podatki zbirajo in obdelujejo. Uporaba in zbiranje t.i. odvečnih podatkov je prepovedana, saj je glavni razlog oz. cilj obveznosti zmanjševati količino podatkov.

- Natančnost (angl. Accuracy)

Cilj tega načela je zaščititi posameznike, na katere se nanašajo zbrani osebni podatki, pred napačnimi odločitvami, ki temeljijo na profiliranju in lahko zmanjšajo tveganje za krajo identitete, kar se običajno zgodi pri zastarelih podatkih. Načelo zahteva, da morajo biti podatki natančni in po potrebi posodobljeni.

- Omejitev shranjevanja (angl. Storage limitations)

Ko je namen zbiranja podatkov izpolnjen ali ta ne velja več, je potrebno podatke trajno odstraniti s strežnikov. Ta zahteva ne velja za določene subjekte oz. jih je mogoče povzeti za arhivske namene, kot so npr. podatki v zdravstvenih kartotekah. Načeloma skuša GDPR uredba količino podatkov optimizirati, da bi zmanjšala obseg morebitnih kršitev oz. možnost zlorabe.

- Celovitost in zaupnost (angl. Integrity and confidentiality)

Zadnje načelo je neposredno povezano s splošno informacijsko varnostjo organizacije iz tehničnih kot tudi organizacijskih vidikov, medtem ko GDPR obravnava zasebnost na splošno in ne v konceptu kibernetske oz. informacijske varnosti. To načelo zasebnosti povezuje kibernetsko in informacijsko varnost z izjavo, da je nujno varstvo osebnih podatkov obravnavati na ustrezen način z izvajanjem ustreznih tehničnih in organizacijskih ukrepov. Namen tega je sklicevanje na najboljše prakse, standarde in okvirje, ki vodijo izvajalce informacijske varnosti pri izvajanju ustreznih zaščitnih ukrepov v omrežjih organizacij za zaščito pred kršitvami podatkov in zlonamernim vdorom.

Z vidika varovanja podatkov oz. informacij je potrebno tudi izpostaviti, da ima posameznik, na katerega se nanašajo osebni podatki, pravico do obveščenosti o načinu

obdelave in o tem, kdo jih obdeluje, saj je ta pravica neposredno povezana z določili o pravici dostopa do podatkov. Posamezniku se mora omogočiti tudi pravico do popravka. Bodisi da podatek popravijo sami bodisi z zahtevo na podlagi kritičnosti do informacij. Pravica do ustreznega odločanja daje posamezniku tudi pravico, da zahteva človekovo posredovanje za zaščito pred samodejnim odločanjem, ki ima pravne učinke. V praksi se takšen primer najpogosteje izvaja pri ocenjevanju kreditne sposobnosti. Ena najbolj spornih pravic v skladu z GDPR je pravica do pozabe oz. pravica do izbrisa. Vodilo te pravice je, da je treba podatke izbrisati, takoj ko namen zbiranja podatkov ni več veljaven ali posameznik, na katerega se nanašajo osebni podatki, umakne soglasje z uporabo svoje pravice do ugovora. Pomembna pravica posameznika je tudi pravica do prenosljivosti podatkov, ki posamezniku, na katerega se nanašajo osebni podatki, omogoča ne samo dostop do kopije, temveč tudi zahtevo podatkov v prenosljivi obliki ali njihov prenos drugemu upravljalcu podatkov. Ta prenos se lahko izvede samodejno ali preko strojno berljive oblike, kot je datoteka, kjer so vrednosti, ločene z vejico (angl. A comma-separated values – CSV) (European Parliament & Council of the European Union, 2016b).

#### *1.5.3.1 Ocena učinka na varstvo podatkov*

Varstvo podatkov zahteva učinkovito izvajanje zasebnosti podatkov, kar je večinoma tehnična domena. Konvencionalna metoda pri informacijski varnosti je ocena tveganja, katere namen je prepoznati in analizirati tveganja ter pridobiti prednostno razvrstitev tveganj, za katero je mogoče uvesti ukrepe za njihovo minimiziranje – ISO 27005. V poslovnem smislu se izvede analiza vpliva na poslovanje (angl. Business Impact Analysis, v nadaljevanju BIA), da dobimo seznam procesov, razvrščenih po prednostnih nalogah glede na kritičnost. Na ta način lahko oblikujemo dobro zasnovan načrt neprekinjenega poslovanja (angl. Business Continuity Planning – BCP), ki omogoča učinkovito in hitro obnavljanje glavnih procesov, hkrati pa tudi izvajanje kontrol, ki se odzivajo na tveganje neuspehov procesa. Podobno kot BIA tudi GDPR zahteva analizo izvedbe ocene učinka na varstvo podatkov (angl. Data Protection Impact Assessment, v nadaljevanju DPIA) za oceno tveganj pri obdelavi nekaterih osebnih podatkov v novih okoljih. V osnovi je za vse nove storitve in procese, ki zahtevajo uporabo osebnih podatkov, priporočljivo izvesti DPIA in dokumentirati njegove korake za dokazovanje skladnosti. Čeprav je ocena izbirna, je obvezna, če se načrtuje obdelava podatkov iz posebnih kategorij (9. člen GDPR). Glavni cilj DPIA je pridobiti informacije, če ima obdelava podatkov visoko tveganje za kršitev pravic in svoboščin posameznikov, na katere se nanašajo osebni podatki. Zato upošteva vpliv na posameznike, na katere se nanašajo osebni podatki, in ne tako kot BIA, katere glavni cilj je finančni vpliv na družbo. Kljub temu sta ti dve oceni med seboj prepleteni, ker zaščita podatkov pomeni informacijsko varnost v omrežju organizacije skupaj z varnimi programskimi aplikacijami, ki ne razkrijejo informacij, kadar pride do incidenta oz. nedovoljenega posega v IS (ICO, 2018).

Kar zadeva uredbo GDPR, je ključnega pomena, da se v varnostno politiko organizacije vključi formaliziran postopek DPIA, saj se s tem najučinkoviteje izognemo kršitvam in nepravilnostim v projektih, če pred začetkom njegovega izvajanja naredimo analizo DPIA. Tako minimiziramo nastanek nezakonitosti ali takšno tveganje celo izničimo. Takšna obveznost je lahko na prvi pogled videti kot nevšečnost in administrativna ovira zaradi zakonodaje. DPIA analiza hitro signalizira, če se pokažejo pomisleki glede obvladovanja zasebnosti, saj jim ocena to pomaga prepoznati, pred kršitvami pa lahko sprožimo dodatne zaščitne ukrepe že v fazi načrtovanja. DPIA kot instrument pomembno pomaga organizaciji izvajati samoregulacijo in preglednost, ki se odraža v zavedanju organizacije glede potrebe do zasebnosti (Hert & Papakonstantinou, 2016, str. 179–181).

Izdelanih je več smernic za izvedbo ocene učinka na zasebnost (angl. Privacy Impact Assessments – PIA). Eden prvih in najpogosteje uporabljenih okvirjev je okvir ocene vpliva na zasebnost (angl. Privacy Impact Assessment Framework – PIAF), ki je bil dokončno razvit leta 2012 in predlaga šeststopenjski postopek. Nastajati je začel že ob načrtovanju oz. začetku razprave o GDPR (ICO, 2018).

Posledica ugotovitev o neskladnosti GDPR uredbe je zavezanost EU, da uveljavi zaščito zasebnosti vseh državljanov EU. V nasprotju z evropsko direktivo iz leta 1995, ki je predhodnica GDPR uredbe, so globe zelo visoke in organizacije spodbujajo k sprejetju upravljanja zasebnosti v skladu z uredbo. Globe so denarne narave in se presojajo glede na težo kršitve. Spodnja meja nalaga globo v višini 10 milijonov EUR ali 2 % letnega prometa v preteklem letu, medtem ko zgornja meja določa 20 milijonov EUR ali 4 % letnega prometa. Pri presoji se ponovno uporabi merilo večje vsote znotraj teh meril glede na kršitev zasebnosti. Zgornjo mejo kazni se uporablja predvsem za kršitve, ki vključujejo posebne kategorije osebnih podatkov, kot so rasa, spolna usmerjenost idr. posebno občutljivi osebni podatki (ICO, 2018; Hert & Papakonstantinou, 2016, str. 188).

### 1.5.4 Zakon o varstvu osebnih podatkov

Podatki v informacijski družbi postajajo vse bolj dragoceno gonilo sodobnega poslovanja, a hkrati tudi vse bolj občutljiva človeška dobrina. Zloraba osebnih podatkov pomeni hud poseg v človekovo dostojanstvo, zasebnost ter integriteto. Zakon o varstvu osebnih podatkov (ZVOP-2), Ur. l. RS, št. 163/2022 prinaša pomembne novosti z implementiranjem določb iz uredbe GDPR. ZVOP-2 informacijskemu pooblaščencu prinaša pooblastila in odgovornost, da ob kršitvah izreka globe. Informacijski pooblaščenec je od uveljavitve ZVOP-2 definiran kot prekrškovni organ, ki je odgovoren za odločanje o prekrških iz posebnega dela ZVOP-2. ZVOP-2 je razširil tudi obvezo po imenovanju pooblaščene osebe za varstvo osebnih podatkov (angl. Data Protection Officer – DPO) na celotni javni sektor. Z uvedbo registra nadomešča in ukinja evidenco dejavnosti, ki jo nalaga upravljalcu in obdelovalcu osebnih podatkov ter jih ustrezno hrani

pri upravljalcu. Novost iz implementirane uredbe prinaša tudi ločeno naslavljanje vodenja evidenc vstopov in izstopov iz službenih prostorov. Evidentiranje vstopov in izstopov lahko vsebuje le osebne podatke, kot so: osebno ime, številka in vrsta uradnega identifikacijskega dokumenta, naslov prebivališča, zaposlitev, registrska številka vozila, datum in ura ter razlog vstopa in izstopa v prostore. ZVOP-2 skladno s splošno uredbo določa tudi definicijo povezovanja zbirk osebnih podatkov, kjer mora javni sektor pred pričetkom zbiranja in povezovanjem zbirk za upravljavca izdelati oceno učinka in se posvetovati z informacijskim pooblaščencem. Zakon posega tudi v določbe o uporabi tehnologije biometrije. Te določbe so ločene na javni in zasebni sektor in se jih ne sme hraniti na napravah, ki lahko identificirajo posameznika. Uporablja se lahko izključno na podlagi zakona, saj je nujna zaščita posameznikov ter premoženja. Na področju videonadzora zakon uveljavlja pomembno spremembo o vsebini obvestila o videonadzoru, ki ga mora upravljalec nadgraditi. ZVOP-2 namreč predvideva, da je posameznik o videonadzoru ustrezno obveščen le, če tovrstno obvestilo prebere, še predno se sam videonadzor izvede. Ustrezno ureja tudi videonadzor na javnih površinah. Ta je dovoljen le, kadar je to upravičeno z nevarnostjo za življenje, osebno svobodo, telo ali zdravje ljudi. Vpogled, uporaba in posredovanje posnetkov so dopustni le za naštete namene in morajo imeti urejeno ustrezno sledljivost. Pri obdelavi osebnih podatkov zakon od upravljavca zahteva, da posamezniku, katerega osebne podatke obdeluje, zagotovi jasne informacije glede načina in obsega obdelave, tveganj in ukrepov, ki jih je sprejel, da se lahko podatke ustrezno zaščiti. V tretjem poglavju ZVOP-2 ureja varstvo osebnih podatkov in ukrepe za njihovo zagotavljanje. Gre za nabor ravnanj, ki s pomočjo tehničnih in organizacijskih postopkov ter ukrepov preprečijo, da bi ostali podatki prišli v roke nepooblaščenim osebam, se nepooblaščeno uporabljali, brisali, spreminjali, uhajali ali izgubili. Novost je vodenje dnevnika obdelave. Zakon določa, kdo ga vodi, kaj mora vsebovati, za katere namene se uporablja in kako dolgo ga je potrebno hraniti. V primeru zaznane kršitve varnosti osebnih podatkov ZVOP-2 določa, da mora upravljalec o kršitvi obvestiti pristojni organ najkasneje v roku 72 ur po zaznani kršitvi. GDPR dopušča državam članicam EU različno implementacijo uredbe v njihovo nacionalno zakonodajo. Poudariti je treba, da se je Slovenija odločila za implementacijo uredbe na zahtevnejši ravni od predlagane v splošni uredbi, kar lahko predstavlja izziv pri razvoju storitev in uporabi IT, ki so razvite in standardizirane za celotno EU (Prelesnik in drugi, 2023; ZVOP-2). Čeprav sama uredba GDPR ni zasnovana za namen informacijske varnosti, je dober vodnik za ustrezno obravnavo varnosti in zaščite podatkov v zgodnejših fazah. Za poslovanje je bistveno, da vzpostavlja načelo odgovornosti, kjer je vsako podjetje odgovorno za pravilno implementiranje uredbe, njeno izvajanje in pravno odgovornost (Barolli, Hyra & Tomco, 2022).

## 1.6 Standardi in okvirji upravljanja informacijske varnosti

Upravljanje IT postavlja strukturo okoli tega, kako podjetje usklajuje svojo IT strategijo s poslovno strategijo in zagotavlja, da podjetje kot celota ostaja na zastavljenih poteh za

doseganje poslovnih in IT ciljev, hkrati pa upravljanje IT opravlja še merjenje uspešnosti IT in razvija strategije za naložbe iz področja IKT. Za uspešno upravljanje in usklajevanje IT strategij s poslovnimi cilji in strategijami potrebujemo okvirje, ki pomagajo k uspešnemu uresničevanju zastavljenih ciljev v skladu s poslanstvom (Hadlington & Chivers, 2020). Da ugotovimo, kateri okvir upravljanja IT je pravi za določeno organizacijo, pa si je potrebno zastaviti vprašanja, kako oddelek IT znotraj organizacije deluje na splošno, katere ključne meritve potrebuje za upravljanje varnosti in drugih IKT operacij ter kakšen donos IT podjetju vrača od naložbe, ki jo investira. Uspešne organizacije IT upravljanja ne podcenjujejo, temveč je enakovredno v hierarhični strukturi z drugimi temeljnimi poslovnimi funkcijami (Von Solms, 1999 str. 51).

Organizacije za varnost informacij in učinkovito upravljanje varnosti implementirajo različne standarde, ki poudarjajo pomen IT v organizacijah, kjer je upravljanje IT ključnega pomena za učinkovito vzdrževanje in izvajanje storitev za učinkovito poslovanje in zasledovanje poslanstva. Družina standardov ISO 27000 je znana kot okvir za uvedbo sistema upravljanja informacij in ima široko področje uporabe, ki se uvaja v vseh organizacijah ne glede na velikost. ISO 27000 je družina 45 standardov, ki obravnavajo tehnična, administrativna in organizacijska vprašanja v zvezi z varnostjo informacij, varstvom podatkov in kibernetsko ter informacijsko varnostjo (Taherdoost, 2022, str. 3–9).

### 1.6.1 Standardi družine ISO / IEC 27000

ISO 27001 je temeljni standard vseh drugih standardov in okvirjev v SUIV. Noben standard nima tako široke pokritosti, kot jo na področju varnosti IT ponuja ISO 27001. Namen ISO 27001 je voditi organizacijo na ravni izvajanja SUIV, izvedljivega glede na poslovne potrebe organizacije. Organizacijo vodi k izvajanju strukturiranega sistema za upravljanje informacijske varnosti s pristopom ocene tveganja in analize poslovnega vpliva, ki vključuje najboljše prakse tega okvirja pri upravljanju obstoječih sistemov. V standardu ISO 27001 niso določene nobene zahteve za katero koli posebno IT, vendar standard vsebuje zahteve za osredotočeno upravljanje procesov po SUIV, zato predstavlja tudi osnovo za identifikacijo osnovnih procesov iz SUIV. Družina standardov ISO 27000 ne predstavlja zgolj ISO 27001, ampak vsebuje serijo standardov za nadzor varnosti, ki jih je potrebno izvajati v sistemu SUIV. ISO 27001 je tesno povezan s standardom ISO 27002, ki daje smernice za organizacijske standarde informacijske varnosti ter prakse upravljanja informacijske varnosti, vključno z izvajanjem in upravljanjem kontrol, pri čemer upošteva okolje organizacije za varovanje informacij (Disterer, 2013, str. 92–97). Standardi iz družine ISO 27000 so (ISO 27000):

- ISO 27000 – SUIV (pregled standarda in besedišče);
- ISO 27001 – Upravljanje informacijske varnosti;
- ISO 27002 – Varnostne tehnike (kodeks ravnanja pri nadzoru informacijske varnosti);

- ISO 27003 – Smernice za izvajanje SUIV;
- ISO 27004 – Merjenje informacijske varnosti;
- ISO 27005 – Obvladovanje tveganj informacijske varnosti;
- ISO 27006 – Zahteve za organe, ki izvajajo revizijo in certificiranje SUIV;
- ISO 27007 – Smernice za presojo SUIV;
- ISO 27008 – Smernice za revizorje glede izvajanja kontrol SUIV;
- ISO 27009 – Smernice za izvajanje kibernetske varnosti in zaščito zasebnosti;
- ISO 27010 in nadaljnji – Smernice za izvajanje tehnik upravljanja informacijske varnosti za medsektorske in med organizacijske komunikacije;
- ISO 27030 in nadaljnji – Standardi za tehnični nadzor in smernice za nadzor standarda ISO 27002.

### 1.6.2 Kontrolni cilji za informacijske in sorodne tehnologije

Obstajajo okvirji, ki pomembno vplivajo na upravljanje informacijske varnosti. Okvir kontrolnih ciljev za informacijske in sorodne tehnologije (angl. Control Objectives for Information and related Technology, v nadaljevanju COBIT 5), ima 90 % skladnost z ISO 27001, vendar je ISO 27001 veliko bolj podroben in natančno opredeljuje upravljanje varnosti. Prednost okvirja COBIT 5 je, da ne obravnava zgolj upravljanje informacijske varnosti, ampak se osredotoča na vso IT v podjetju. Organizaciji pomaga zagotoviti usklajenost med uporabo IT z zadanimi poslovnimi cilji. Obvladovanje IT zajema vodenje IT organizacijske strukture za potrebe IT po ciljih COBIT 5, kot odgovornost uprave organizacije. Za učinkovito delovanje IT mora vodstvo vzpostaviti notranji nadzor nad sistemom (ISACA, 2012). Organizacije z uporabo COBIT okvirja dosegajo (ISACA, 2012):

- ustvarjanje vrednosti z učinkovito in inovativno uporabo poslovne IT;
- zadovoljstvo poslovnih uporabnikov z vključevanjem v IT in ustvarjanjem storitev;
- skladnost z ustrezno zakonodajo, predpisi, pogodbenimi sporazumi, politikami in standardi;
- tesnejše prilagajanje poslovnih potreb z IT cilji.

COBIT 5 je zasnovan tako, da je njegov glavni namen pomagati vodstvu pri podpori odločanju, zato vsebuje ključne elemente, ki so potrebni za učinkovito vodenje ter razumevanje področja managementa informatike. COBIT 5 s svojim pristopom predstavlja nabor najboljših praks za uskladitev poslovnih ciljev z viri IT, tako da spodbuja sodelovanje med IT in drugimi oddelki z namenom minimiziranja tveganj pri izrabi virov IT. COBIT 5 predstavlja odlično ogrodje za poenotenje procesov v celotni organizaciji (ISACA, 2012).

### 1.6.3 Zbirka napotkov za upravljanje in uvajanje storitev informacijske tehnologije

Zbirka napotkov za upravljanje in uvajanje storitev informacijske tehnologije (angl. Information Technology Infrastructure Library, v nadaljevanju ITIL), predstavlja okvir najboljših praks, ki pomaga zagotavljati visokokakovostne informacijske storitve. Pristop, ki ga uporablja ITIL, je namenjen združevanju procesov, ljudi in tehnologije za podporo zagotavljanju storitev, razvoja ter vzdrževanja IT za končne uporabnike in stranke. ITIL okvir zagovarja, da je poslovni uspeh v veliki meri odvisen od stabilnosti, fleksibilnosti in integracije komponent IT z ostalimi storitvami. Če omrežje, baze podatkov ali strežniki prekinejo delovanje ali če incidenta ni mogoče odpraviti oz. tveganja ne obvladujemo, lahko to močno vpliva ne samo na poslovanje znotraj podjetja, temveč na vse storitve in končne uporabnike. Če lahko organizacija z večjo zanesljivostjo nemoteno zagotavlja storitve strankam, ima veliko večje možnosti za poslovni uspeh. Ker se potrebe strank in tehnologije hitro spreminjajo, je nujno, da imamo na voljo vrsto dobrih praks, ki bodo pomagale podjetju, da se hitreje prilagaja. ITIL zagovarja preprostost dobrih praks na način, ki je usmerjen v stranke, ponuja prilagodljive storitve in prinaša dodano vrednost. ITIL pomaga zagotoviti, da standardi procesov IT učinkovito prispevajo k splošni poslovni strategiji organizacije, se odlično integrira v povezavi z okvirjem COBIT 5 ter zagotavlja, da so viri IT dodeljeni na smiseln in dosleden način, v skladu s cilji organizacije (Ferreira Lopes, 2021, str. 293).

ITIL vsebuje pet osnovnih komponent (Ferreira Lopes, 2021, str. 294):

- veriga vrednosti storitev ITIL;
- ITIL prakse;
- vodilna načela ITIL;
- upravljanje;
- stalno izboljševanje.

Nabor najboljših praks je razdeljen v tri različice, in sicer splošne prakse, prakse upravljanja storitev in prakse tehničnega upravljanja. Zajema štiri različne dimenzije, ki so prepletene s praksami ITIL ter verigo vrednosti, to so: organizacije, ljudje, informacije, IT, partnerji, dobavitelji in poslovni procesi. Namen teh prepletenih praks je pomagati ekipi za IT oz. oddelku informatike zagotavljati storitve ter vplivati na poslovno učinkovitost ter vodenje vseh procesov. Na IT ekipo vpliva s povečanjem učinkovitosti in produktivnostjo ekipe z ločevanjem različnih nalog upravljanja, odgovornosti, uporabe orodij ter vlog. Torej ITIL okvir ponuja zbirko znanj za doseganje zahtev sistema upravljanja storitev (Ferreira Lopes, 2021, str. 293–295).

### 1.6.4 Okvir za kibernetsko varnost ameriškega nacionalnega inštituta za standarde in tehnologijo

Prenovljen okvir ameriškega nacionalnega inštituta za standarde in tehnologijo za upravljanja kibernetske varnosti (angl. National Institute of Standards and Technology Cybersecurity Framework, v nadaljevanju NIST) je bil izdan leta 2017 po odredbi nekdanjega predsednika ZDA, Baracka Obame. NIST bi lahko primerjali s prilagojeno različico ISO 27001. Okvir NIST je še posebej cenjen v državah ZDA zaradi enostavnosti in celostnega pristopa k razumevanju informacijske varnosti iz vidika širokega spektra industrij. Zagotavlja skupni jezik za industrijo in vlado za obravnavo in upravljanje informacijskih in kibernetskih tveganj na podlagi poslovnih potreb, ne da bi postavili dodatne regulativne zahteve. Opredeljuje ukrepe, ki so koristni za zmanjševanje tveganj na področju kibernetske in informacijske varnosti (Taherdoost, 2022, str. 10). Dejanja NIST so združena v pet domen (Taherdoost, 2022, str. 10–11):

- Prepoznavanje (angl. Identify);
- Zaščita (angl. Protect);
- Zaznavanje (angl. Detect);
- Odziv (angl. Respond);
- Obnovitev (angl. Recover).

Vsaka od petih domen je organizirana na visoki ravni varnosti. Znotraj vsake domene so kategorije in podkategorije. Kategorije predstavljajo skupek dejavnosti znotraj domene; na primer kategorija pod domeno Zaščita je ozaveščanje in usposabljanje. Podkategorije predstavljajo posebne kontrole oz. dejanja, ki celovito dopolnjujejo kategorijo Zaščita. Primer podkategorije znotraj domene Ozaveščanje in usposabljanje je, da uporabniki razumejo vloge in odgovornosti. Podkategorije okvirja NIST imajo tudi povezavo z drugimi okvirji kibernetske in informacijske varnosti in upravljanja tveganj, ki povezujejo kontekst njihovega izvajanja z integracijo drugih standardov. S tem se celovito dopolnjujejo pri upravljanju IT. Vsaka podkategorija vsebuje več kontrol, ki so ovrednotene s pomočjo izvedbenih nivojev. NIST torej predstavlja okvir za oceno zrelosti informacijske varnosti organizacije iz katere koli panoge (Taherdoost, 2022, str. 10).

## 1.7 Sistem upravljanja informacijske varnosti

Uresničevanje informacijske varnosti ni enkraten projekt, ampak je cikličen ter ponavljajoči postopek. SUIV pomaga organizaciji pri varovanju občutljivih podatkov z vzpostavitvijo, delovanjem, pregledovanjem in izboljševanjem informacijske varnosti, ki obravnava vedenje zaposlenih, podatke ter tehnologijo. SUIV pomaga organizacijam, da vzpostavijo protiukrepe glede ranljivosti, povezanih z informacijsko varnostjo, kar zagotavlja varno osnovo za poslovno rast in izpolnitev več zakonskih pričakovanj in

zahtev glede informacijske varnosti za organizacije ter nenazadnje uspešno zasledovanje poslovnih ciljev in zadanega poslanstva (Taherdoost, 2022, str. 2–3).

SUIV je sestavljen iz različnih procesov, ki se začnejo z določitvijo varnostnih zahtev, ki se še naprej nadgrajujejo s strategijami in rezultati meritev. Večina varnostnih zahtev izhaja iz organizacije same, drugi viri varnostnih zahtev pa so lahko pravne, regulativne ali pogodbene narave. Na strukturo SUIV vplivajo vse varnostne zahteve organizacije, poslovni cilji, postopki, procesi ter nenazadnje tudi velikost in struktura organizacije. Za zaščito sredstev v organizaciji SUIV ponuja niz postopkov in smernic za upravljanje virov in dejavnosti. Poleg tega za zagotavljanje dosledne uporabe varnostnih načel, politike SUIV sestavljajo instrumenti in metode, ki jih mora vodstvo uporabljati za zadovoljevanje varnosti informacij pri vseh nalogah in aktivnostih, ki jih opravlja v poslovnih procesih (Helmke & Uebel, 2014, str. 203–205).

Eden glavnih ciljev SUIV je obvladovanje tveganj. Za prepoznavanje in merjenje organizacijskega tveganja in zagotavljanja neprekinjenega poslovanja se izvajajo varnostne politike ter nadzor za minimizacijo tveganj. Za celovito podporo izvajanju varnostne politike SUIV vsebuje dokumentacijo vseh varnostnih postopkov. Strukturirano upravljanje informacijske varnosti, kot rezultat uvedbe SUIV, zahteva tudi postopke za ustvarjanje, komuniciranje ter vzdrževanje in ažuriranje politik ter postopkov v organizaciji. Standardizacija procesov upravljanja informacijske varnosti zagotavlja več prednosti. Na primer zmanjšuje stroške ali omogoča večjo združljivost sistemov v celotni logistični verigi. Standard SUIV določa zahteve za sistem SUIV, ki lahko ublažijo varnostne nezgode v IKT okolju, pogodbene kazni ali izgubo ugleda, kot je razkrivanje zaupnih informacij oz. njihovo uhajanje (Helmke & Uebel, 2014, str. 205–209).

SUIV ni zgolj tehnični pristop, temveč poenoti upravljanje tveganj s pomočjo politik, postopkov, procesov, ljudi, sredstev in IT sistemov. Dobro načrtovani SUIV je učinkovit za upravljanje vseh teh elementov (Taherdoost, 2022, str. 3–5). Vsaka organizacija ima edinstveno infrastrukturo ter ljudi, zato ne najdemo dveh popolnoma enakih izvedb SUIV. To je razlog, da morajo podjetja skrbno načrtovati svoj SUIV, prepoznati prednosti, poslovne procese in potrebno raven zaščite informacij. Torej mora za učinkovito vzpostavitev SUIV sistema organizacija do potankosti poznati svoj poslovni model. Po dosedanjih priporočilih strokovnjakov informacijske varnosti je SUIV priporočljivo graditi s stališča upravljanja tveganj. Postopek nenehnega izboljševanja postane jasen s pomočjo cikla načrtuj, izvedi, preveri in ukrepaj (angl. Plan, Do, Check, Act, v nadaljevanju PDCA), ki izvira iz področja ekonomije in je poznan tudi kot Demingov krog kakovosti se uporablja za nadzor in stalno izboljševanje izdelkov ter storitev v štirih fazah PDCA (Helmke & Uebel, 2014, str. 204–205):

V prvi fazi, fazi načrtovanja (angl. Plan), se vzpostavi SUIV. Identificira se informacije, ki jih je zaradi njihove vrednosti potrebno zaščititi. Določi se obseg in razpon

odgovornosti poslovodstva v pisni obliki. Pripravi se izjavo o uporabnosti (angl. Statement of Applicability – SoA), politiko informacijske varnosti, smernice za informacijsko varnost in pravilnik o smernicah za zahteve o skladnosti. Glavna prioriteta v tej fazi je izvajanje standarda ISO 27005 – Obvladovanje tveganj informacijske varnosti.

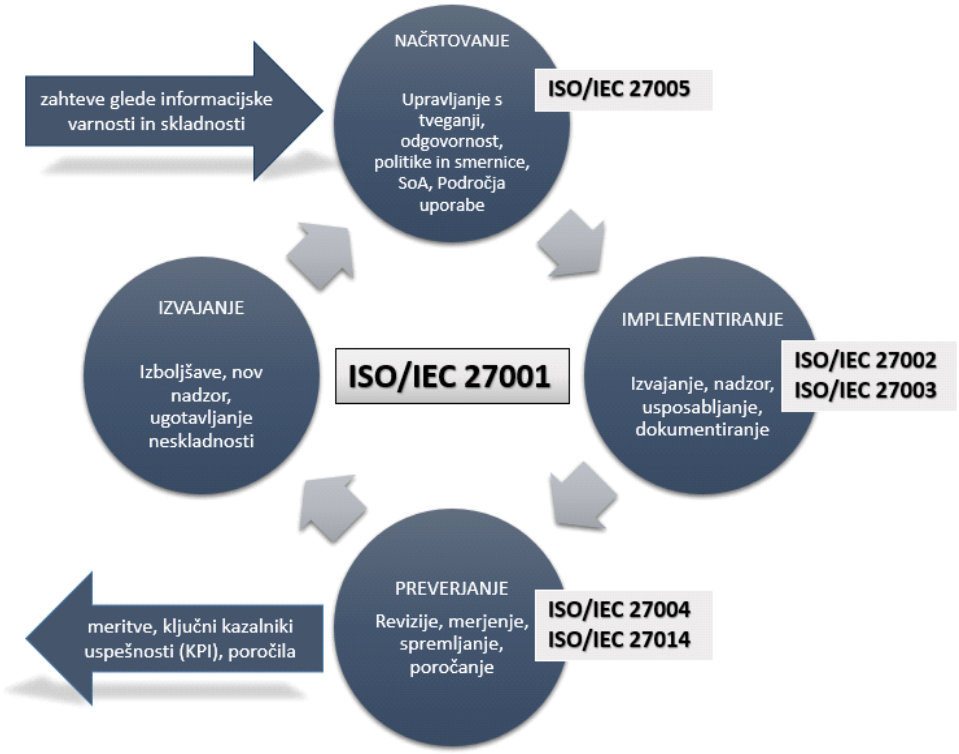
V drugi fazi se izvaja implementacija (angl. Do). SUIV s pomočjo standarda ISO 27002 – Kodeks ravnanja za nadzor informacijske varnosti in ISO 27003 – Smernice oz. varnostne tehnike SUIV, organizacija udejanja v praksi. Zaposlene se v tej fazi integrira in usposablja za njihove odgovornosti, pravice in obveznosti. Vzpostavlja se tudi dokumentacija, ki predstavlja potrditev izvajanja nadzora.

V tretji fazi preverjanja (angl. Check) se SUIV pregleduje in spremlja učinkovitost informacijske varnosti. Izvajajo se meritve, ki se jih analizira in ocenjuje. V ta namen je potrebno razviti ustrezen meritveni okvir z ustreznimi metrikami. Notranje revizije se izvajajo z namenom pridobitve informacij za izboljšanje poslovnih procesov in varnosti, oceni se varnostne incidente in trenutne razmere na področju informacijske varnosti na ravni organizacije. S pomočjo teh revizij in določanjem ravni zrelosti v ustreznem modelu se preveri, ali je standard ISO 27001 v splošnem izpolnjen oz. ali v organizaciji izpolnjujejo minimalne zahteve. V tej fazi pooblaščeni certificiran organ izvede postopke certificiranja SUIV v skladu z zahtevami ISO 27001. Vsi ustrezni rezultati se poročajo in predložijo zainteresiranim skupinam oz. deležnikom in bistvenim nosilcem odločanja znotraj organizacije. V tej fazi procesa kroga kakovosti je v pomoč standard ISO 27004 – Spremljanje, merjenje, analiziranje in vrednotenje, ter ISO 27014, ki preverja smernice in koncepte po načelih za upravljanje informacijske varnosti znotraj organizacije.

V četrti fazi, fazi izvajanja (angl. Act), se skozi vse tri predhodne faze SUIV stremi k nenehnemu izboljševanju in nenehnemu izvajanju cikla PDCA. Na podlagi revizije se izvajajo spremembe in preventiva za nadzor ter ugotavljanje celovite skladnosti.

Učinkovito izvajanje SUIV je odločitev strateškega upravljanja in je odvisno od varnostnih zahtev organizacije, zastavljenih ciljev, organizacijskih postopkov, velikosti, strukture in izvajanja dejavnosti. Certifikat ISO 27001 organizacijam predstavlja velike ekonomske prednosti, kot so prihranek stroškov zaradi obvladovanja varnostnih incidentov, boljša primerljivost storitve varovanja informacij, izpolnjevanje zakonskih zahtev in pozitiven trženjski učinek skozi pogled SUIV. Iz druge strani pa zahteva kar precejšni finančni vložek, ki pa se s časom nedvomno močno obrestuje, če organizacija upošteva, da noben nadzor ne more doseči popolne informacijske varnosti in se organizacije osredotočajo k nenehnim izboljšavam (Taherdoost, 2022, str. 3; Helmke & Uebel, 2013, str. 208). Slika 5 prikazuje Demingov krog kakovosti stalnega izboljševanja izdelkov in storitev, kot je informacijska varnost.

*Slika 5: Demingov krog kakovosti za sistem upravljanja informacijske varnosti*




*Prirejeno po Helmke & Uebel (2013, str. 205).*

Neprestano je potrebno izvajati dodatne ukrepe za spremljanje, vrednotenje ter izboljševanje učinkovitosti in uspešnosti nadzora varovanja informacij, ki so usklajene s cilji organizacije. V večini je SUIV povezan z organizacijami v gospodarskem sektorju, vendar ima pomembno vlogo vse pogosteje tudi v javnem sektorju in izobraževalnih ustanovah. Vse institucije imajo v lasti ogromno občutljivih osebnih podatkov, ki jih je potrebno ustrezno zaščititi. Velja opozoriti, da standardi zagotavljajo minimalne zahteve, ki jih je potrebno izpolniti, preden je mogoče vzpostaviti učinkovit SUIV v organizaciji. Pri stremenju k odličnosti je v veliko pomoč preizkušen in uveljavljen postopek kontinuiranega izvajanja PDCA cikel, ki ocenjuje tveganja, kot so tveganja povezana z ljudmi, postopki IT. Predstavlja tudi bistveni temelj organizacijam, da vzpostavijo konkurenčno prednost v izpopolnitvi poslovnega modela (Horikawa in drugi, 2023).

### 1.7.1 Priprava in izvajanje varnostnih politik

Varnostne politike določajo obvezne smernice za vpliv na ugodno organizacijsko vedenje pri uporabi IT ali pri delu s podatki v IS z namenom minimiziranja tveganj ter hitrih reakcij ob incidentu. Vse politike informacijske varnosti (angl. Information security policy) bi morale biti v skladu s cilji organizacije oz. poudarjati zastavljene cilje. Z varnostnimi politikami ustvarjamo varnostne protokole, dodeljujemo jasne vloge in odgovornosti ter zaposlenim nakazujemo smernice za optimalno uporabo politik med

opravljanjem vsakodnevnih nalog ter zadolžitev. Vloge, odgovornosti in smernice prav tako definirajo, s kom naj se vzpostavi stik in kako se obravnavajo varnostni incidenti v IS. Kadar so pravilniki dvoumni, zapleteni, nejasni ali težavni, na uporabnika vplivajo negativno. Zato je prvo pravilo politike narediti razumljive, ustrezne in čim bolj dostopne vsem zaposlenim (Da Veiga, 2016, str. 139–140).

Na varnostno vedenje močno vplivajo dobro zastavljene varnostne politike, kar ugotavljata Haeussinger in Kranz (2013) v raziskavi, ki kaže, da je promocija in načrtovanje politike informacijske varnosti temeljni element vsakega programa učinkovitega upravljanja informacijske varnosti, ki pozitivno vpliva na ozaveščenost zaposlenih. Choi, Levy in Hovav (2013) ugotavljajo, da ozaveščanje uporabnikov o varnostnih politikah prispeva k spretnostim zavedanja o informacijski varnosti, saj zavedanje pomembno vpliva na spretnost ustreznega ukrepanja v primeru pojava varnostnega incidenta. Varnostna politika sama po sebi še ne zagotavlja skladnosti, zato morajo organizacije oz. njihovo vodstvo spodbujati svoje zaposlene, da aktivno upoštevajo organizacijske varnostne politike.

Standard ISO 27001 opisuje najboljše prakse in priporočila za pripravo varnostne politike v SUIV ter vključuje vse vidike varovanja informacij. Obstaja 14 varnostnih področij kontrol za pripravo varnostnih politik po standardu ISO 27001 (Stickman Cyber, 2021):

- Informacijske varnostne politike (angl. Information security policies)

Cilj je zagotavljati ustrezno upravljanje in podporo varnosti informacij v skladu s poslovnimi zahtevami in ustreznimi zakoni ter predpisi na področju organizacije.

- Organiziranje informacijske varnosti (angl. Organization of information security)

Cilj je vzpostavitev okvirja za upravljanje in nadzor za učinkovito delovanje informacijske varnosti v organizaciji ter dodelitev odgovornosti za posebne naloge. Kontrole obravnavajo tudi mobilne naprave ter delo na daljavo z namenom, da vsak, ki dela od doma ali ni fizično prisoten v organizaciji, med opravljanjem dodeljenih nalog upošteva vse ustrezne prakse informacijske varnosti.

- Varnost človeških virov (angl. Human resource security)

Cilj je zagotoviti, da vsi človeški viri organizacije (zaposleni in pogodbeni partnerji) razumejo svoje odgovornosti, so ustrezno izobraženi ter seznanjeni z vlogami, katere opravljajo v organizaciji. Zajema odgovornost posameznikov pred zaposlitvijo, njihove odgovornosti med opravljanjem dela ter obravnava odgovornosti, ko oseba ne opravlja več funkcije po pogodbi – bodisi ker so zapustili organizacijo bodisi zamenjali položaj znotraj organizacije.

- Upravljanje sredstev (angl. Asset management)

Namen je dokumentirati organizacijsko premoženje z opredeljenimi ustreznimi zaščitnimi ukrepi ter odgovornostjo glede na tveganja. To zagotavlja, da so informacijska sredstva podvržena ustrezni zaščiti, npr. občutljivi podatki niso predmet nepooblaščenega razkritja, spreminjanja, brisanja, uhajanja ali uničenja.

- Nadzor dostopa (angl. Access control)

Opredeljuje omejitev dostopa do objektov in naprav za obdelavo informacij. To pomeni, da zaposleni lahko vidi samo informacije, ki so pomembne za opravljanje nalog, določenih za delovno mesto.

- Kriptografija (angl. Cryptography)

Govori o šifriranju podatkov in upravljanju občutljivih informacij, da organizacije uporabljajo pravilne in učinkovite metode kriptografskih protokolov za zaščito zaupnosti, razpoložljivosti in celovitosti informacij.

- Fizična in okoljska varnost (angl. Physical and environmental security)

Cilj je preprečiti nepooblaščeni osebi fizični dostop, katerega namen bi bil povzročanje škode ter poseganja v procese in objekte za obdelavo podatkov v organizaciji. To so lahko fizične datoteke, programska ali strojna oprema.

- Varnost poslovanja (angl. Operations security)

Obravnava pravilno in varno delovanje IKT za obdelavo in varovanje informacij. Zagotavlja, da ima organizacija potrebne zaščite za zmanjšanje tveganj pred napadi v IS (npr. požarni zid), zajema zahteve organizacije za varnostno kopiranje sistemov za preprečevanje izgub podatkov. Opredeljuje postopek, da ima organizacija dokumentirane dokaze, ko se zgodijo incidenti. Ščiti integriteto programske opreme, zajema tehnično upravljanje ranljivosti, da nepooblaščene osebe ne izkoriščajo pomanjkljivosti sistema ter da imajo sistemi ustrezne mehanizme revidiranja.

- Varnost komunikacij (angl. Communications security)

V smislu določanja načinov za zagotavljanje zaščite informacij v omrežjih. Vsebuje postopke in protokole za upravljanje varnosti omrežja z namenom, da zaupnost, celovitost in razpoložljivost informacij v teh omrežjih ostane nedotakljiva.

- Pridobivanje, razvoj in vzdrževanje sistemov (angl. System acquisition, development and maintenance)

Cilj je zagotoviti, da varnost informacij ostane osrednji del procesov organizacije v celotnem življenjskem ciklu. 13 kontrol obravnava notranje in zunanje varnostne zahteve, ki zagotavljajo storitve preko javnih omrežij.

- Odnosi z dobavitelji (angl. Supplier relationship)

Zadeva pogodbene sporazume, ki jih imajo organizacije z zunanjimi strankami. Obravnava zaščito dragocenih sredstev organizacije, ki so dostopna dobaviteljem ali ko lahko ti nanje vplivajo. Opredeljuje tudi način, kako obe oz. vse pogodbene strani ohranjajo dogovorjeno raven varnosti informacij in zagotavljanja storitev.

- Upravljanje incidentov na področju informacijske varnosti (angl. Information security incident management)

Cilj je ustvariti dosleden in učinkovit pristop k obvladovanju incidentov informacijske varnosti. Del tega procesa vključuje določitev, kateri zaposleni prevzamejo odgovornost za določena dejanja, s čimer se zagotovi dosleden in učinkovit pristop k življenjskemu ciklu upravljanja incidentov ter odzivu na njih.

- Informacijska varnost z vidika upravljanja neprekinjenega poslovanja (angl. Information security aspects of business continuity management)

Cilj je ustvariti učinkovit sistem za obvladovanje motenj poslovanja. Obravnava neprekinjeno informacijsko varnost in opisuje ukrepe, ki jih je potrebno sprejeti za zagotovitev, da se neprekinjeno poslovanje vključi v varnostne politike in SUIV.

- Skladnost (angl. Complicance)

Zagotavlja postopke za uspešno izogibanje kršenja zakonskih določil in regulativ ter pogodbenih obveznosti pri spoštovanju varnostnih zahtev informacijske varnosti, z namenom razumeti pravne in pogodbene zahteve ter obveznosti.

Standard ISO 27001 opredeljuje štirinajst opisanih domen pri izvajanju varnostnih postopkov in politik v organizaciji. Poudariti je potrebno, da organizacije niso dolžne izvajati vseh 144 kontrol znotraj 14 področij. Kontrole so le priporočila oz. seznam možnosti, ki jih je priporočljivo upoštevati glede na potrebe organizacije. Skupek teh 14 priporočil pomaga organizacijam prepoznati tveganja, s katerimi se soočajo pri pripravi ustrezne in učinkovite ter celovite varnostne politike in SUIV.

### 1.7.2 Prepoznavanje tveganja

Prepoznavanje tveganj (angl. Risk Identification) je proces ugotavljanja tveganj, ki bi programu, podjetju ali naložbi lahko preprečila doseganje ciljev, bodisi iz notranjega okolja organizacije bodisi zunanjega okolja. Za celovito prepoznavanje tveganj moramo opredeliti, kaj predstavlja vrednost, prepoznati grožnje in ranljivosti ter obstoječe protiukrepe in morebitne posledice škode. Pri tem moramo določiti premoženje, ki ga bi potencialno tveganje lahko ogrozilo. Stopnja podrobnosti identifikacije mora biti dovolj visoka, da predstavlja dovolj informacij za oceno tveganja, ki predstavlja in določa splošni obseg ocene tveganja (Shedden, Smith & Ahmad, 2010).

Za celovito prepoznavanje in analiziranje tveganj moramo prepoznati čim več nevarnosti. Upoštevati moramo, da se lahko znotraj ali zunaj organizacije pojavijo grožnje človeškega izvora, kot je npr. zlonamerna programska oprema (angl. Malware) ali višja sila, npr. naravne nesreče, ki lahko ogrozijo informacijska sredstva naključno ali namerno. Vse grožnje moramo prepoznati in jih kategorizirati splošno glede na njihovo vrsto in vir izvora, da ne bi spregledali nepričakovanih groženj in se usmerili preozko, ko jih poskušamo identificirati. Pri prepoznavi tveganja je potrebno upoštevati, da lahko nevarnost vpliva na več sredstev, zato se učinek lahko razlikuje glede na prizadeta sredstva. V oceno tveganja je pomembno vključiti tudi izkušnje iz prejšnjih incidentov, ki jih upravljamo z managementom znanja ter s predhodnimi ocenami tveganja. V pomoč so nam lahko standardizirani katalogi groženj, a moramo biti pazljivi in upoštevati, da se grožnje nenehno spreminjajo, zlasti kadar se spremenijo zunanje okoliščine organizacije. Grožnje lahko razvrstimo po vrsti, izvoru ali načinu, torej ali gre za namerno oz. naključno, naravno, človeško ali grožnjo iz zunanjega okolja organizacije. Rezultat je seznam možnih groženj, razvrščenih glede na njihovo vrsto ali glede na vir za določeno organizacijo oz. panogo delovanja (Wei, Wu & Chu, 2018, str. 49–51).

V skladu z ISO 27001 lahko ranljivosti opredelimo kot izkoriščanje grožnje v smislu povzročitve škode na sredstvih organizacije ali na organizacijo samo. Ranljivosti lahko obstajajo v celotnem organizacijskem procesu, kot npr. v poslovnih procesih, vodenju organizacije, kadrovski službi, organizacijski strukturi ali celo fizičnem okolju ter najpogosteje v konfiguracijah IS na področju strojne in programske opreme ali kot posledica zunanjega izvajanja (angl. Outsourcing) nalog, aktivnosti ali procesa. Če sam obstoj ranljivosti brez grožnje ne povzroča škode in ne predstavlja tveganja, ni potrebno razviti nobenega protiukrepa. Vendar zaznane ranljivosti ne smemo zanemariti, temveč jo moramo spremljati. Spremembe predstavljajo grožnjo, ki jo je mogoče izkoristiti, zato lahko zaradi spremembe znotraj procesa ne glede na to, da gre za inovacijo, zbudimo speče tveganje (Brenner, 2007, str. 5).

Nepravilno izveden ali nepravilno delujoč varnostni ukrep oz. nepravilna uporaba le-tega je lahko slabost. Ranljivosti je mogoče razvrstiti na strojno in programsko opremo,

omrežja, človeške vire, fizično lokacijo in organizacijsko strukturo glede na potencialne grožnje. Rezultat tega predstavlja seznam ranljivosti glede na sredstva in obstoječe nadzorne ukrepe. Prepoznati in ugotoviti moramo tudi posledice izgube zaupnosti, celovitosti in razpoložljivosti. Iz tega vidika je potrebno sredstvom določiti finančno vrednost, saj je učinek lahko kratkotrajen ali trajen. Upoštevati je treba več vidikov od izgube delovnega časa, izgube priložnosti, zdravja in varnosti, škodovanja ugledu in uničenja dobrega imena ter tudi finančne stroške, povezane s popravilom povzročene škode ter strokovno svetovanje, da dobimo strukturiran seznam scenarijev incidentov glede na škodo in posledice (Wei, Wu & Chu, 2018, str. 48; Shedden, Smith & Ahmad, 2010).

### 1.7.3 Ocena tveganja

Ocena tveganja (angl. Risk assessment) je postopek, v katerem ugotovimo nevarnosti in jih poskušamo ovrednotiti. Gre za določitev kvantitativnih in/ali kvalitativnih vrednotenj tveganja, povezanih s konkretnim stanjem in prepoznano nevarnostjo. Organizacije uporabljajo oceno tveganja za določitev obsega potencialne nevarnosti, povezanega z IS in integrirano IKT. Rezultat tovrstnega postopka pomaga prepoznati bistvene nadzorne ukrepe. Tveganje je funkcija verjetnosti, da dani viri groženj izvedejo določeno potencialno ranljivost. Zato je pomembno prepoznati možne grožnje v IS, kjer je potrebno pod stalnim nadzorom analizirati tveganja z morebitnimi ranljivostmi in kontrolami. Vpliv se nanaša na obseg škode, ki bi jo lahko povzročila grožnja zaradi ranljivosti sistema (Tianshui & Gang, 2014).

Ko so pogoji opredeljeni z osnovnimi merili, je naslednji korak izvedba ocene tveganja. Učinkovita ocena tveganja vključuje prepoznavanje tveganj, analizo tveganj z oceno tveganja ter vrednotenje tveganj. Po standardu ISO 27000 je tveganje kombinacija verjetnosti pojava nepričakovanega dogodka in njegovih posledic. Ocena tveganja številčno oz. količinsko opredeli tvegaje in omogoča, da se določenim tveganjem daje prednost glede na njihovo resnost ogrožanja. S pomočjo ocene tveganja je mogoče informacijskim sredstvom ugotoviti obstoječe ali možne grožnje ter ranljivosti, analizirati in oceniti obstoječe protiukrepe in njihov učinek na obstoječa tveganja. Ugotovimo lahko potencial posledic in končno določitev tveganja, ki predstavlja večjo nevarnost na podlagi ocenjevalnih lestvic. Za doseganje učinkovitosti in upravičenosti rezultatov se ocena tveganja običajno izvede v večkratnih ponovitvah. Prva ponovitev je ocena na najvišji ravni za ugotavljanje potencialno visokih tveganj, ki upravičujejo naslednje ponovitve. Ponovitve omogočajo podrobno analizo ugotovljenih tveganj. Ko nam ocena tveganj pokaže dovolj koristnih informacij, da predstavlja dobro osnovo za odločanje o izbiri učinkovitih ukrepov za obvladovanje tveganj, lahko izvedemo nadaljnje potrebne postopke. V kolikor ne dobimo dovolj informacij, ocenjujemo tveganja kontinuirano in iterativno, dokler ne bodo na voljo ustrezne informacije za smiselno interpretacijo in ukrepanje. Ocena tveganja mora opredeliti tveganja glede na zaupnost, celovitost in

razpoložljivosti z uporabo meril za ocenjevanje tveganj (Calder & Watkins, 2019; Tianshui & Gang, 2014).

### 1.7.4 Analiziranje tveganja

Ko izvedemo postopke ocene in prepoznavanje tveganja, proces zaključimo z obvladovanjem tveganj z oceno vpliva ter verjetnostjo za oceno tveganja kot celotno analizo tveganja (angl. Risk analysis). Prvi in bistveni korak analize tveganja je izbira primerne metode za izvedbo analize. Stopnja podrobnosti analize in izbire metode se razlikuje od kritičnosti sredstev, obsega znanih ranljivosti in/ali števila predhodnih incidentov. Analizo tveganja je mogoče izvesti s kvalitativnimi in kvantitativnimi metodami oz. kombinacijo obeh. Pogosto se na začetku uporabi kvalitativna metoda za določitev splošne ravni tveganja in prepoznavanje glavnih tveganj. Nato se za nadaljevanje preučevanja tveganj uporablja kvantitativne metode. Kvantitativne metode so pogosto dražje in veliko bolj kompleksnejše od kvalitativnih. Zasnova analize mora biti skladna z merili za oceno tveganja, opredeljenimi z določenimi oz. okvirnimi pogoji (Jaiswal, 2019, str. 857–858).

Kvalitativne metode tveganja za opis obsega potencialnih vplivov ter njihove verjetnosti pojava uporabljajo okvir kvalifikacijskih lastnosti od nizkega, srednjega do visokega tveganja. Glede na dane okoliščine lahko okvir kvalitativnih metod po potrebi prilagodimo. Prednost kvalitativne metode analiziranja je enostavna in razumljiva berljivost rezultatov, medtem ko je izbiro subjektivnega zastavljenega okvira mogoče obravnavati kot slabost. Kakovost kvantitativne analize tveganja je odvisna od natančnosti, popolnosti in veljavnosti uporabljenih modelov. Pri kvantitativnih metodah se običajno uporablja zgodovinske podatke iz preteklih nastalih incidentov. Prednost je v tem, da je mogoče cilje in pomisleke glede zaščite neposredno razbrati. Pomanjkljivost pa predstavlja pomanjkanje podatkov o novih tveganjih ali novih ranljivostih, ki bi lahko ali so že nastala (Karabacak & Sogukpinar, 2005, str. 149–152).

Z analizo tveganja je potrebno oceniti učinke ter jih finančno ovrednotiti tako, da se jih razvrsti glede na kritičnost in pomembnost. Določanje vrednosti se največkrat izvede z dvema meriloma. Najprej z določitvijo stroškov nadomestitve vrednosti ob ponovni vzpostavitvi in po drugi strani z določitvijo stroškov, ki nastanejo kot posledica učinkov na ravni operativnosti postopkov v primeru izgube ali ogrožanja vrednosti sredstev. To vključuje pravne in regulativne posledice, ki izhajajo iz razkritja, spreminjanja, prekinitve storitev ali uničenja informacij oz. drugih sredstev. Največkrat je vrednost, ki nastane kot posledica vpliva na poslovni proces, večja od preproste nadomestitve, zato je vrednotenje premoženja ključni dejavnik pri oceni učinka scenarija nezaželenega dogodka, saj največkrat prizadene več kot le eno sredstvo. Iz tega izhaja spoznanje, da imajo različne ranljivosti in grožnje različen vpliv na vrednost, kot so izguba zaupnosti, celovitosti ali razpoložljivosti. Posledice se da ponazoriti z denarnimi, tehničnimi ali človeškimi merili

vpliva. Pri prvi ponovitvi ocene učinka se navadno določi preprosta nadomestna vrednost, pri naslednji ponovitvi pa se določi takojšnja vrednost škode, ki je nastala zaradi učinkov scenarija nezaželenega dogodka. Rezultat ocenjevanja je seznam ocenjenih posledic scenarija incidenta, ki se odražajo v vrednostnih merilih vpliva (Pan & Tomlinson, 2016, str. 271–274).

Ko določimo scenarije incidentov, moramo z uporabo metod kvalitativne in kvantitativne analize določiti verjetnost pojava posameznega scenarija. To določimo na podlagi pogostosti groženj in poteka izkoriščanja določenih ranljivosti. Upoštevati je potrebno stališča empirične vrednosti in ustrezne statistike za verjetnost pojava nevarnosti, ugotoviti, kateri so namerni viri nevarnosti, motivacija storilca, predvideti sposobnost storilca kaznivega dejanja, razpoložljivost virov za kaznivo dejanje, geografsko lego, atraktivnost premoženja za oškodovanje, naključne in namerne vire za nevarnost, ekstremne vremenske pojave, človeške dejavnike ter njihove vplive in nenazadnje tudi učinkovitost obstoječih ukrepov (Pan & Tomlinson, 2016, str. 275). Upoštevati je potrebno, da se tako namerni kot nenamerni viri nevarnosti nenehno spreminjajo. Po opravljeni oceni verjetnosti moramo imeti na voljo seznam scenarijev nesreč z njihovo verjetnostjo nastanka. Vrednost verjetnosti kombiniramo z vrednostjo posledic. Poleg tega se lahko za določanje stopnje tveganja uporablja tudi druge spremenljivke, kot so stroški ali pomisleki interesnih skupin. Pri končnemu rezultatu analize se za določanje stopnje tveganja uporablja metode za oceno tveganja po standardu ISO TR 13335, ki obravnava smernice za upravljanje varnosti v IKT. V tretjem delu pa tehnike za upravljanje varnosti IKT (Szmit & Szmit, 2015, str. 17).

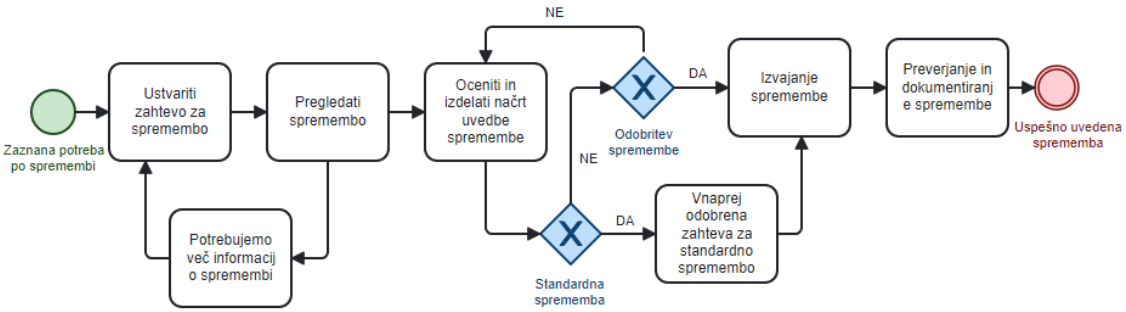
### 1.7.5 Uvajanje in obvladovanje sprememb v varnostni politiki

Podjetja in organizacije uvajajo spremembe z namenom izboljševanja politik, povečevanja produktivnosti, drugačnega pristopa do deležnikov, boljšega projektnega vodenja, izkoriščanja novih priložnosti oziroma prilagajanja vedno bolj dinamičnem poslovnemu okolju, kar pa ni enostaven in enkraten proces. Sprememba ni enkraten dogodek, ampak je postopek prehoda organizacije in njenih deležnikov iz trenutnega v bodoče izboljšano stanje z namenom zagotavljanja dolgoročnih pozitivnih učinkov na poslovanje ali zagotavljanje varnosti (Alhogail & Mirza, 2014, str. 542). Učinkovito obvladovanje sprememb je tesno povezano z reševanjem problemov, na katere naletimo pri uvajanju sprememb v delovnem okolju. Vedno se srečamo tudi s človeškim dejavnikom, največkrat v obliki upora do sprememb. V kolikor pa izvedemo pravilni pristop ter pri spremembah sodeluje tudi vodstvo (angl. Board management), s tem pokažemo, da je sprememba doletela celotno podjetje, zato lahko človeški dejavnik uporabimo v prid uvajanja spremembam (Ramluckan & van Niekerk, 2020).

Za varnostno usmerjene organizacije je pisanje politik upravljanja sprememb nujen del priprave za zaščito organizacijskih sredstev. Z izvajanjem jasnega postopka upravljanja

sprememb lahko zagotovimo, da organizacija zmanjša motnje in tveganja, koz prikazuje slika 6. Ko gre za oblikovanje politik in postopkov, ki delujejo v prid organizacij in ne kot administrativna obveza, ki jo zaposleni občutijo in sprejemajo kot oviro poslovnih procesov, lahko govorimo o učinkoviti informacijsko-varnostni politiki (Ramluckan & van Niekerk, 2020).

*Slika 6: Proces upravljanja sprememb*




*Vir: lastno delo.*

Smith (2019) navaja, da ne glede na to, ali gre za nujne spremembe, standardne spremembe ali rutinske spremembe, kot so spremembe aplikacij, programske opreme ali omrežja, je treba obravnavati pristop k vsaki vrsti sprememb. Pri pisanju politike upravljanja sprememb morajo organizacije upoštevati različne faze procesa upravljanja in vključiti politike, ki se ujemajo s temi fazami.

Po priporočilih Združenja strokovnjakov za upravljanje sprememb (angl. Association of Change Management Professionals – ACMP) mora politika upravljanja sprememb vključevati naslednjih sedem stopenj (ACMP, 2019):

- načrtovanje (angl. Planning) – faza oblikovanja in načrtovanja sprememb v sistemih IT;
- vrednotenje (angl. Evaluation) – določitev stopnje tveganja, povezana s spremembo oz. vrsto spremembe in s cilji ter s tem, katere od postopkov sprememb bomo uporabili pri izvedbi določenih sprememb;
- odobritev (angl. Approval) – pridobitev odobritve odgovornih (vrhnjega managementa), da sprožimo proces načrtovane spremembe;
- komunikacija (angl. Communication) – ustrezna komunikacija in obveščanje ljudi na vseh ravneh, s pričakovanimi spremembami, časovnim okvirjem in vsemi drugimi potrebnimi podrobnostmi o spremembah;
- izvedba (angl. Implementation) – sprememba se izvede v skladu z načrtom in v predvidenem času;
- dokumentiranje (angl. Documentation) – vse spremembe, preglede, odobritve in načrte je potrebno dokumentirani v skladu s standardi informacijske varnosti;

- spremljanje spremembe (angl. Post-Change review) – po spremljanju izvajanja spremembe se opravi pregled po spremembah, da določimo potrebne prilagoditve.

## 1.8 Ozaveščanje in izobraževanje zaposlenih

Varnost katerega koli sistema je tako močna, kot je močan najšibkejši člen verige. Ko gre za varnost informacij in IS v organizaciji, so ljudje najšibkejši člen, ki sodelujejo v sistemu. Čeprav so organizacijski varnostni sistemi vse inteligentnejši in tehnološko izpopolnjeni, jih upravljamo ljudje. Organizacije se vse bolj zatekajo k uporabi sodobnih varnostnih algoritmov v kombinaciji z AI z namenom zagotavljanja, da organizacijski podatki ostanejo zaščiteni, kljub naraščajočim trendom in sofisticiranosti informacijskih groženj ter napadov. S kombinacijo obstoječih algoritmov varnostnih sistemov s tehnologijo veriženja blokov (angl. Blockchain) lahko varnost še izboljšamo, vsaj v teoretičnem smislu. Pomembno je zavedanje, da večina kibernetskih napadov in informacijskih incidentov uspe zaradi ranljivosti, ki je posledica človeškega dejavnika oz. interakcije (Khando, Gao, Islam & Salman, 2021, str. 2–4).

Prvi korak k oblikovanju učinkovite varnostne strategije je zagotoviti, da vsi zaposleni poznajo pomen informacijske varnosti in znajo slediti standardnemu protokolu za varno uporabo IKT. Vsaka sprememba SUIV izhaja iz obvladovanja tveganj, katerih cilj je ohranjanje dobrega imena in ugleda organizacije, spoštovanja zasebnosti, predpisov, zaščita intelektualne lastnine in ohranjanje neprestanega izvajanje storitev oz. razpoložljivosti z namenom izvajanja osnovne dejavnosti (angl. Core Business) (Zhen, Dong, Xie & Chen, 2022). Za doseganje rezultatov, ki se odražajo v določenih meritvah zaposlenih ali po kazalnikih uspešnosti – KPI, mora biti načrt upravljanja sprememb izveden v skladu s smernicami po standardu ISO 27001, ki nalaga pet ključnih aktivnosti za uspešno implementacijo sprememb (Culot, Nassimbeni, Podrecca & Sartor, 2021, str. 79–82):

- ozaveščanje zaposlenih o informacijski varnosti kot del obveznosti in naloge vsakega zaposlenega;
- ozaveščanje zaposlenih o politikah in postopkih informacijske varnosti ter njihovi odgovornosti pri zasledovanju in izvajanju politik ter postopkov;
- spreminjanje navad zaposlenih v njihovem pristopu do informacijske varnosti;
- kontinuirano spodbujanje motiviranja odgovornih ljudi (vodji), da ocenjujejo in ovrednotijo tveganja na informacijsko varnost in sooblikujejo ustrezne odzive, da se tveganje minimizira na sprejemljivo raven v okviru SUIV;
- vključevanje informacijske varnosti v delovne aktivnosti kot vsakodnevne rutine v vse ravni procesov organizacije.

Za ustvarjanje okolja, v katerem ljudje spremenijo svoje vedenje, mora biti načrt upravljanja sprememb učinkovit na dveh ravneh. Dosegati mora namen, da zaposleni spremenijo svoje vedenje ter zagotoviti, da so odgovorni za informacijsko varnost dovolj aktivno vključeni v spremembo pri ozaveščanju posameznikov, da se to namero tudi uresničuje. Spreminjanje vedenja ljudi je zelo zahtevno in abstraktno delo. Organizacije, ki poskušajo spremeniti ljudi, zgolj zaradi doseganja določene ravni za zadovoljevanje standardov, običajno dosežejo nasprotni učinek, tj. upor do sprememb s strani zaposlenih. Razlog temu je, da pristop in uporabljeni postopki uvajanja sprememb ne dosežejo sprejetja na posameznikovi osebni ravni in jih zaradi odpora ne ponotranjijo (Zhen, Dong, Xie & Chen, 2022).

Organizacije spremembe največkrat vpeljujejo na način, da zaposlenim to predstavijo na programih usposabljanja za vpeljevanje sprememb, ki se izvaja kot linearen projektni načrt dogodkov. Usposabljanja so sicer dobra taktika, vendar največkrat ne dosežejo pozitivnega pristopa do posameznikovega vedenja. Vedenjsko prepričanje zaposlenih ustvarja ugoden ali neugoden odnos do vedenja, če zaposleni ne verjame, da so dobre prakse varovanja informacij dobre za celotno organizacijo ter njena sredstva. V tem primeru verjetno do takšne spremembe občuti upor. Če zaposleni verjame, da njegovi sodelavci aktivno podpirajo spremembe, zlasti tisti, ki jih sam osebno spoštuje, obstaja velika verjetnost, da bo do sprememb občutil manj upora ter jih sčasoma sprejel in ponotranjil. Za vzpostavitev takšne kulture je v največji meri odgovorno vodstvo podjetja, saj če nadrejeni zaposlenih ali oseba, ki je odgovorna za dobre prakse, te naloge ne obravnava prednostno, verjetno ne bo oblikovan namen sprejetja uvajanja sprememb (Khando, Gao, Islam & Salman, 2021, str. 16).

Organizacije, ki imajo razvito dobro varnostno organizacijo kulturo, imajo največkrat tudi dobre kazalnike organizacijske klime, saj novosti in spremembe vpeljujejo po načelih učeče se organizacije (angl. Learning organization), kjer se z novostmi in spremembami spopadajo na vseh hierarhičnih ravneh. Dobre prakse uspešnega uvajanja sprememb kažejo, da zaposleni veliko hitreje in pozitivneje sprejmejo spremembe, če se jim te predstavi skozi igrifikacijo (angl. Gamification), pri kateri sodeluje celotna organizacija skupaj z vodstvom in zaposlenimi, saj tako lažje sprejmejo dejstvo, da se spremembe tičejo vseh in ne zgolj zaposlenih na ravni nižjega in srednjega managementa. S tem načinom sam prikaz spremembe ne ustvarja upora, temveč poskuša namen spremembe prikazati skozi igro (Smith, 2019, str. 21).

Ajzen (1991) ugotavlja, da je pri vpeljevanju sprememb potrebno spremljati in opazovati zaposlene, da se na prvi stopnji ugotovi, ali je njihov zaznani odziv na spremembe resničen, in če ni, je potrebno prilagoditi in iskati izvor tega problema. Če želimo spremeniti prepričanje ljudi o učinkovitosti dobrih praks varovanja informacij, moramo najprej preveriti prepričanje v njihovi zavesti, kar pa je zelo težko ali celo nemogoče. Zato se vse začne pri vzpostavljanju dobre varnostne kulture in dobre organizacijske klime.

Informacijska varnost je največkrat nepriljubljena tema izobraževanj in prevečkrat prepuščena upravljalcem omrežij in strojne opreme. Bistvo celovitega varovanja informacij se začne pri vsakem zaposlenemu. Visoka raven zavedanja varovanja informacij zahteva spremembe v odnosu in vedenju vseh zaposlenih na vseh ravneh organizacije. To najlažje dosežemo po smernicah dobrih praks organizacij z visoko vzpostavljeno varnostno kulturo in nenehnim učenjem ter vlaganjem sredstev v znanje. Dobra praksa, ki je naletela na najmanj odpora s strani zaposlenih, je učenje skozi igro, ki jo je potrebno organizirati in implementirati v fazo izobraževanja, da jasno pokaže, ali zaposleni razumejo spremembe ali verjamejo, da je sprememba potrebna in koristna ter ali so pripravljeni spremeniti svoje vedenje in navade oz. reprogramirati svojo zavest (Zhen, Dong, Xie & Chen, 2022; Pattinson in drugi, 2020, str. 3–5).

## 1.9 Prihodnost varovanja informacij in obvladovanja človeških vplivov v informacijski varnosti

Sodobne tehnologije (kot npr. veriženje blokov) nedvomno zelo vplivajo na pomen varnosti v informacijski tehnologiji, saj je tudi v decentralizirani naravi poskusov napada jasno, da jim je mogoče zaupati. Nekatere vlade in podjetja že s pridom izkoriščajo tovrstno tehnologijo, saj je še posebej učinkovita za zaščito občutljivih zapisov. Ko je enkrat določena informacija zapisana v bloku, je ni več mogoče spremeniti, ker tehnologija uporablja kriptografijo. V prihodnosti bo tovrstna tehnologija vse bolj uporabljena v informacijski varnosti, saj odpravlja potrebo po uporabi gesel, posledično bo manj napadov socialnega inženiringa, saj je njihov cilj pridobitev gesla s strani žrtve napada. Prednost predstavlja tudi pri doseganju konsenza med strankami procesa glede identifikacije (Al-Amri, Alsuwat & Alsuwat, 2021, str. 246).

Vse bolj se krepi tudi pomen človekovega prizadevanja v boju proti kibernetskem kriminalu in ranljivostim v IS. Prakso predstavlja vključevanje skupine oziroma množice ljudi za skupni cilj (angl. Crowdsourcing). To je način za hitrejše reševanje problemov in predstavlja moč povezljivosti s pomočjo razširjene uporabnosti socialnih medijev in dostopnosti v povezljivosti, bodisi z idejami, časom, strokovnim znanjem bodisi sredstvi, ki prispevajo k projektu ali skupnemu namenu. Skupina ljudi za skupni cilj se osredotoča ne le na poročanje o incidentih na področju informacijske varnosti, temveč tudi na testiranje tehnologij informacijske varnosti. Številne spletne platforme svojim uporabnikom omogočajo preizkušanje programske opreme z možnostjo množičnega testiranja (Ye & Jensen, 2022, str. 1204).

Kombinacija množičnega izvajanja in strojnega skeniranja izkorišča prednosti človeške in računalniške inteligence, hkrati pa blaži slabost vsakega od njih, zato v bodoče mogoče takšna kombinacija tehnologij predstavlja trend na področju informacijske varnosti. V bodoče bo vse več organizacij uporabljalo AI za odkrivanje varnostnih ranljivosti in množično testiranje za potrditev odkritih ranljivosti. Z uporabo tehnologije veriženja

blokov bodo organizacije lahko te informacije o ranljivostih shranile z uporabo zapisov, ki jih ne bo mogoče spreminjat ter jih bo mogoče deliti med seboj na podlagi globalnih sporazumov o sodelovanju na področju kibernetske in informacijske varnosti. Veliko oviro pri medsebojnem deljenju in razkritju informacij o varnosti predstavljajo Zakoni o varstvu osebnih podatkov. To oviro je mogoče odpraviti le na zakonodajni ravni, zato bo v naslednjih letih vsem državam, ki dajejo pomen informacijski in kibernetski varnosti, predstavljal velik izziv, kako pripraviti ustrezno zakonodajo za zaščito podatkov in zakonodajo o mednarodni izmenjavi informacij. Dostopanje do ažurnih podatkov predstavlja ključni dejavnik za učinkovito obrambo pred kibernetskimi in informacijskimi grožnjami. Tehnologija, ki bo močno spreminjala način varovanja informacij, je AI. Ponudnikom rešitev varnosti omogoča povečanje odpornosti računalniške infrastrukture. Nekatera svetovna podjetja v energetskem sektorju uporabljajo ML za preučevanje normalnosti delovanja omrežja in v realnem času pridobivajo poročila o morebitnih nepravilnostih oziroma odstopanjih v delovanju omrežja sistema (Al-Amri, Alsuwat & Alsuwat, 2021, str. 247).

### 1.9.1 Umetna inteligenca in njene koristi ter nevarnosti za informacijsko varnost

V začetkih tehnologije AI je ta bila predstavljena kot koncept posnemanja človeških možganov za raziskovanje kompleksnih realnih problemov v praksi s holističnim človeškim pristopom. Njen namen je, da omogoča računalnikom oponašanje človeškega razmišljanja ter s tem veliko hitreje rešuje problem in se v realnem času nanj odzove. AI je opredeljena kot simulacija človeške inteligence v strojih in računalniških omrežjih, ki so v glavnem programirani na način človekovega razmišljanja v ponavljajočih vzorcih. AI lahko med svojimi številnimi koristmi informacijske in kibernetske varnosti prepozna vzorce iz velikih količin podatkov (angl. Big data), kar omogoča odkrivanje trendov v funkcijah zlonamerne programske opreme, saj je glavni namen velikih količin podatkov, upravljanje in podatkovna analitika ter podpora odločanju na podlagi dejstev oz. podatkov. Te tehnologije lahko grožnje klasificirajo veliko hitreje, kot do tega zaznavanja pridejo ljudje (Al-Amri, Alsuwat & Alsuwat, 2021, str. 247–248).

AI že ima in bo v prihodnosti imela pomemben vpliv na informacijsko varnost, s priložnostmi in nevarnostmi, ki jih tehnologija ponuja. Zaskrbljujoče je poročanje o povečanju sposobnosti kibernetskih napadov, saj tehnologija AI napadalcem omogoča, da izboljšajo učinkovitost in zmogljivost svojih napadov. Napadalci lahko uporabijo AI za razvoj naprednih tehnik napada, kot so izkoriščanje ranljivosti, socialni inženiring in zlonamerna programska oprema. AI omogoča tudi avtomatizacijo procesov, kar še povečuje hitrost in obseg napadov. Za preprečevanje negativnih vplivov, ki jih prinaša AI, se lahko z njo tudi ubranimo, saj je lahko zelo koristna pri preprečevanju kibernetskih napadov ter pri hitrem prepoznavanju anomalij pri nedovoljenem uhajanju podatkov iz IS. Z vidika vloge človeka lahko AI avtomatizira varnostne postopke. Izvaja lahko nadzor dostopa do sistemov, zaznava in odpravlja ranljivosti ter izvede Ad Hoc analizo

varnostnih postopkov. Izzivi in tveganja, ki jih AI prinaša, so tudi napake v programu ali pa jo napadalci zlorabijo za svoje koristi. Pojavijo se lahko lažno pozitivni ali lažno negativni rezultatu pri sistemih za odkrivanje napadov na podlagi AI. Ena od najnevarnejših zlorab AI je izdelava ponaredkov oz. tehnik prevar, kot je primer zloraba identitete osebe z digitalno obdelavo (angl. Deepfake). Ob vseh izzivih in priložnostih, ki jih AI ponuja, se pojavljajo etična vprašanja v zvezi z informacijsko varnostjo, ob analizi osebnih podatkov pa lahko nastanejo vprašanja o zlorabi zasebnosti (Meissner & Keding, 2021; Gnanabharathy, 2018).

### 1.9.2 Vpliv umetne inteligence na človeški dejavnik

AI in ML delujeta tako, da ustrezno reagirata s pomočjo obdelave velikih količino podatkov. Na ta način lahko tovrstna tehnologija uspešno nadzoruje informacijsko tveganje posameznika, saj skozi algoritem nenehno spremlja ozaveščenost uporabnika o informacijski varnosti, posameznikovih navadah ter vzorcih človeškega razmišljanja z namenom iskanja ranljivosti znotraj vzorcev. S prepoznavanjem vedenjskih vzorcev lahko optimiziramo trende, ki so pomembni za delovni proces. Ta lastnost AI kaže, da je primerna za izvajanje rutinskih nalog na nižjih ravneh, ki se ponavljajo in potekajo znotraj zaprtega sistema upravljanja. Nenazadnje pa je ne glede na področje poslovanja ali področje uporabe AI vedno dobra toliko, kot so kakovostni podatki na katerih temelji. Pri upravljanju vsake tehnologije so ključni ljudje in procesi, tehnologijo pa moramo dojemati zgolj kot sredstvo (Chignell, Chung, Yang, Cento & Raman, 2021, str. 1495–1497; Marble in drugi, 2015).

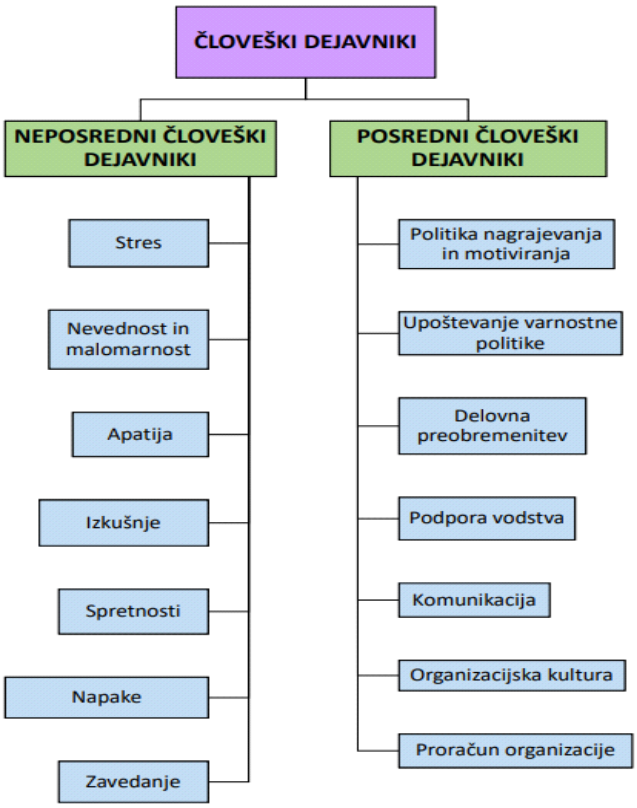
Vsak informacijski incident ali kibernetski napad ima v izvoru človeški um, in tudi najsodobnejši algoritmi AI in ML ne morejo do potankosti zares razumeti ali upati posnemati kaotične in raznolike narave človeškega uma, zato bo pri AI človeška inteligenca še vedno bistvenega pomena pri procesu odločanja. Pomemben vidik, ki ga človeški dejavnik vključuje, je zavedanje varnostnih tveganj, usposabljanja in izobraževanja uporabnikov ter odgovornosti pri upravljanju in vzdrževanju AI. AI je odlična pri avtomatizaciji rutinskih nalog in pridobivanju novih spoznanj iz obstoječih podatkov. AI ne more ustvarjati radikalnih novih izdelkov in poslovnih modelov. Sama po sebi predstavlja številne izzive za informacijsko varnost. AI sistemi so običajno kompleksni in vključujejo veliko količino podatkov, kar lahko predstavlja tveganje za zlorabo ali nepooblaščen dostop do podatkov. AI sistemi niso odporni na napake ali manipulacije, kar lahko vodi do resnih varnostnih incidentov. Zato je pomembno, da se pri razvoju in uporabi AI upoštevajo ustrezni varnostni standardi in protokoli, da se zagotovi zasebnost, integriteta in zaupnost podatkov ter prepreči morebitne zlorabe. Hiter razvoj tehnologije na podlagi AI terja, da se vzpostavijo etične smernice in regulative, ki bodo urejale, kako se sistemi, ki temeljijo na AI, razvijajo, uporabljajo in kako se z njimi ravna, da so informacijsko varni. Kot vidimo morata AI in človeški dejavnik sodelovati v sinergiji, da se zagotovi čim ustreznejša varnost inteligentnih sistemov. AI je torej

tehnologija, ki bo ljudem pomagala pri avtomatiziranem izvajanju rutinskih kontinuiranih nalog, še dolgo ali verjetno nikoli pa ne bo nadomestila t.i. intelektualnega človeškega kapitala, ki vključuje ustvarjalnost, domišljijo, vodenje, analiziranje, humor, izvirne misli in druge abstraktne vzorce človeškega vedenja (Chignell, Chung, Yang, Cento & Raman, 2021, str. 1496; Gnanabharathy, 2018).

# 2 VPLIV ČLOVEŠKIH DEJAVNIKOV NA UPRAVLJANJE INFORMACIJSKE VARNOSTI

Vse pogostejši so incidenti v zvezi z informacijsko varnostjo, ki je posledica interakcije ljudi, ki se posredno ukvarjajo s SUIV. Tveganja v IS imajo negativne posledice na organizacijsko delovanje in sredstva. Varnostni sistemi niso odvisni samo od preprečevanja tehničnih težav, ampak so odvisni tudi od ljudi, ki uporabljajo te sisteme. Izzivi digitalne dobe v informacijski varnosti izvirajo iz netehničnih sil in so posledica človeških in organizacijskih vprašanj, zato je pomembno razumeti in obravnavati vse povezane dejavnike, ki vplivajo na varovanje informacij (Parsons, McCormac, Butavicius & Ferguson, 2010, str. 1–3). Dve glavni kategoriji vpliva človeških dejavnikov na SUIV lahko delimo na neposredne in posredne dejavnike, kot prikazuje slika 7.

*Slika 7: Človeški dejavniki, ki vplivajo na sistem upravljanja informacijske varnosti*




*Prirejeno po Alavi, Islam, Jahankhani & Al-Nemrat (2013).*

Človeški dejavniki so veda psihološke znanosti o ljudeh pri opravljanju vsakodnevnih nalog. Proučevanje človeških dejavnikov se ukvarja predvsem z razumevanjem človeških zmožnosti. Človeški dejavniki veljajo za kombinacijo ergonomije in psihologije. Področje človeških dejavnikov ima štiri glavne cilje: povečanje varnosti, zmanjševanje napak, poenostavljanje delovnih nalog in povečevanje produktivnosti na vseh ravneh poslovnih funkcij za doseganje organizacijskih ciljev. Dejavniki iz slike 7 so bili največkrat izpostavljeni in ugotovljeni s strani raziskovalcev s sistematičnim pregledom literature. Neposredni dejavniki so večinoma odvisni od določenih posameznih značilnosti in imajo pomemben vpliv na varnost IS. Posredni dejavniki pa so močno odvisni od zunanjih dejavnikov, ki so odvisni od organizacijskih vprašanj (Alavi, Islam, Jahankhani & Al-Nemrat, 2013, str. 2).

## 2.1 Neposredni človeški dejavniki

Neposredni dejavniki temeljijo na posameznikih, ki neposredno vplivajo na splošno varnost v SUIV organizacije. Ti posamezniki so vključeni v prizadevanja organizacije za dosego svojih ciljev. Na primer napaka, apatija, stres, zavedanje in izkušnje imajo neposreden odnos oz. značaj in nenazadnje svojo osebnost – ljudi. Ti dejavniki vplivajo na varnost IS tako, da neposredno vplivajo na posameznike. Večinoma so neposredni dejavniki odvisni od lastnosti posameznika (Alassaf & Alkhalifah, 2021; Alavi, Islam, Jahankhani & Al-Nemrat, 2013, str. 2).

### 2.1.1 Stres

Stres (angl. Stress) na posameznika v delovnem okolju lahko povzroči velike delovne obremenitve v kombinaciji s kratkimi roki končanja aktivnosti in projektov, lahko izvaja pritisk na zaposlene, ki uničuje dobro organizacijsko klimo. Ljudje se na stres odzovejo negativno, vendar je stres v dinamičnem času s hitrim potekom dogodkov, brez ločevanja zasebnega in poslovnega življenja, lahko zelo tvegan za varnost IS. Stres vodi v človeške napake in izgorelost. Ljudje pod vplivom stresa so lahko nagnjeni k tveganemu vedenju in nenamernemu izogibanju varnostnim politikam. Stres in izčrpanost imata neposreden odnos do ranljivosti IS. Neuravnotežena in prekomerna obremenitev ustvarja stres in dodaten pritisk na zaposlene. Vsakodnevne obremenitve močno spodkopavajo moralo in ogrožajo zasledovanje organizacijske etike, kar privede do negativnih delovnih rezultatov. Ta upad morale in etike resno ogroža varnost IS, ker se ljudje ne počutijo cenjene, ampak občutijo, da se od njih zahteva zgolj izpolnitev dodeljenih nalog. Organizacije morajo poskrbeti, da so zaposleni zaščiteni tako od zunanjih kot notranjih pritiskov z izvajanjem tehnik in delavnic za obvladovanje stresa in uspešno doseganje zastavljenih ciljev (angl. Time management). Učenje zaposlenih za ločevanje zasebnega in poslovnega življenja in organizacijsko spodbujanje k izobraževanju ter vlaganje v razvoj kadrov lahko na posameznika deluje razbremenilno (Gratian, Bandi, Cukier, Dykstra & Ginther, 2018, str. 346; Alavi, Islam, Jahankhani & Al-Nemrat, 2013, str. 6).

### 2.1.2 Nevednost in malomarnost

Zaposleni v organizacijah včasih namerno ali nenamerno ne posvečajo dovolj pozornosti varnostni politiki. Primer malomarnosti in nevednosti (angl. Negligence) uporabnika je, kadar namesti piratsko programsko opremo oz. programsko opremo brez uradne licence. Piratstvo se dogaja, ko zaposleni ne ponotranjijo varnostne politike in s tem kršijo pravila o nameščanja programske opreme iz različnih razlogov, kot je posledica pomanjkanja usposabljanja o varnosti informacij. Število nesreč v IS, ki jih pripisujemo človeški interakciji, je veliko. Naključne kršitve tvorijo večino varnostnih incidentov, povezanih z zlorabo zaradi nevednosti in malomarnosti. To vpliva na varnost IS in odstopanja od skladnosti pri revizijah IS. Organizacije posvečajo vse več pozornosti krepitvi tehničnih zmogljivosti za premagovanje tega vprašanja, vendar sta neznanje in malomarnost zaposlenih zaradi nevednosti vprašanji, ki zaslužita neprestano spremljanje. Prav tako je zelo težko revidirati vedenje ljudi. Nekateri avtorji so obravnavali to težavo s predlaganjem uporabe teorije motiviranja in nagrajevanja. Seveda s predpostavko o uspešnem in zadostnem ozaveščanju zaposlenih o varnostni politiki ter postopkih (Alavi, Islam, Jahankhani & Al-Nemrat, 2013, str. 6).

### 2.1.3 Apatija

Apatijo (angl. Apathy) v organizacijskem kontekstu razumemo kot nezainteresiranost zaposlenih v smislu pomanjkanja občutkov in čustev pri opravljanju delovnih zadolžitev, s katerimi prispevajo k doseganju ciljev organizacije in ciljev v situacijah, ko bi morali pokazati pro-socialno vedenja oz. vedenje, ki je pozitivno vrednoteno z jasnim izkazovanjem empatije. Apatija v organizacijah sproža pomembne polemike in vprašanja zaradi pomanjkanja zainteresiranosti oz. pripravljenosti za učinkovito izvajanje organizacijskih postopkov in politik. Apatija pri varnosti IS povzroča in vnaša negotovost v smislu dojemanja in upoštevanja varnostnih politik, ker jim ljudje niso pripravljeni slediti. Ustvari se okolje, v katerem zaposleni verjamejo, da nimajo svoje odgovornosti. Pozitiven odnos, motivacija in optimalni delovni pogoji pripomorejo k boljši uspešnosti in posledično h boljši varnostni kulturi, medtem ko apatija in neodzivnost proizvajajo nezaželene zaznave v smislu nepozornosti in nezainteresiranosti sledenju ciljev organizacije (Alavi, Islam, Jahankhani & Al-Nemrat, 2013, str. 5). Hinson (2003) navaja, da pozitiven odnos učinkuje tudi na učinkovitejše izvajanja varnostnih politik, vendar je izredno težko vzpostaviti model in izmeriti odnos in motivacijo zaposlenega do samega dela. Thomson in van Kiekerk (2012) trdita, da slaba komunikacija med zaposleni in višjim vodstvom prispeva k nerazumevanju izvajanja politik, kar privede do apatije zaposlenih. Ne gre zanemariti, da so v organizacijah, kjer obstaja prisilno okolje (angl. Pressing), zaposleni frustrirani in nezadovoljni. Prisilno okolje je bilo opredeljeno kot okolje, kjer v organizaciji vse narekuje višji management, podrejeni pa nimajo pravice vzpostaviti in uveljaviti svojih mnenj ne glede na to, ali ima management pravilne ali napačne usmeritve. Prisilno okolje vzpostavlja monarhijo, kjer posvetovanja z

zaposlenimi ni in ti največkrat niti ne poznajo zastavljenih ciljev podjetja ali pa ti niso realno definirani po metodi specifično, merljivo, dosegljivo, realistično in časovno omejeno (angl. Specific, Measurable, Attainable, Relevant, Time-bound – SMART).

Na srečo sta digitalizacija in globalizacija tovrstne modele vodenja skoraj izbrisala, saj ne prinašajo strateške konkurenčne prednosti organizacijam. V takšnem okolju ljudje niso motivirani za svoje delo in zasledovanje organizacijskih ciljev, kot so cilji varnosti IS. Na primer, če član poslovodstva spremeni postopke brez upoštevanja človeških in organizacijskih omejitev, se bo oblikovalo prisilno okolje in zaposlenim bo primanjkovalo zanimanja za sledenje varnostnih politik. Cilj takšnega vodenja in zasledovanja politike vodi v neuspešnost organizacije in poveča možnost za ustvarjanje ranljive organizacije z vidika učinkovitosti zasledovanja varnosti IS (Alavi, Islam, Jahankhani & Al-Nemrat, 2013, str. 5).

### 2.1.4 Izkušnje

Izkušnje (angl. Experience) prispevajo k človeškemu znanju (Thomson & van Niekerk, 2012, str. 41). Zaposleni imajo različne poglede na dejavnike izkušenj v povezavi s konceptom varnosti IS. Nekateri trdijo, da ljudje razumejo koncepte in postopke varnosti IS in se opirajo na človeške dejavnike pri njihovemu interpretiranju, vključno z izkušnjami. Medtem ko nekateri zasledujejo teorijo in trdijo, da je uspešna izvedba informacijske varnosti v veliki meri odvisna od znanja in izkušenj ljudi, ki ustvarjajo pozitiven odnos do varnosti in posledično pozitivnejšega varnostnega vedenja (Herzog, 2010). Izkušnje so nujno potrebne za harmonizirano izvajanje politik informacijske varnosti. Zaposleni brez ali s pomanjkanjem izkušenj usposabljanja o varovanju informacij in podatkov predstavljajo resno grožnjo vsem informacijskim sredstvom, s katerimi se rokuje pri delu. Učinkovito varnostno vedenje je bolj povezano s psihologijo vedenja ljudi, ki poznajo etične in moralne standarde ter se zavedajo nevarnosti in škode, ki jo lahko z neustreznim vedenjem povzročijo. Največjo vlogo pri tem igra organizacijsko okolje in management. Če potegnemo črto in zanemarimo izkušnje pri delu z informacijsko varnostjo, je za nenadzorovani prosti pretok informacij oz. njihovo uhajanje največkrat kriva nejasna varnostna politika in njeno izvajanje na ravni organizacije z vidika šibkosti zaznavanja človeškega vedenja do informacijske varnosti (Alavi, Islam, Jahankhani & Al-Nemrat, 2013, str. 3–4).

### 2.1.5 Spretnosti

Spretnosti (angl. Skills) olajšajo opravljanje delovnih nalog in vlog posameznika. Spretnosti igrajo pomembno vlogo pri uspešnem delovanju zaposlenega pri zasledovanju ciljev organizacije in uspešnemu opravljanju delovnih zadolžitev. Izobraževanje in usposabljanje sta ključnega pomena pri razvijanju veščin in dvigovanju zavesti za ohranjanje strokovnosti in ustrezne usposobljenosti. Spretnosti so ena glavnih sil pri

obravnavanju vprašanj IS kot odziv na incidente. Odsotnost ustreznih in ustrezno usposobljenih strokovnjakov prispeva k neuspešnemu zasledovanju varnostne politike in varnosti IS. Zaposleni morajo imeti zadostno znanje in spretnosti za obravnavo nalog in zahtev sledenju politike informacijske varnosti ter njenih postopkov. Na primer če ljudje ne vedo, kako to storiti in se ukvarjajo s sumljivimi e-poštnimi sporočili, obstaja korelacija, da jih bodo odprli in s tem povzročili škodo organizaciji. Pomembno je tudi, da sposobnosti ljudi niso precenjene ali podcenjene, saj se napake lahko zgodijo še tako izurjenim in spretnim strokovnjakom. Organizacije se ne smejo osredotočati samo na ljudi s popolno tehnološko usposobljenostjo, bistvo za ohranjanje celovite varnosti je namreč usmerjanje pozornosti na najšibkejše člene varnostne verige. Programe usposabljanj, ki zaposlenim omogočajo ustrezno znanje o varnostnih politikah in tehnikah varnosti IS ter izpolnjevanje organizacijskih ciljev, je potrebno jasno definirati in zastaviti v strateških načrtih (Pattinson in drugi, 2020, str. 3). To postane še toliko pomembnejše, ko se poslovno vedenje zaposlenih zaradi novih tehnoloških sprememb hitro spreminja tudi zaradi dinamičnega poslovnega okolja. Organizacije morajo biti dovolj agilne, da lahko te novosti in spremembe integrirajo hitro in predvsem učinkovito v svoje interno okolje poslovanja ter znajo te izkušnje tudi dokumentirati (Evans, He, Maglaras, Yevseyeva & Janicke, 2019, str. 111; Alavi, Islam, Jahankhani & Al-Nemrat, 2013, str. 3).

### 2.1.6 Napake

Napaka (angl. Error) je neuspeh načrtovanih dejanj za dosego cilja. Načrt delovanja je lahko primeren, a stvari vseeno ne potekajo po načrtu ali pa zasledujejo začrtano pot, vendar je načrt neprimeren za dosego zastavljenega cilja. Napako je mogoče opredeliti tudi kot razhajanje v sistemu, ki deluje po jasno in natančno zadanih postopkih. Incidenti IS se pogosto zgodijo, ko je bil uporabljen ustrezen varnostni ukrep, a je ta neobčutljiv na neustrezno človeško vedenje (Gratian, Bandi, Cukier, Dykstra & Gainther, 2018). Na primer verifikacije politik za gesla ljudem naročajo, da izberejo primerno varnostno geslo. Taka gesla najverjetneje predstavljajo kombinacijo črk z vsaj eno veliko črko in/ali številko, ki si jih bodo nekateri uporabniki težko zapomnili. V izogib temu si ljudje zapišejo gesla na nezanesljivih mestih, kot so vidna polja na njihovih delovnih mestih ali celo na samolepilni e-listek na zaslonu, da so vidna vsem pri izvajanju delovnih aktivnosti. Ob tem je velika verjetnost za nevarnost zlorabe razkritega podatka. Človeške napake so lahko namerne ali nenamerne. Kraemer in Carayon (2006) menita, da je človeška napaka v informacijski varnosti neprevidni naključni incident, ki jo še poslabšajo slabo zastavljeni ukrepi varnostnih politik IS na organizacijski ravni. Njuna ugotovitev raziskave zaključuje, da so posredne sile, kot sta komunikacija in varnostna kultura posameznika, glavni vir človeških napak. Posledično se lahko varnostni sistem v IS z izredno tehnološko napredno hrbtenico "*spotakne*" ob človeški napaki. Z drugimi besedami, številne tehnične ukrepe je mogoče premagati z napakami ljudi, bodisi namernimi bodisi nenamernimi. Varnostne politike so zasnovane tako, da omejujejo

vedenje z namenom odpravljanja napak, vendar je vedenje težko določiti, meriti in nadzorovati v kateri koli organizaciji (Alavi, Islam, Jahankhani & Al-Nemrat, 2013, str. 3).

### 2.1.7 Zavedanje o varnosti informacij

Programi ozaveščenosti o informacijski varnosti zagotavljajo, da zaposleni v organizaciji razumejo svoje odgovornosti pri soupravljanju varnosti v IS. Uporabniki bi torej morali prijaviti vsako sumljivo e-poštno sporočilo, ki ga prejmejo. Zavedanje o informacijski varnosti (angl. Information Security Awareness, v nadaljevanju ISA) se dotika razumevanja in zavesti ljudi o varnosti IS preko upoštevanja začrtanih varnostnih politik. Varnostne politike si je mogoče napačno razlagati in narobe razumeti, zato je program ozaveščanja in učenja o varnosti informacij prav tako pomemben kot kateri koli drug postopek upravljanja IS (Rahman Ahlan, Lubis & Lubis Ridho, 2015). Organizacije so zelo zaskrbljene glede sposobnosti svojega kadra pri sledenju in izvajanju pravil ter predpisov o varnosti informacij in varnostnih politik nasploh. Številni avtorji omenjajo tudi razkorake v raziskavah varnostnega zavedanja v organizacijah, zato je zelo težko opredeliti primere dobre prakse o ustreznem ozaveščanju o varnosti informacij s področja vpliva človeških dejavnikov. Zavedanje je najmočnejši neposredni človeški dejavnik, ki vpliva na informacijsko varnost, in je sestavljeno iz znanja, odnosa in vedenja (Parsons in drugi, 2014; Alavi, Islam, Jahankhani & Al-Nemrat, 2013, str. 4).

## 2.2 Posredni človeški dejavniki

Posredni dejavniki imajo določen vpliv na neposredne dejavnike ter na SUIV. Ti dejavniki vplivajo na ljudi skozi elemente, ki jih v veliki meri nadzorujejo in upravljajo organizacije, nad njimi pa posamezniki, predvsem nižji in srednji management, nimajo vpliva oz. so brez pristojnosti nad odločanjem izvrševanja aktivnosti v procesu upravljanja organizacije (Jahankhani, Fernando, Nkhoma & Mouratidis, 2007).

### 2.2.1 Politika nagrajevanja in motiviranja

Politika nagrajevanja in motiviranja (angl. Reward and recognition policy) v organizacijah nagrajuje dobro vedenje in delovanje zaposlenih ali pa kaznuje za neprimerno izvedene aktivnosti oz. naloge. Obstajajo določene povezave med ljudmi in odnosom do politike nagrajevanja in motiviranja. Spodbude in motivacija ter nagrajevanje (finančno ali nefinančno) so pomembni dejavniki v organizacijah za spodbujanje pozitivne zavesti pri opravljanju vsakodnevnih delovnih aktivnosti. Nagrajevanje in motiviranje vpliva na motivacijo ljudi z namenom, da bi učinkoviteje sprejemali zastavljene ukrepe za varovanje IS po celotni hierarhiji organizacije. Organizacije bi na osnovi te politike morale nagrajevati zaposlene, ki poročajo o nesrečah

in incidentih na IS s prijavo vsakega sumljivega vedenja, namesto da bi kaznovale ljudi, ki zaradi nevednosti odpirajo sumljiva e-poštna sporočila. Nagrajevanje mora biti takšno, da pozitivno vpliva na pripadnost in povečuje organizacijsko varnostno klimo ter zaposlene odvrača od namernega povzročanja incidentov. Zaposleni na način motivacije in nagrad lažje sledijo varnostnim politikam, saj so nagrajeni za svoje dobro vedenje, organizacijam pa ustvarjajo prihranke sredstev, ki bi sicer bili porabljeni za reševanje incidentov (Reason & Hobbs, 2017; Alavi, Islam, Jahankhani & Al-Nemrat, 2013, str. 7).

### 2.2.2 Upoštevanje varnostne politike

Varnostna politika (angl. Information Security Policy) je organizacijski dokument, v katerem so opisani varnostni postopki in pravila. Zaposleni na vseh ravneh organizacije morajo razumeti varnostno politiko in sodelovati pri izvajanju v skladu s svojim položajem. Uveljavljanje varnostne politike je pomembno vprašanje za varnost IS in njeno uspešno delovanje bi moralo biti neposredno podprto s strani vodstva (Ruighaver, Maynard & Chang, 2007). Varnost omrežja, nadzor dostopa, opisi delovnih mest in politika gesel so primeri dejavnikov, ki so opredeljeni v varnostni politiki. Kršitve pravil IS so premalo raziskane in na tem področju obstaja še mnogo vrzeli. Nivo organizacije obsega definirane varnostne politike in postopke, ki uporabnikom povedo, kako morajo ravnati z informacijskimi sredstvi, da ostanejo varna in temeljijo na predhodno opravljenih analizah tveganja. Pomembno je načrtovati tudi dovolj visok proračun, namenjen informacijski varnosti. Priporočljiva je tudi primerjava politik s konkurenco in iskanje varnostnih razhajanj ter njihovo izpopolnjevanje z mednarodnimi standardi informacijske varnosti, kot je npr. ISO 27001 ter z različnimi okvirji upravljanja informacijske varnosti, kot sta COBIT 5 in ITIL (Rožanec & Lahajnar, 2017, str. 94).

### 2.2.3 Delovna preobremenitev

Človeški možgani imajo omejene zmogljivosti pomnjenja obdelav informacij in pomnjenja predmetov v spominu, sprejemanja odločitev in izvajanja nalog. Preobremenitev (angl. Workload) lahko povzroči težave s človeško zmogljivostjo in se odraža v počasnejšem izvajanju delovnih zadolžitev in nalog ter povečuje tveganje za povzročitev nastanka napak. Preobremenitev lahko povzroči težave z uspešnostjo, saj je povezana s kompetencami, kot npr. nekatere naloge zahtevajo manj osredotočenosti pri zaposlenih z več izkušnjami. Visoka delovna obremenitev negativno vpliva na varnost IS in posledično tudi na zadovoljstvo pri delu ter prispeva k višji fluktuaciji, s tem pa k izgubi usposobljenega delovnega kadra. S tem se ustvarja potencialne šibkosti in organizacijsko škodo z vidika človeških dejavnikov zaradi neprestane menjave kadra. Organizacijski dejavniki, kot so velika delovna preobremenitev, tvorijo pri ljudeh konflikt interesov med produktivnostjo in informacijsko varnostjo (Soltanmohammadi, Asadi & Ithnin, 2013, str. 333–334).

### 2.2.4 Podpora vodstva

Za uveljavitev politik v zvezi z varovanjem IS ter informacij v organizaciji mora vodstvo podpirati projekte že od faze načrtovanja do vseh faz implementiranja, nadgrajevanja in vzdrževanja. Vloga upravljanja varnosti IS ne sme samo zagovarjati, ampak tudi jasno sporočati politike varovanja informacij IS ter postopke v celotni organizaciji. Najmočnejši dejavnik upravljanja varnosti IS v organizacijah je dodelitev ustreznega proračuna v ta namen, ki je v celoti pod nadzorom uprave družbe. Splošno mnenje uprave je, da je za varnost IS v celoti odgovoren IT oddelek, ki bi moral zagotoviti namestitev ustrezne in varnostne programske sisteme za ohranjanje varnosti informacij (Pham Cong, Brennan & Furnell, 2019). Za zagotavljanje ustrezne varnosti mora višje vodstvo stremeti k temu, da neposredno sodeluje z odgovorno osebo, ki je zadolžena za informacijsko varnost in med njimi poteka jasna komunikacija, da se lahko nemoteno izvajajo celoviti procesi SUIV s strani vseh zaposlenih. Za učinkovito delovanje varnostnih politik in nemoteno delovanje komunikacijskega procesa je v celoti odgovorno vodstvo, ki sprejema proračun in mora biti sodelovanje med upravo in oddelkom za IT v popolnih sinergijah, da lahko govorimo o popolni podpori vodstva pri varovanju informacij (Alavi, Islam, Jahankhani & Al-Nemrat, 2013, str. 8).

### 2.2.5 Komuniciranje

Komunikacija (angl. Communication) je v organizacijskem kontekstu izmenjava sporočil in idej med ljudmi znotraj in zunaj organizacije za doseganje zastavljenih poslovnih ciljev. Komuniciranje zaposlenim omogoča, da sporočilo prenesejo ustreznemu slušatelju, destinaciji ali sistemu in ga ta tudi ustrezno razume. Obstaja veliko oblik komuniciranja, najpogostejše oblike komunikacije s človeško interakcijo so komunikacija iz oči v oči – pogovor in pisanje elektronskih sporočil ter pisanje na papir s pisalom. Namen učinkovite komunikacije je tudi ozaveščenost in motiviranost, zato na komunikacijo prevečkrat gledamo kot na samoumevno in pozabljamo na varnostne zahteve občutljivih informacij, kjer ključno vlogo igra ravno usklajena komunikacija. Varnostna politika občutljivih informacij se prevečkrat šteje kot grožnja v smislu konkurenčne klavzule v pogodbi o zaposlitvi. Če komunikacija ni pravilna ali se jo zlorabi, lahko škodi tudi varnosti celotnega IS in poslovnim procesom organizacije. Vodstvo mora učinkovito komunicirati z zaposlenimi in skrbeti za učinkovito komunikacijo skupaj z zavedanjem in namenskim zasledovanjem zastavljenih politik varnosti IS, poslovnih informacij ter poslovnih skrivnosti. Učinkovita komunikacija vključuje doseganje vseh zaposlenih v organizaciji na vseh ravneh hierarhije. Primeri komunikacije vključujejo varnostno ozaveščanje, delavnice, e-poštna sporočila, telefonske sestanke in osebna srečanja. V e-pošti izmenjujemo informacije med zaposlenimi v organizaciji in drugimi deležniki iz zunanjega okolja, ki je povezano v globalni kibernetski prostor, zato igra zaupnost pomembno vlogo v procesu komuniciranja. Zaposleni morajo biti seznanjeni z vrsto informacij, ki jih pošiljajo

zunanjim oz. tretjim osebam, da ne bi prišlo do kršitve zaupnosti. Upoštevati pa je treba tudi poslovna pravila dostopa do informacij in njihove obdelave znotraj organizacije (Alavi, Islam, Jahankhani & Al-Nemrat, 2013, str. 7; Pattinson & Anderson, 2007, str. 364).

### 2.2.6 Organizacijska kultura

Organizacijska kultura je sestavljena iz vrednot, prepričanj, praks, stališč in vedenj, ugleda ter etičnosti njenih zaposlenih. Ruighaver, Maynard in Chang (2007) verjamejo, da kultura informacijske varnosti (angl. Information security culture, v nadaljevanju ICS) zagotavlja vedenjski model, v katerem organizacije lažje obvladujejo zaščito informacij in vseh informacijskih sredstev. Zaposleni upoštevajo vgrajeno varnostno politiko kot del ISC znotraj širše organizacijske kulture. Podpora vodstva je potrebna za zagotovitev, da se ISC spodbuja za povečanje učinkovitosti izvajanja varnostnih politik organizacije kot celote. To lahko najučinkoviteje dosegamo s povečanjem programov ozaveščanja, usposabljanja in izobraževanja. Vrhnji management bi moral redno izvajati revizijo organizacijske kulture z namenom trajnostnega razvoja organizacije, boljšega obvladovanja organizacijske strukture in z namenom učinkovitejšega doseganja poslovnih ciljev (Alavi, Islam, Jahankhani & Al-Nemrat, 2013, str. 7). Proces spreminjanja organizacijske kulture se začne s potrebo po spremembi, v katero se vloži veliko organizacijskih sredstev za sprejemanje novih vrednot, prepričanj in stabilnejše organizacijske kulture, če sprememba pozitivno vpliva na izide organizacije. Bistvena razlika dojemanja organizacijske kulture in organizacijske klime je, da je kultura usmerjena v preteklost oz. prihodnost, organizacijska klima pa naj bi odražala trenutno stanje. Organizacijsko kulturo naj bi bilo težje spreminjati kot organizacijsko klimo, obe pa se pojavljata na nivoju odnosov in vrednot. Organizacijska kultura je podzavest posameznika, medtem ko organizacijska klima deluje kot skupek posameznikovega zavedanja (Moretti & Markič 2017).

### 2.2.7 Proračun organizacije

Vodenje organizacije zahteva finančna sredstva, torej je obstoj organizacije odvisen od ustreznega strateškega načrtovanja proračuna za posamezne temeljne in podporne funkcije organizacije. Strokovnjaki za informacijsko varnost zatrjujejo, da obstaja visoka korelacija med proračunom in učinkovitostjo varnosti IS ter informacij, ki jih vsebuje (Gratian, Bandi, Cukier, Dykstra & Ginther, 2018, str. 347). Finančna sredstva oz. proračun imajo močan vpliv, da varnost IS izpolnjuje svoje cilje. Organizacije morajo imeti učinkovito strategijo obvladovanja stroškov za reševanje tehničnih in človeških zahtev za zasledovanje varnosti IS. Organizacije ne morejo zasledovati ciljev varnosti IS v zadostni meri, če mehanizem za nadzor dostopa ni uporabljen ali če zaposleni niso ustrezno usposobljeni in seznanjeni v skladu s politikami o varovanju informacij in varnosti IS. Čeprav varnostne investicije v IS zahtevajo precejšnje finančne naložbe, se

žal vodstvo še vedno premalo zaveda, da hrbtenico njihovega poslovanja predstavlja izključno IS, kjer se nahajajo vsi podatki, informacije, poslovne skrivnosti in konkurenčne prednosti oz. celoten poslovni model, ki prinaša dodano vrednost organizaciji. Investicije, kot so vzdrževanje zdravega delovanja IS, so nujno potrebne, poleg tega je nujno potrebno zagotoviti tudi varnostno kopiranje in obnovitve po morebitnih nesrečah in incidentih. To bi morala biti glavna skrb odgovornih (celotnega vodstva) za izvajanje varnostne politike in varovanje vseh sredstev v IS. Pomen usposabljanja se pojavi, ko je poudarjen element stroškovne učinkovitosti. Nekateri ukrepi za zmanjšanje stroškov, na primer avtomatizirano zagotavljanje dostopa uporabnikom, zahtevajo programe usposabljanja, ki so cenejši. To dokazuje pozitiven odnos med načrtovanjem proračuna in neposrednim vplivom človeških dejavnikov na varovanje informacij (Pattinson in drugi, 2020, str. 3; Alavi, Islam, Jahankhani & Al-Nemrat, 2013, str. 6; Pattinson & Anderson, 2007, str. 366).

# 3 PREVERJANJE VELJAVNOSTI VPRAŠALNIKA, IZRAČUN VPLIVA ZNANJA NA ODNOS IN VEDENJE TER OCENA ZAVEDANJA S PREDLOGI IZBOLJŠAV INFORMACIJSKE VARNOSTI

## 3.1 Metodologija

Empirični del raziskave temelji na anonimnem predhodno preizkušenem anketnemu vprašalniku v angleškem jeziku po okvirju za merjenje človeškega vpliva na informacijsko varnost (angl. Human Aspect of Information Security Questionnaire, v nadaljevanju HAIS-Q). Ker je bil vprašalnik preveden v slovenski jezik in se s tem neizogibno pojavijo dobesedni prevodi, razširitve, posplošitve in prevodi s prevzetimi besedami, smo zaradi terminoloških in leksikalnih razlik veljavnost vprašalnika v slovenskem jeziku ponovno preverili z metodo faktorske analize. Namen HAIS-Q je raziskati človeški vpliv na informacijsko varnosti po treh dimenzijah znanja, odnosa ter vedenja pri zaposlenih v izbranem podjetju.

Zaposleni so svoje zavedanje o informacijski varnosti v spletnem vprašalniku ocenjevali s pomočjo petstopenjske Likertove lestvice od 1 do 5, kjer je 1 pomenilo »*Sploh se ne strinjam*«, 2 »*Se ne strinjam*«, 3 »*Niti se strinjam, niti se ne strinjam*«, 4 »*Se strinjam*« in 5 »*Popolnoma se strinjam*«. Spletni vprašalnik je bil izdelan na odprtokodni aplikaciji za izvajanje spletnega anketiranja 1KA ankete, razvoj katerega poteka na Centru za družboslovno informatiko na Fakulteti za družbene vede.

Empirični podatki so bili pridobljeni med decembrom 2022 in februarjem 2023. Anketni vprašalnik je bil anonimen ter prostovoljen. Vabilo zaposlenim k raziskavi je bilo poslano preko IS izbranega podjetja. Zbrani podatki so bili analizirani tako, da nobenega od

odgovorov ni bilo mogoče povezati z nobenim od zaposlenih. Anonimnost pridobljenih podatkov raziskave in namen analize sta bila podana v začetnem nagovoru zaposlenim, da so se lahko prepričali, da se s podatki ravna v skladu z etičnimi načeli. Za večjo anonimnost vprašalnika so bili v spletni platformi 1Ka ankete izklopljeni določeni parapodatki, ki omogočajo ustvarjanje enoličnih elektronskih revizijskih sledi – IP naslovov (angl. Internet Protocol – IP).

Za testiranje in potrditev veljavnosti podatkov zaradi prevoda smo uporabili faktorsko analizo (angl. Factor analysis – FA) z uporabo metode glavnih faktorjev (angl. Principal axis factoring – PAF). Ena izmed uporabnosti statistične metode faktorske analize je tudi zbiranje dokazov o veljavnosti. Faktorska analiza velja za enega najmočnejših pristopov multivariatne analize pri ugotavljanju konstruktne veljavnosti. Sama veljavnost pa ni lastnost merilnega instrumenta, temveč se nanaša na interpretacijo in razlago dobljenih rezultatov (Knekta, Runyon, Eddy & Brickman 2019, str. 6). Pogoj veljavnosti je potreben vsakič, ko se instrument uporabi, čeprav je že preverjen in potrjen za določeno populacijo in določene namene, kar pa ne pomeni, da velja za vse populacije, vse namene ter vse jezike (Kane, 2016, str. 198–201). S faktorsko analizo smo faktorske uteži določili na osnovi specifičnih varianc in z uporabljeno ortogonalno rotacijo faktorjev (angl. Varimax). Z uporabo eksplorativne faktorske analize smo poiskali skrite vzorce v naboru podatkov, lahko poiščemo povezave in jih pojasnimo med različnimi koncepti in konstrukti ter s tem prispevamo k ustvarjanju novih teorij (Knehta, Runyon, Eddy & Brickman 2019, str. 2). S pridobljenimi skupnimi faktorji za vsako izmed dimenzij smo s pomočjo dveh regresijskih modelov izračunali medsebojni vpliv med dimenzijami. Prvi regresijski model je testiral ali znanje napoveduje odnos, drugi model pa je testiral ali znanje in odnos napoveduje vedenje zaposlenih do informacijske varnosti. Na koncu smo iz pridobljenih odgovorih HAIS-Q izračunali še ocene ISA, katere rezultat smo dobili kot odstotek skupnega števila ugodnih odgovorov za vsako od treh glavnih dimenzij in po ciljnih področjih vprašalnika. Metoda izračuna ISA je povzeta po raziskavi avtorjev Pattisons in drugi (2016), ki so tudi avtorji HAIS-Q vprašalnika. Pred oceno ISA je bilo treba pridobljene podatke iz HAIS-Q normalizirati, saj je bil pri številnih vprašanjih uporabljen nasprotni vrstni red točkovanja (Parsons in drugi, 2014, str. 170).

## 3.2 Opis vprašalnika HAIS-Q, kaj meri ter praktična uporaba

Kruger in Kearney (2006) sta prvič priporočila model znanja, odnosa in vedenja (angl. The Knowledge, Attitude and Behavior, v nadaljevanju KAB) za merjenje ozaveščenosti o informacijski varnosti. Temelji na treh medsebojno povezanih komponentah, in sicer na afektu, vedenju in kogniciji, kar ustreza znanju, odnosu in vedenju. Parsons in drugi (2014) so v študiji orisali razvoj HAIS-Q in njegovo povezavo z modelom KAB po izvedbi testnega preizkušanja na vzorcu 500 zaposlenih Avstralcev. Uporabili so podoben pristop kot Kruger in Kearney (2006), kjer so upoštevali obstoječe politike in postopke informacijske varnosti, ki so relevantne za anketirance po modelu KAB, le da so bila

vprašanja oblikovana na podlagi vidikov upravljanja informacijske varnosti, kjer je bil cilj ugotoviti splošno prakso uporabe IT pri zaposlenih. Pod-področja v modelu HAIS-Q so bila oblikovana z namenom, da bi ugotovili pogoste človeške napake. Za vsako pod-področje je bilo ustvarjeno vprašanje, povezano z znanjem, odnosom in vedenjem. Rezultati njihove študije kažejo, da obstaja pozitivna povezava med znanjem in odnosom do politik ter postopkov informacijske varnosti ter vedenjem anketirancev. Parsons, Calić, Pattinson in Butavicius (2017) so dokazali konvergentno veljavnost vprašalnika, kar pomeni stopnjo skladnosti, merjeno v dveh ali več poskusih istega konstrukta z različnimi merskimi postopki. Notranja zanesljivost je bila dokazana s Cronbachovo alfo. Vsi rezultati so zavzemali interval med 0,75 in 0,82, kar je nad priporočljivo vrednostjo 0,70. Študija, ki so jo izvedli McCormac in drugi (2017b), je dala podobne rezultate v prvem testiranju, ki so zavzemali interval med 0,75 in 0,83 ter pri ponovnem testiranju med 0,78 in 0,84. Mittal in Ilavarasan (2019) sta prišla do zaključka, da v njunem primeru HAIS-Q ne prinese zanesljivih rezultatov, saj je zanesljivost konstruktov v devetih od osemnajst primerov pokazala Cronbachovo alfo manjšo od priporočene vrednosti, kar je verjetno nastalo zaradi metodoloških pomanjkljivosti.

McCorman in drugi (2017b) so izvedli nadaljnjo študijo o uporabi vprašalnika HAIS-Q, kjer se je vprašalnik izkazal kot učinkovit instrument za merjenje varnostne ozaveščenosti tako študentov, kot državnih uslužbencev v Avstraliji. Poročali so tudi o učinku družbene zaželenosti, kar lahko privede do netočnih meritev, vendar so ocenili, da kopičenje netočnih podatkov ni pomembno vplivalo na splošne rezultate. Učinku družbene zaželenosti – neresničnih odgovorov, se lahko izognemo z izvajanjem anket na spletu, saj s tem udeleženci ne občutijo pritiskov in možnosti identifikacije posameznih vprašalnikov. S tem pa pridobimo bolj resnične odgovore (Duffy, Smith, Terhanian & Bremer, 2005).

Predhodne študije so pokazale, da je ISA mogoče do neke mere predvideti z več dejavniki, kot so starost, spol, izobrazba, digitalna pismenost in nekateri osebnostni dejavniki (Hadlington, Popovac, Janicke, Yevseyeva & Jones, 2018; McCorman in drugi, 2017a; Pattinson, Butavicius, Parsons, McCormac & Calić, 2015). Na primer Pattinson, Butavicius, Parsons, McCormac in Calić (2015) so proučevali nezlonamerno računalniško vedenje in posamezne dejavnike, kot so starost zaposlenih, stopnjo izobrazbe, poznavanje IT ter njihovo osebnost. Rezultati so pokazali, da imajo zaposleni, ki so manj impulzivni, bolj odprti pri komunikaciji in manj poznajo uporabo računalnikov oz. IT, verjetno manj tvegano vedenje. Ta študija ni preučevala morebitnih razlik med moškimi in ženskami ter vedenja glede informacijske varnosti, vendar so rezultati odkrili pomembno pozitivno razmerje med starostjo in vedenjem glede varnosti informacij, kar kaže, da so starejši zaposleni poročali o boljšem in pravilnejšem vedenju glede informacijske varnosti kot mlajši zaposleni (Pattinson, Butavicius, Parsons, McCormac & Calić, 2015). Študije so na primer pokazale, da bodo posamezniki, ki so bolj vestni pri opravljanju delovnih nalog, imajo prijaznejši odnos do sodelavcev, višjo izobrazbo, imajo

boljše znanje pri rokovanju z IT, so notranje motivirani ter imajo manjšo nagnjenost h tveganju, imeli posledično verjetno višje ocene ISA.

V slovenskem okolju so Fujs, Vrhovec in Vavpotič (2021) HAIS-Q uporabili za kategorizacijo uporabnikov z namenom ocene človeškega vidika informacijske varnosti, kategorizirali uporabnike na podlagi pridobljenih ocen ter določili, kako na podlagi pridobljenih rezultatov prilagoditi usposabljanje uporabnikov. Uporabili so pristop v kombinaciji HAIS-Q in multivariatne metode razvrščanja v skupine. 63 spremenljivk, kar obsega celoten HAIS-Q, so združili v sedem faktorjev. Te faktorje pa so v drugem koraku uporabili za potrebe razvrščanja v skupine. Analizo so opravili na podlagi 165 uporabnikov IS na eni izmed slovenskih univerz. Rezultati analize so pokazali tri skupine uporabnikov (uporabnike z visokim, zmernim in nizkim tveganjem). Uporabniki z nizkim tveganjem dosegajo boljše rezultate pri posameznih področjih HAIS-Q. Uporabniki z zmernim in/ali visokim tveganjem pa so zanimivi z vidika prilagajanja individualnih usposabljanj, saj ti dve skupini najbolj odstopata od želenega. Z raziskavo so želeli doseči, da se uporabniki izobražujejo na področjih, ki jih najslabše pokrivajo ter optimizirajo stroške usposabljanj. V primerjavi s pristopi, ki so jih uporabili Parsons, Calić, Pattinson in Butavicius (2017), takšen pristop omogoča kategorizacijo uporabnikov na podlagi spremenljivk HAIS-Q in ne samo po demografskih karakteristikah (Fujs, Vrhovec & Vaupotič, 2021).

HAIS-Q iz priloge 5 vsebuje 63 trditev, od tega jih je 29 pozitivno ter 34 negativno ubesedenih, na sedmih različnih ciljnih področjih. Vsako od sedmih ciljnih področij ima po tri izjave o znanju, odnosu in vedenju. Parsons in drugi (2017) so pregledali različne politike informacijske varnosti po različnih sektorjih in panogah ter z ugotovitvami iz intervjujev z odgovornimi za informacijsko varnost razvili znotraj naslednja ciljna področja in pod-področja, kot prikazuje tabela 1.

*Tabela 1: Območja fokusa HAIS-Q*

| **Dimenzija** | | | **Ciljna področja** | **Pod-področja** |
|---|---|---|---|---|
| ZNANJE | ODNOS | VEDENJE | Upravljanje gesel | uporaba istega gesla |
| | | | | skupna raba gesel |
| | | | | izbira primernega gesla |
| | | | Uporaba elektronske pošte | odpiranje povezav v e-poštnih sporočil poznanih pošiljateljev |
| | | | | odpiranje povezav v e-poštnih sporočil neznanih pošiljateljev |
| | | | | odpiranje priponk v e-poštnih sporočilih neznanih pošiljateljev |
| | | | Uporaba interneta | prenos datotek |
| | | | | dostop do spletnih mest |
| | | | | vnos podatkov na spletna mesta |

se nadaljuje

*Tabela 1: Območja fokusa HAIS-Q (nad.)*

| | | | | |
|---|---|---|---|---|
| | | | Uporaba družabnih omrežij | nastavitev zasebnosti družabnih omrežij |
| | | | | upoštevanje teže posledic |
| | | | | objavljanje informacij o delu |
| | | | Mobilne naprave in delo na daljavo | fizično varovanje osebnih elektronskih naprav |
| | | | | pošiljanje občutljivih informacij preko Wi-Fi omrežja |
| | | | | nadzor nad elektronskimi napravami na javnih mestih |
| | | | Ravnanje z informacijami | obdelovanje občutljivih dokumentov |
| | | | | vstavljanje prenosnih naprav – npr. USB |
| | | | | puščanje občutljivih materialov na vidnih mestih |
| | | | Poročanje o incidentih | poročanje o sumljivem vedenju |
| | | | | ignoriranje slabega vedenja sodelavcev |
| | | | | poročanje o vseh varnostnih incidentih |

*Prirejeno po Parsons in drugi (2014).*

### 3.3 Opis modela, ki temelji na HAIS-Q vprašalniku

Okvir HAIS-Q je ustvarjen na podlagi modela KAB, ki sta ga prva priporočila Kruger in Kearney (2006) in je bil s strani znanstvene sfere deležen precejšnje pozornosti, uporabljen na različnih področjih raziskav ter pogosto uporabljen kot model za merjenje informacijske varnosti. Poudariti je potrebno, da izjave KAB predstavljajo le določen del celotnega konceptualnega modela, ki se razvija, testira in potrjuje z uporabo hibridnega ponavljajočega raziskovalnega pristopa. Na razmerje med znanjem, odnosom in vedenjem vplivajo številni individualni, intervencijski in organizacijski dejavniki. Na primer psihološki dejavnik, kot je udeležba na usposabljanjih in seminarjih ter kultura informacijske varnosti v podjetju lahko vplivajo na znanje, odnos in vedenje zaposlenih. V KAB modelu se znanje osredotoča na to, kar zaposleni ve, odnos se osredotoča na to, kaj si zaposleni misli, vedenje pa na to, kaj zaposleni počne. Predhodne empirične študije so pokazale, da KAB pomaga napovedati, kako zaposleni dojemajo informacijsko varnost. V kontekstu upravljanja informacijske varnosti znanje odraža spoznanja zaposlenih o informacijski varnosti. Odnos odraža, kako zaposleni gledajo na informacijsko varnost, vedenje pa odraža ukrepe, ki naj bi jih zaposleni sprejemali, ko se soočajo s tveganji informacijske varnosti oz. varnostnim incidentom. Predhodne raziskave so potrdile HAIS-Q kot zanesljivo merilo ISA in dokazale notranjo veljavnost. Dokaz, da je HAIS-Q zanesljiv in veljaven merilni instrument ISA, lahko organizaciji omogoči, da ocenijo učinkovitost izvedenih usposabljanj o informacijski varnosti in preverijo spremembe zaposlenih v ravni zavedanja o informacijski varnosti (Parsons, Calić, Pattinson & Butavicius, 2017, str. 3; Parsons, McCormac, Butavicius, Pattinson & Jerram, 2014, str. 166–167).

## 3.4 Demografske značilnosti vzorca raziskave

Metode opisne statistike, s katerimi opisujemo značilnosti vzorca, proučujejo opisne metapodatke o populaciji in njenih značilnosti. Demografski podatki vzorca so prikazani v tabeli 2. Raziskava je bila opravljena v izbranem podjetju na vzorcu 105 zaposlenih, kar predstavlja 36,70 % od skupno 286 aktivnih službenih računov (100 %). 63 anketirancev (60 %) je moškega spola in 42 anketirank (40 %) je ženskega spola. Starostni strukturi od 21 do 30 let pripada 25 anketirancev (23,80 %), od 31 do 40 let 27 anketirancev (25,70 %), od 41 do 50 let 23 anketirancev (21,90 %), od 51 do 60 let 17 anketirancev (16,20 %) ter 61 let ali več 13 anketirancev (12,40 %).

Izobrazbena struktura anketirancev je naslednja: največ zaposlenih 82 (78,10 %) ima specializacijo po višješolski izobrazbi, visokošolsko oz. univerzitetno izobrazbo, 9 zaposlenih (8,60 %) ima srednješolsko izobrazbo, sledijo zaposleni s specializacijo po visokošolski izobrazbi, magisterijem ali več, medtem ko ima 8 (7,60 %) ter 6 zaposlenih (5,70 %) višješolsko izobrazbo.

Četrtina zaposlenih, 27 (25,70 %), ima od 6 do 10 let delovne dobe, 20 oz. 19,00 % zaposlenih ima od 11 do 15 let delovne dobe. Po 12 anketirancev imajo skupine: do 5 let delovne dobe, od 21 do 25 let in od 31 do 35 let delovne dobe. 10 anketirancev (9,50 %) ima od 16 do 20 let delovne dobe, od 26 do 30 let ter od 36 do 40 let delovne dobe ima najmanj anketirancev, teh je v obeh skupinah po 6 anketirancev (5,70 %).

*Tabela 2: Demografski podatki vzorca zaposlenih*

| **Demografski podatki anketiranih** | | | |
|---|---|---|---|
| | | Frekvenca | Odstotek |
| Spol | Moški | 63 | 60,0 |
| | Ženski | 42 | 40,0 |
| Starost | do 21 do 30 let | 25 | 23,8 |
| | od 31 do 40 let | 27 | 25,7 |
| | od 41 do 50 let | 23 | 21,9 |
| | od 51 do 60 let | 17 | 16,2 |
| | 61 let ali več | 13 | 12,4 |
| Najvišja dosežena formalna izobrazba | Srednješolska | 9 | 8,6 |
| | Višješolska | 6 | 5,7 |
| | Specializacija po višješolski izobrazbi, visokošolska ali univerzitetna | 82 | 78,1 |

se nadaljuje

*Tabela 2: Demografski podatki vzorca zaposlenih (nad.)*

| | | | |
|---|---|---|---|
| | Specializacija po visokošolski izobrazbi, magisterij ali več | 8 | 7,6 |
| Delovna doba | do 5 let | 12 | 11,4 |
| | od 6 do 10 let | 27 | 25,7 |
| | od 11 do 15 let | 20 | 19,0 |
| | od 16 do 20 let | 10 | 9,5 |
| | od 21 do 25 let | 12 | 11,4 |
| | od 26 do 30 let | 6 | 5,7 |
| | od 31 do 35 let | 12 | 11,4 |
| | od 36 do 40 let | 6 | 5,7 |
| Skupno | | 105 | 100,0 |

*Vir: lastno delo.*

## 3.5 Izvedba faktorskih analiz

### 3.5.1 Faktorska analiza za dimenzijo znanje

Pred izvedbo faktorske analize smo iz tabele korelacijske matrike (angl. Corelation matrix), ki ima dimenzije 21 x 21, preverili, da med posameznimi spremenljivkami obstaja povezava, in da med seboj spremenljivke korelirajo. Trditve oz. indikatorji so bili merjeni na Likertovi lestvici od 1 do 5, zaradi tega med njimi ni močne razpršenosti. Z nadaljnjo eksploratorno faktorsko analizo smo obstoječe spremenljivke nadomestiti z manjšim številom faktorjev. Keiser-Meyer-Olkinova statistika (v nadaljevanju KMO) med seboj primerja velikosti korelacijskih in parcialnih korelacijskih koeficientov ter znaša 0,682 za dimenzijo znanje, kar je sprejemljivo oz. kaže na povprečno stopnjo medsebojne povezanosti. Vzorec je primerne velikosti, če vrednost KMO zavzema vrednost vsaj 0,5 (Hair, Celsi, Money, Samouel & Page, 2016). Za dimenzijo odnosa znaša KMO 0,643, kar kaže na povprečno stopnjo medsebojne povezanosti. Za tretjo dimenzijo vedenja znaša KMO 0,857, kar prav tako kaže na primernost vzorčenja.

Bartlettov test sferičnosti pokaže smiselnost uporabe faktorske analize. Z njim preizkušamo ničelno domnevo, da je osnovna korelacijska matrika enaka matriki enote, kar pomeni, da obstaja odvisnost med opazovanimi spremenljivkami. Tveganje je manjše od 0,05 in zato lahko zavrnemo ničelno domnevo, saj med njima obstaja povezanost. Stopinje prostosti za iskani Hi-kvadrat ($\chi^2$) so enake 210.

Podatki v tabeli 3 pokažejo, da so primerni za izvedbo faktorske analize in določitev števila novih faktorjev.

*Tabela 3: KMO Statistika in Bartlettov test sferičnosti*

| KMO Statistika in Bartlettov test sferičnosti | | **ZNANJE** | **ODNOS** | **VEDENJE** |
|---|---|---|---|---|
| Kaiser-Meyer-Olkin mera ustreznosti vzorca – KMO | | 0,682 | 0,643 | 0,857 |
| Bartlettov test sferičnosti | Hi-kvadrat ($\chi 2$) | 1194,038 | 1444,718 | 1989,388 |
| | Stopinje prostosti | 210 | 210 | 210 |
| | Statistična značilnost (p) | 0,000 | 0,000 | 0,000 |

*Vir: lastno delo.*

Po Kaiserjevem pravilu je število glavnih skupnih faktorjev enako številu lastnih vrednosti (angl. Eingenvalues), katerih vrednost znaša vsaj ena ali več. Za dimenzijo znanje se nakazuje na šest faktorjev, saj ima prvih šest večjo lastno vrednost od ena. Šest glavnih skupnih faktorjev je zajelo 69,01 % variabilnosti, saj sta skupna in specifična variabilnosti pri tej metodi združeni. Spremenljivke so razvrščene po velikosti faktorskih uteži. Šest faktorjev po metodi glavnih osi (angl. Principal Axis Factoring) zajame skupaj 57,37 % variabilnosti opazovanih spremenljivk, razvidno iz priloge 6.

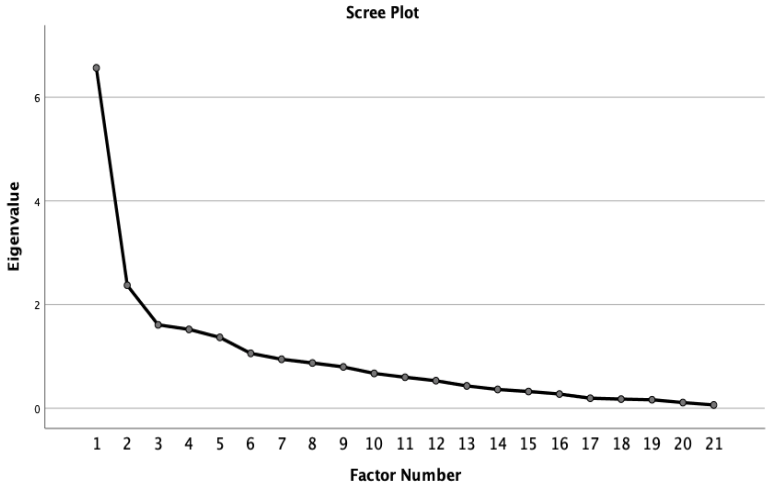
V družboslovju so informacije pogosto manj natančne in ni neobičajno, da rešitve celotne pojasnjene variance predstavljajo manj kot 60 %, kar je še vedno zadovoljivo (Hair, Black, Babin & Anderson, 2014, str. 107).

Prvotna rešitev faktorskih uteži ni podala ustrezne rešitve, da bi vsebinsko pojasnili posamezne faktorje, zato je bila uporabljena rotacija faktorjev za pridobitev njihove enostavnejše pojasnjevalne strukture. Priloga 1 prikazuje podane faktorske uteži (angl. Factor loadings) za dimenzijo znanje, ki so večje od vrednosti 0,4 po rotaciji Varimax.

Kot kriterij izbire števila faktorjev smo uporabili tudi Cattellov diagram drobirja (angl. Scree Plot). Iz diagrama smo razbrali točko, kjer se krivulja prelomi in na podlagi tega kriterija izbrali toliko komponent, kot jih je na levi strani točke preloma.

Catellov diagram oz. tudi diagram lastnih vrednosti na sliki 8 nakazuje na šest faktorjev, saj zadržimo tiste, ki imajo večjo lastno vrednost kot faktor, ki se nahaja na točki preloma krivulje. Metoda velja za subjektivno, saj dopušča več možnih rešitev, vendar jo je kot dodaten test smiselno uporabiti za preverjanje izbora števila faktorjev.

*Slika 8: Cattelov diagram drobirja za dimenzijo znanja*




*Vir: lastno delo.*

### *3.5.1.1 Faktorji za dimenzijo znanje*

Iz priloge 1 lahko ugotovimo, da je za dimenzijo znanje izbranih šest faktorjev. S prvim faktorjem je močno povezanih pet indikatorjev, in sicer:

- Sprejemljivo je odpreti priloge e-poštnih sporočil neznanih pošiljateljev.
- Na službeni računalnik lahko naložim katere koli datoteke, če mi te pomagajo opraviti moje delo.
- Na katerem koli spletnem mestu lahko vnesem kakršne koli podatke, če mi ti pomagajo pri opravljanju mojega dela.
- Povezav v e-poštnih sporočilih neznanega pošiljatelja ne odpiram.
- Med službenim časom ne bi smel dostopati do določenih spletnih mest.

Indikatorje, ki so povezani s prvim faktorjem, se vsebinsko najbolje opiše kot odpiranje prilog e-sporočil, nalaganje datotek in vnašanje podatkov. Prvi faktor predstavlja znanje o odpiranju prilog e-sporočil, prenosu datotek in vnašanje podatkov.

Z drugim faktorjem so močno povezani trije indikatorji:

- Za službene račune je primerno, da uporabljam enaka gesla kot jih na osebnih profilih družabnih omrežij.
- Gesla, ki jih uporabljam na delovnem mestu, lahko delim s sodelavci.
- Uporaba različnih simbolov, številk in črk je potrebna pri izbiri službenih gesel.

Indikatorji, ki so povezani z drugim faktorjem, se vsebinsko najbolje opišejo kot upravljanje z gesli. Drugi faktor predstavlja znanje z upravljanjem gesel.

S tretjim faktorjem so močno povezani trije indikatorji:

- Pri opravljanju dela na javnih mestih moram imeti računalnik ves čas pod nadzorom.
- Če najdem nosilec spomina (USB ključ) na javnem mestu, tega ne bi smel priključiti na službeni računalnik.
- Sprejemljivo je, da službene datoteke z občutljivimi podatki pošiljam tudi preko javnega omrežja Wi-Fi.

Indikatorji, ki so povezani s tretjim faktorjem, se vsebinsko najbolje opišejo kot ravnanje z mobilnimi napravami in varovanje informacij. Tretji faktor predstavlja znanje pri delu na daljavo.

S četrtim faktorjem so močno povezani trije indikatorji:

- O službi in delu lahko na družabnih omrežjih objavim, kar želim.
- Slabega varnostnega vedenja sodelavcev ne smem prezreti.
- Na delovni mizi lahko izven delovnega časa in moje navzočnosti (tudi čez noč) pustim dokumente, ki vsebujejo občutljive podatke.

Indikatorje, ki so povezani s četrtim faktorjem, se vsebinsko najbolje opiše kot objavljanje informacij o delu in ignoriranje slabega varnostnega vedenja. Četrti faktor predstavlja znanje o varovanju službenih informacij.

S petim faktorjem sta močno povezana dva indikatorja:

- Poročanje o varnostnih incidentih nadrejenim ni obvezno.
- Če opazim, da se nekdo v mojem delovnem okolju vede sumljivo, to sporočim nadrejenim.

Indikatorja, ki sta povezana s petim faktorjem, se vsebinsko najbolje opiše kot poročanje o slabem varnostnem vedenju in varnostnih incidentih. Peti faktor tako predstavlja znanje o varnostnih incidentih.

S šestim in zadnjim faktorjem iz dimenzije znanja sta povezana dva indikatorja:

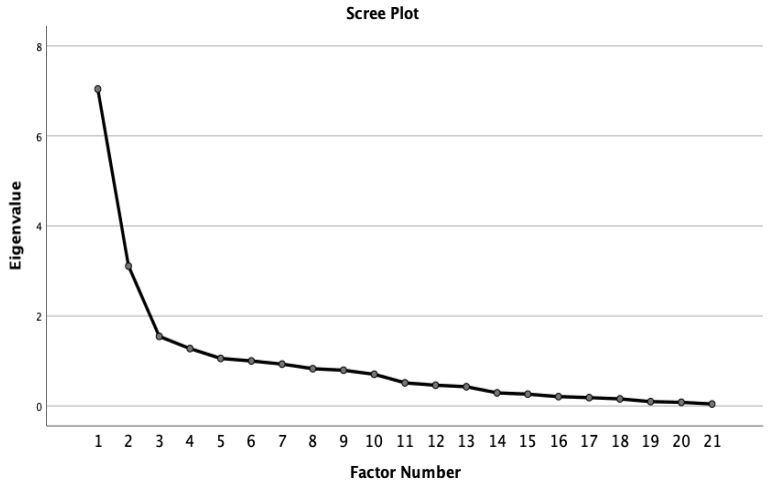
- Ne morem biti odpuščen zaradi nečesa, kar objavim na družabnih omrežjih.
- Občasno moram pregledati nastavitve zasebnosti na računih družabnih omrežij.

Indikatorja, ki sta povezana s šestim faktorjem, se vsebinsko najbolje opiše kot objavljanje službenih informacij in nastavitve zasebnosti. Šesti, zadnji faktor prve dimenzije, predstavlja znanje o zasebnosti.

### 3.5.2 Faktorska analiza za dimenzijo odnos

Priloga 7 – Celotna pojasnitev variance za dimenzijo odnos, prikazuje rezultate rotacije po metodi glavnih osi za tri glavne skupne faktorje, ki skupno zajamejo 49,68 % variabilnosti opazovanih spremenljivk. Pred rotacijo so trije skupni faktorji zajeli 55,68 % variabilnosti, saj se v tej metodi upošteva združeno skupno in specifično variabilnost. Pri faktorjih 4 in 5, kljub temu, da imata lastno vrednost večjo od ena, komunaliteta ni dosegla kriterija vrednosti vsaj 0,4 – Prikazano v prilogi 4. Posledično ima indikator več kot 60,00 % specifične variabilnosti. Da bodo indikatorji dejansko merili iskane latentne faktorje, ki jih ni mogoče neposredno izmeriti, morajo imeti dovolj visoke vrednosti komunalitet indikatorjev. Ker imata 4. in 5. faktor velik del specifične variabilnosti, nista primerna za uspešno merjenje iskanih faktorjev. Cattellov diagram drobirja na sliki 9 nakazuje prelom pri tretjem faktorju, zato se tudi po tej metodi odločimo za izbor treh faktorjev.

*Slika 9: Cattelov diagram drobirja za dimenzijo odnosa*




*Vir: lastno delo.*

#### *3.5.2.1 Faktorji za dimenzijo odnos*

Iz priloge 2 ugotovimo, da so s faktorsko analizo za dimenzijo odnos izbrani trije faktorji. S prvim faktorjem se močno povezuje osem indikatorjev:

- Nič slabega se ne more zgoditi, če zanemarim sumljivo vedenje sodelavca.

- Nič slabega se ne more zgoditi, če odprem povezavo v e-poštnem sporočilu neznanega pošiljatelja.
- Službeno geslo, ki vsebuje samo črke, je varno.
- Ni pomembno, katere podatke sem delil na spletnem mestu, če mi to pomaga pri opravljanju mojega dela.
- Ni pomembno, če na družabnih omrežjih objavljam stvari, ki jih običajno ne bi povedal/a v javnosti.
- Če najdem nosilec spomina (USB ključ) na javnem mestu, se ne more zgoditi nič slabega, če ga priključim na službeni računalnik.
- Če se nekdo v mojem delovnem okolju vede sumljivo in to zanemarim, se ne more zgoditi nič slabega.
- Odpiranje e-poštnih priponk od neznanega pošiljatelja je tvegano dejanje.

Indikatorje, ki so povezani s prvim faktorjem, se vsebinsko najbolje opiše kot odnos do ignoriranja slabega varnostnega vedenja, odpiranje povezav neznanih pošiljateljev in uporabo ustreznih gesel. Prvi faktor predstavlja odnos do varne obdelave podatkov in informacij, ki prihajajo od drugih oseb.

Prav tako je z drugim faktorjem močno povezanih osem indikatorjev:

- Tvegano je dostopati do občutljivih službenih datotek in podatkov na prenosnem računalniku, če nepooblaščene osebe vidijo računalniški zaslon.
- Tvegano je pošiljati občutljive datoteke z občutljivimi podatki preko javnega omrežja Wi-Fi.
- Tvegano je, da izven delovnega časa in moje navzočnosti (tudi čez noč) pustim dokumente, ki vsebujejo občutljive podatke, na vidni delovni površini.
- Poteza deljenja službenih gesel s sodelavci je slaba ideja, čeprav me včasih za to prosijo.
- Objavljati določene informacije o mojem delu na družabnih omrežjih je tvegano dejanje.
- Odlaganje nerazrezanih dokumentov z občutljivimi podatki v koš za papir je varno dejanje.
- To, da lahko v službi dostopam do določenega spletnega mesta, še ne pomeni, da je to tudi varno.
- Pri opravljanju dela na javnih mestih (kavarna, restavracija, knjižnica) je varno pustiti prenosni računalnik brez nadzora, čeprav samo za trenutek.

Indikatorje, ki so povezani z drugim faktorjem, se vsebinsko najbolje opiše kot dostopanje do občutljivih podatkov in pošiljanje ter objavljanje službenih informacij. Drugi faktor predstavlja odnos do občutljivih podatkov in informacij.

S tretjim in zadnjim faktorjem iz dimenzije odnosa so močno povezani naslednji trije indikatorji:

- Prenos datotek na službeni računalnik je lahko tvegan.
- Varno je uporabljati enaka gesla na družabnih omrežjih in službenih računih.
- Priporočljivo je, da redno pregledujem nastavitve zasebnosti na družabnih omrežjih.

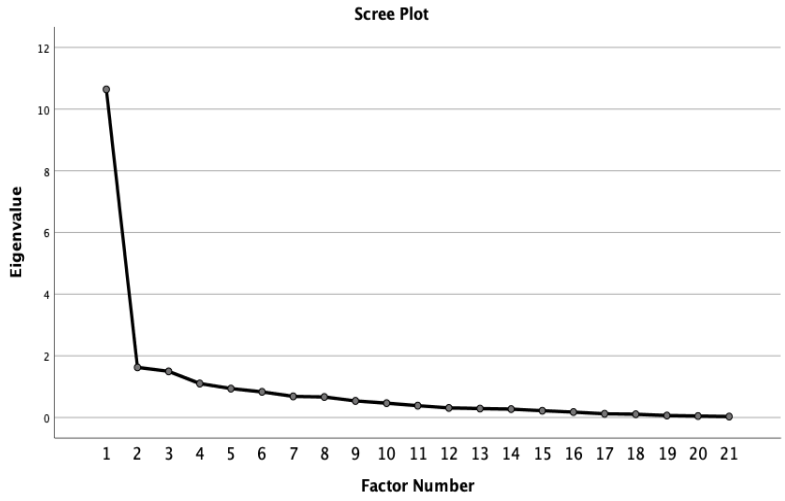
Indikatorje, ki so povezani s tretjim faktorjem, se vsebinsko najbolje opiše kot uporaba enakih gesel, spremljanje zasebnosti in prenos datotek. Tretji faktor predstavlja odnos do zasebnosti in varovanje službenih informacijskih sredstev.

### 3.5.3 Faktorska analiza za dimenzijo vedenje

Rezultat rotacije po metodi glavnih osi za dimenzijo vedenje vidno iz priloge 8, znaša za tri skupne faktorje približno 60,10 % variabilnosti opazovanih spremenljivk. Pred rotacijo so trije skupni faktorji zajeli 65,53 % variabilnosti, z upoštevano združeno skupno in specifično variabilnostjo. Prav tako kot pri faktorski analizi za dimenzijo odnos, tudi v faktorski analizi za vedenje 4. faktor ni primeren, čeprav njegova lastna vrednost znaša več kot ena.

Priloga 4 prikazuje komunaliteto 4. faktorja na intervalu med 0 in 1 bližje 0, kar je pokazatelj, da je skoraj celotna variabilnost tega indikatorja posledica specifičnega dejavnika. Cattellov diagrama drobirja na sliki 10 enako kot pri dimenziji odnos tudi za vedenje nakazuje točko preloma pri tretjem faktorju.

*Slika 10: Cattelov diagram drobirja za dimenzijo vedenja*




*Vir: lastno delo.*

#### *3.5.3.1 Faktorji za dimenzijo vedenje*

Iz priloge 3 ugotovimo, da so za dimenzijo odnos s faktorsko analizo izbrani trije faktorji. S prvim faktorjem se močno povezuje devet indikatorjev:

- Med službenim časom z dostopom do spletnega mesta obiščem vsa spletna mesta, ki jih želim.
- Na službeni računalnik naložim vse datoteke, ki mi omogočajo lažje opravljanje mojega dela.
- Če je povezava v e-poštnem sporočilu neznanega pošiljatelja videti zanimiva, to povezavo odprem.
- Datoteke z občutljivimi podatki pošiljam tudi preko javnega omrežja Wi-Fi.
- V službenih geslih uporabljam kombinacijo številk, simbolov in črk (malih in velikih).
- Če mi je pošiljatelj nepoznan, ne odpiram prilog v e-poštnem sporočilu.
- S sodelavci delim svoja službena gesla.
- Med delom na javnem mestu (kavarna, restavracija, knjižnica) včasih pustim prenosni računalnik brez nadzora.
- Kadar nisem na delovnem mestu, včasih pustim na vidni delovni površini dokumente z občutljivimi podatki.

Indikatorji, ki so povezani s prvim faktorjem, se vsebinsko najbolje opišejo kot dostopanje do spletnih mest, pošiljanje datotek in izbira ustreznih gesel. Prvi faktor predstavlja vedenje do izbire primernega gesla ter dostopanje do in varovanje občutljivih informacij.

Z drugim faktorjem se močno povezuje naslednjih šest indikatorjev:

- Če bi opazil/a, da sodelavec/ka ignorira varnostna pravila in politike, glede tega ne bi storil/a ničesar.
- Če bi videl/a, da se v delovnem okolju nekdo vede sumljivo, bi o tem opozoril nadrejenega.
- Ko je potrebno uničiti dokumente, ki vsebujejo občutljive podatke, vedno poskrbim, da jih uničim s pomočjo rezalnika papirja (šreder).
- V službeni računalnik ne bi priključeval/a nosilca spomina (USB ključ), ki ga najdem na javnem mestu.
- Za družabna omrežja in službene račune uporabljam različna gesla.
- Nastavitev zasebnosti na družabnih omrežjih ne pregledujem redno.

Indikatorje, ki so povezani z drugim faktorjem, se vsebinsko najbolje opiše kot ravnanje z občutljivimi podatki in informacijami ter varnostno vedenje. Drugi faktor tako

predstavlja vedenje do varnostnih incidentov ter zaščito občutljivih podatkov pred nepooblaščenim dostopom.

S tretjim in zadnjim faktorjem dimenzije vedenje je močno povezanih pet indikatorjev:

- Na družabnih omrežjih ne objavim ničesar, dokler ne premislim morebitnih negativnih posledic.
- O delu na družabnih omrežjih objavim, kar želim.
- Ko delam z dokumenti, ki vsebujejo občutljive podatke, preverim, da nepooblaščene osebe ne vidijo računalniškega zaslona.
- Pred vnosom podatkov ocenim varnost spletnega mesta.
- Če bi opazil/a varnostni incident, bi to nemudoma prijavil/a nadrejenemu.

Indikatorje, ki so povezani s tretjim oz. zadnjim faktorjem dimenzije vedenja, se vsebinsko najbolje opiše kot objavljanje občutljivih informacij in podatkov ter njihovo obdelavo. Tretji faktor predstavlja vedenje do obdelave in objave občutljivih podatkov in informacij.

S pomočjo faktorske analize smo ugotovili, da lahko med merjenimi spremenljivkami določimo novo množico spremenljivk (manj kot je merjenih), ki predstavljajo to, kar je skupnega vsem opazovanim spremenljivkam in jih lahko pojasnimo z manjšim številom posredno opazovanih spremenljivk oz. faktorji. Za dimenzijo znanja smo dobili 6 faktorjev, ki so definirani na podlagi 21 merjenih indikatorjev. Za dimenzijo odnosa smo dobili 3 faktorje, ki so bili definirani na podlagi 21 merjenih indikatorjev. Prav tako smo za dimenzijo vedenja dobil 3 faktorje na podlagi 21 merjenih indikatorjev.

### 3.6 Statistika zanesljivosti

Za preverjanje notranje konsistentnosti oz. notranje zanesljivosti anketnega inštrumenta smo uporabili koeficient Cronbach alfa (angl. Cronbach's alpha), ki ugotavlja, ali je anketni inštrument z več vprašanji na Likertovi lestvici zanesljiv. Knekta, Runyon, Eddy in Brickman (2019) navajajo, da je zanesljivost nujna komponenta za standardizacijo merskega instrumenta, ne zadostuje pa za samo veljavnost instrumenta. Zanesljivost se nanaša na sposobnost merskega instrumenta, da ob ponovitvi merjenja z njim dobimo podobne oz. primerljive rezultate, ob predpostavki, da koncepte merimo med enako skupino anketirancev (Hair, Celsi, Money, Samouel & Page, 2016).

Splošno osnovno pravilo je, da je rezultat alfe, ki je med vrednostjo 0,60 in 0,70, običajno sprejemljiv (Nunnally, 1978). Hair, Celsi, Money, Samouel in Page (2016) navajajo, da rezultat 0,6 velja za spodnjo sprejemljivo mejno vrednost zanesljivosti. Metoda omogoča raziskovalcu, da vidi, ali so odgovori veljavni. Vrednost alfe prikazano v tabeli 4 so lahko na intervalu od 0 do 1, kjer vrednost 1 predstavlja popolno korelacijo, vrednost 0 pa

ničelno korelacijo. Rezultat pokaže, kako zanesljivi so zbrani podatki. Na primer če bi veliko število zaposlenih odgovorilo v vprašalniku pri dimenziji odnosa, da se strinjajo, da je poteza deljenja službenih gesel s sodelavci slaba ideja, čeprav jih včasih za to prosijo, pri dimenziji vedenja bi pa v resnici odgovarjali, da s sodelavce delijo svoja službena gesla, potem bi test Cronbach alfe verjetno pokazal nizko oceno notranje konsistentnosti.

*Tabela 4: Zanesljivost merjenja notranje konsistentnosti s koeficientom Cronbach alfa*

| **Cronbach alfa (α) rezultat** | **Zanesljivost merjenja** |
|---|---|
| $\alpha \geq 0{,}9$ | Odlična |
| $0{,}9 > \alpha \geq 0{,}7$ | Dobra |
| $0{,}7 > \alpha \geq 0{,}6$ | Sprejemljiva |
| $0{,}6 > \alpha$ | Nezanesljiva |

*Prirejeno po Hair, Celsi, Money, Samouel & Page (2016).*

### 3.6.1 Statistika zanesljivosti notranje konsistentnosti HAIS-Q

Tabela 5 predstavlja Cronbach alfe za merjenje notranje konsistentnosti za dimenzijo znanja, odnosa in vedenja po celotnem KAB modelu. Rezultat Cronbach alfe za dimenzijo znanje znaša 0,828, za dimenzijo vedenja 0,868, kar kaže na dobro zanesljivost indikatorjev. Za dimenzijo odnos pa znaša vrednost 0,946, kar kaže na odlično zanesljivost indikatorjev oz. zanesljivost merjenja konstrukta.

*Tabela 5: Rezultati Cronbach alfe za notranjo konsistentnost HAIS-Q instrumenta po KAB dimenzijah*

| **Dimenzija** | **Cronbach alfa (α)** | **Število indikatorjev** |
|---|---|---|
| Znanje | 0,828 | 21 |
| Odnos | 0,868 | 21 |
| Vedenje | 0,946 | 21 |

*Vir: lastno delo.*

### 3.6.2 Statistika zanesljivosti za ciljna področja HAIS-Q

Priloga 9 prikazuje rezultate koeficientov Cronbach alfe za sedem ciljnih področij. Ti rezultati Cronbachovih alf kažejo, da ima HAIS-Q, kot splošno merilo ISA, dobro zanesljivost oz. notranjo konsistentnost znotraj ciljnih področij. Vrednosti koeficientov zanesljivosti zavzemajo interval od 0,744 do 0,894, kar kaže na dobro zanesljivost.

### 3.6.3 Statistika zanesljivosti faktorjev za dimenzijo znanje, odnos in vedenje

Priloga 10 prikazuje, da je petim od šestih vrednosti faktorjev za dimenzijo znanje znašala Cronbach alfa več kot 0,80, kar pomeni dobro zanesljivost konstrukta, prav tako pa znaša vrednost šestega faktorja 0,785, kar še vedno pokaže dober rezultat notranje konsistentnosti. Priloga 11 pokaže za dimenzijo odnos za vse tri dobljene faktorje vrednost Cronbach alfe, ki kaže na dobro zanesljivost in veljavnost konstrukta. Najvišja vrednost znaša za 1. faktor 0,874 ter najnižja vrednost Cronbach alfe za 2. faktor 0,793. Za 3. faktor pa znaša vrednost koeficienta 0,818. Zanesljivost zadnje dimenzije, vedenja, so vrednosti koeficienta Cronbach alfe pokazale kot dobro, razvidno iz priloge 12. Za 1. faktor znaša 0,947, za 2. faktor 0,860 ter za 3. faktor pokaže test Cronbach alfe odlično zanesljivost 0,821, kar pokaže dobro oz. odlično zanesljivost.

## 3.7 Izračun medsebojnega vpliva med dimenzijami znanja odnosa in vedenja

Medsebojni vpliv dobljenih faktorjev po dimenzijah preverjamo z dvema regresijskima modeloma. Za dimenzijo znanja – 6 faktorjev, dimenzijo odnosa – 3 faktorji in dimenzijo vedenja – 3 faktorji, ki smo jih predhodno dobili s faktorsko analizo. Pred analiziranjem smo za spremenljivke – faktorje po dimenzijah, ki so vključeni v model, izračunali Cronbach alfe za vse tri dimenzije kot merilo notranje skladnosti. Rezultati iz priloge 17 kažejo na dobro stopnjo zanesljivosti in so presegli mejno priporočeno vrednost 0,7.

V prvem regresijskem modelu smo izračunali vpliv faktorjev znanja na dimenzijo faktorjev odnosa, kjer je bila odvisna spremenljivka odnos, neodvisna pa znanje. Druga regresija prikazuje vpliv faktorjev med dimenzijo znanja na dimenzijo odnosa in vedenja, kjer sta bili odnos in znanje neodvisni spremenljivki ter vedenje odvisna spremenljivka.

S koeficientom multiple determinacije ($R^2$) pokažemo natančnost modela oz. linearno zvezo med odvisno in neodvisnimi spremenljivkami. Koeficient lahko zavzame interval med 0 in 1, kot prikazuje tabela 6, pri čemer vrednosti, ki so bližje 1, pomenijo večjo natančnost modela. Za določanje moči povezanosti spremenljivk uporabljamo lestvico vrednosti koeficienta R – koeficient multiple korelacije.

*Tabela 6: Vrednost koeficienta multiple korelacije in moč povezanosti*

| Vrednost koeficienta | Moč povezanosti |
|---|---|
| 0,00 | Ni povezanosti |
| 0,01–0,19 | Neznatna povezanost |
| 0,20–0,39 | Šibka povezanost |
| 0,40–0,69 | Zmerna povezanost |
| 0,70–0,89 | Močna povezanost |
| 0,90–0,99 | Zelo močna povezanost |

se nadaljuje

*Tabela 6: Vrednost koeficienta multiple korelacije in moč povezanosti (nad.)*

| | |
|---|---|
| 1,00 | Popolna povezanost |

*Prirejeno po Hair, Black, Babin & Anderson (2014).*

### 3.7.1 Vpliv znanja na odnos

Model iz tabele 7 za odvisno spremenljivko odnosa ima glede na znanje dobro pojasnjevalno moč. Vrednost regresijskega koeficienta (R) med dimenzijama znanja in odnosa znaša 0,857, kar kaže, da je linearna povezanost med odvisno in neodvisno spremenljivko močna. Koeficient multiple determinacije ($R^2$) pokaže na podlagi vzorčnih podatkov, da znanje o informacijski varnosti zaposlenih predvideva 73,50 % variabilnosti v njihovem odnosu do informacijske varnosti.

Statistično značilnost modela preverjamo z analizo variance odvisne spremenljivke, razvidno iz priloge 13 (F-preizkus), ki je pokazala, da je močno statistično značilna ($p = 0,000 < 0,01$). To pomeni, da lahko s stopnjo tveganja zavrnemo ničelno domnevo, da je regresijski koeficient enak nič in sprejmemo alternativno domnevo, ki pravi, da je model statistično pomemben, da je v modelu prisotna linearna odvisnost ter da ima model kot celota ustrezno pojasnjevalno moč.

Iz priloge 14 vpliv dimenzije znanja na odnos predstavlja koeficient ($\beta = 0,823$; $p = 0,000 < 0,01$). S t-statistiko preverimo domnevo ali so regresijski koeficienti statistično značilno različni od nič, kar predstavlja, da neodvisna spremenljivka vpliva na odvisno spremenljivko. Razmerje med dimenzijama znanja in odnosa lahko izrazimo z enačbo $Y= 0,752 + 0,823 X$, kjer Y predstavlja odnos in X označuje znanje. Znanje ($\beta = 0,823$, $t = 16,897$, $p < 0,000$) je pozitivno povezano z odnosom.

*Tabela 7: Ocene mer korelacije med dimenzijama znanje in odnos*

| Model | R | $R_1^2$ | Popravljeni $R_1^2$ | Standardna napaka ocene |
|---|---|---|---|---|
| 1 | .857[a] | 0,735 | 0,732 | 0,14606 |
| a (Konstanta), Znanje | | | | |
| b Odvisna spremenljivka: Odnos | | | | |

*Vir: lastno delo.*

### 3.7.2 Vpliv znanja na odnos in vedenje

Model za odvisno spremenljivko vedenja iz tabele 8 ima glede na znanje in odnos prav tako dobro pojasnjevalno moč. Vrednost regresijskega koeficienta (R) med dimenzijami

znanja in odnosa na dimenzijo vedenja znaša 0,807, kar kaže, da je linearna povezanost med odvisnima in neodvisno spremenljivko močna. Koeficient multiple determinacije ($R^2$) pokaže na podlagi vzorčnih podatkov, da znanje in odnos do informacijske varnosti zaposlenih predvideva 65,10 % variabilnosti v njihovem vedenju do informacijske varnosti.

*Tabela 8: Ocene mer korelacije med dimenzijami znanje, odnos in vedenje*

| Model | R | $R_1^2$ | Popravljen $R^2$ | Standardna napaka ocene |
|---|---|---|---|---|
| 1 | .807[a] | 0,651 | 0,645 | 0,23535 |
| a (Konstanta), Odnos, Znanje | | | | |
| b Odvisna spremenljivka: Vedenje | | | | |

*Vir: lastno delo.*

Statistično značilnost modela razvidno iz priloge 15 preverimo z analizo variance odvisne spremenljivke (F-preizkus), ki je pokazala, da je razlika močno statistično značilna ($p = 0,000 < 0,01$). To pomeni, da lahko s stopnjo tveganja zavrnemo ničelno domnevo, da sta regresijska koeficienta enaka nič in sprejmemo alternativno domnevo, da je regresijski model statistično pomemben in je v modelu prisotna linearna odvisnost ter ima ustrezno pojasnjevalno moč.

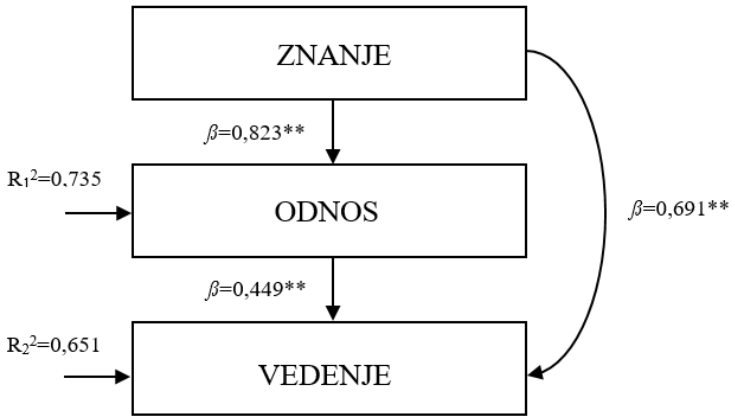
Iz Priloge 16 razberemo, da vpliv dimenzije znanja na vedenje predstavlja koeficient $\beta = 0,691$; $p = 0,000 < 0,01$, ter da vpliv dimenzije odnosa na vedenje predstavlja koeficient $\beta = 0,449$; $p = 0,006 < 0,01$.

T-statistika pokaže, da sta regresijska koeficienta statistično različna od nič in neodvisni spremenljivki vplivata na odvisno spremenljivko. Razmerje med dimenzijami znanja odnosa in vedenja lahko opišemo z enačbo $Y = -0,636 + 0,691\ X1 + 0,449\ X2$, kjer Y predstavlja dimenzijo vedenja, X1 predstavlja znanje in X2 predstavlja dimenzijo odnosa. Tako znanje ($\beta = 0,691$, $t = 4,532$, $p < 0,000$) kot odnos ($\beta = 0,449$, $t = 2,829$, $p < 0,006$) sta pozitivno povezana z vedenjem.

Z modelom, povzetim iz študije Parsons in drugi (2014) z rezultati regresijskih analiz, pokažemo rezultate, da znanje o informacijski varnosti zaposlenega predvideva približno 74,00 % variance v njihovem odnosu ter da je 65,00 % variance vedenja posledica znanja ter odnosa do informacijske varnosti.

Vrednosti koeficientov beta (β), prikazanih na sliki 11, kažejo, da ima znanje o informacijski varnosti večji vpliv na odnos do informacijske varnosti kot na vedenje do informacijske varnosti.

*Slika 11: Model vpliva znanja na odnos in vedenje (**p < 0.01)*




*Prirejeno po Parsons in drugi (2014).*

Ugotovitve nakazujejo, da je učinek znanja na vedenje posredovan z odnosom do informacijske varnosti, kar potrjuje model, ki smo ga zasledovali po Parsons in drugi (2014).

## 3.8 Merjenje zavedanja varovanja informacij

ISA je opredeljena kot razumevanje zavedanja do informacijske varnosti, ki je poudarjena v politikah, postopkih, pravilih in smernicah organizacije (Parsons, Calić, Pattinson & Butavicius, 2017). Pattinson in drugi (2016) ISA opredeljujejo kot kombinacijo poznavanja politik in postopkov informacijske varnosti organizacije ter odnosa uporabnika do tega, kako jih upošteva. Politike in postopki informacijske varnosti organizacije v splošnem vsebujejo priporočila o tem, kako naj se zaposleni obnašajo v prostoru organizacije, ko imajo opravka z upravljanjem gesel, spletno varnostjo in upravljanju ter poročanju o incidentih. ISA vključuje raven uporabnikovega razumevanja politik in postopkov za varovanje informacij in pomena spoštovanja zastavljenega. Povedano z drugimi besedami: ali počnemo in upoštevamo vse, da preprečimo izgubo zaupnosti, celovitosti ali razpoložljivosti podatkov in informacij (McCormac in drugi, 2017a; Parsons, McCormac, Butavicius, Pattinson & Jerram, 2014). Parsons, Calić, Pattinson in Butavicius (2017) predlagajo, da ISA temelji na treh vidikih: znanju, odnosu in vedenju. Če ima zaposleni ustrezno oceno ISA, je seznanjen z varnim vedenjem informacijske varnosti in njegovo vedenje temelji na najboljših praksah. Proces merjenja je eden glavnih pogojev za učinkovito upravljanje informacijske varnosti, saj z njim ugotavljamo, v kolikšni meri so izpolnjeni cilji informacijske varnostne politike in koliko ti cilji prispevajo k stanju celovite varnosti v organizaciji (Payne, 2006).

Tabela 9 prikazuje ravni rezultatov ISA, kjer so vrednosti ISA izračunane kot odstotek skupnega števila ugodnih odgovorov. Po uporabi obratnega vrstnega reda točkovanja

določenih trditev HAIS-Q vprašalnika so ugodni odgovori predstavljali vsoto odgovorov, ki so bili s strani anketirancev označeni kot "*Popolnoma se strinjam*" oz. "*Se strinjam*" in izraženi kot odstotek skupnega števila odgovorov za vsako fokusno področje informacijske varnosti znotraj HAIS-Q okvirja. Metoda je povzeta iz študije Pattisons in drugi (2016). Izračun ocene ISA se izračuna po enačbi (1):

$$ISA\ \% = \frac{Popolnoma\ se\ strinjam + se\ strinjam}{\text{Število vseh odgovorov} - \text{izločeni odgovori}} \quad (1)$$

Pattisons in drugi (2016) so za rezultat ISA določili kategorizirano lestvico ocenjevanja vrednosti, kaj predstavlja slabo, sprejemljivo in dobro oceno ISA:

- rezultati nad 80 veljajo za dobro zavedanje varnostnih groženj, s katerimi se sooča organizacija;
- rezultati od 60 do 79 veljajo za primerno zavedanje varnostnih groženj;
- rezultati pod 60 so obravnavani kot področja, katera je potrebno izboljšati in štejejo za slabo zavedanje informacijske varnosti.

*Tabela 9: ISA – odstotek pozitivnih odgovorov »Se strinjam« in »Popolnoma se strinjam«*

| Ciljno področje | Znanje | Odnos | Vedenje | Zavedanje informacijske varnosti – ISA |
|---|---|---|---|---|
| Upravljanje gesel | 95,3 | 93,0 | 89,5 | 92,6 |
| Uporaba elektronske pošte | 58,4 | 67,9 | 74,3 | 66,9 |
| Uporaba interneta | 86,3 | 94,6 | 85,8 | 88,9 |
| Uporaba družabnih omrežij | 87,2 | 94,3 | 89,8 | 90,4 |
| Mobilne naprave (delo od doma) | 96,2 | 97,4 | 86,0 | 93,2 |
| Ravnanje z informacijami | 94,0 | 96,5 | 89,8 | 93,4 |
| Poročanje o incidentih | 95,8 | 89,5 | 93,6 | 93,0 |
| Splošno stanje | 87,6 | 90,5 | 87,0 | 88,3 |

*Vir: lastno delo.*

### 3.8.1 Ocena ISA za znanje

Ocena ISA je bila izračunana na podanih HAIS-Q vprašanjih, glavnih treh področjih znanja, odnosa in vedenja. V prilogi 18 je navedena skupna ocena ISA za vprašanja, ki temeljijo na znanju. Splošno stanje za znanje ISA znaša 87,80 %, kar velja za dobro zavedanje varnostnih groženj. Najvišjo oceno ISA je vsebovala trditev "*Pri opravljanju dela na javnih mestih moram imeti računalnik ves čas pod nadzorom*", in sicer 99,00 %. Ta ocena ISA velja za odlično zavedanje, saj je 11,20 % nad povprečjem splošnega stanja oz. ocene ISA za znanje. To nakazuje na to, da zaposleni razumejo pomen varovanja zasebnosti med obdelavo službenih podatkov in informacij. Domnevamo tudi lahko, da

se zaposleni zavedajo potencialne nevarnosti tehnik socialnega inženiringa, npr. vizualnega vdora, pogovorno "*gledanje čez ramo*" (angl. Shoulder surfing) pri opravljanju službenih nalog na javnih mestih. Sledita trditvi "*Če opazim, da se nekdo v mojem delovnem okolju vede sumljivo, to sporočim nadrejenim*" in "*Slabega varnostnega vedenja sodelavcev ne smem prezreti*" s 97,10 %. Ta ocena ISA je pokazatelj, da se zaposleni dobro zavedajo pomembnosti hitrega odziva v primeru zaznave nevarnega vedenja, ki bi lahko povzročilo varnostni incident v IS podjetja.

Najnižjo oceno ISA je prejela trditev "S*prejemljivo je odpreti povezave v e-poštnih sporočilih ljudi, ki jih poznam*" s 25,70 %. To je zelo slab rezultat ISA in je za 62,10 % pod povprečjem ocene ISA za znanje. Nizka ocena lahko nakazuje na koncept poslovanja podjetja, ki je v lasti tuje gospodarske organizacije in glavnina procesa komunikacije poteka preko video povezav in e-pošte, predvsem z ljudmi, s katerimi se niso nikoli osebno srečali. Vseeno pa nakazuje na potencialno nevarnost oz. ranljivost in možnost vdora preko posredovane zlonamerne povezave z metodo socialnega inženiringa oz. preko človeške interakcije kot izsiljevalske programske opreme, ki šifrira datoteke v računalniku oz. se lahko razširi po celotnem IS. Največkrat se po namestitvi uporabniku prikaže pojavno okno, da bodo datoteke povrnjene v prvotno stanje po plačilu odkupnine. Tovrstni napadi največkrat prispejo kot povezava v e-poštnem sporočilu oz. se nehote prenese z zlonamernega spletnega mesta. Sledi trditev "*Povezave v e-poštnih sporočilih neznanega pošiljatelja ne odpiram*" s 70,50 %, kar nakazuje na prizadevanje za izboljšanje ISA, saj je prepoznano tveganje, da lahko zaposleni padejo v poskuse lažnega predstavljanja, prevare in podobne spletne poskuse goljufij. To zavedanje lahko izboljšamo npr. z izobraževanjem in praktično delavnico etičnega hekanja z lažnim predstavljanjem (angl. Phishing) v kombinaciji s HAIS-Q. Poleg tega se lahko ta statistika uporabi za izboljšanje varnostnih kontrol v IS, ki bi zaposlenim preprečile prenos preko povezav na zlonamernih spletnih mestih in preko datotek, ki vsebujejo zlonamerno programsko kodo.

### 3.8.2 Ocena ISA za odnos

Skupna ocena oz. splošno stanje ISA razvidno iz priloge 19 za vprašanja, ki temeljijo na odnosu, znaša 90,50 %, kar velja za odlično zavedanje o varnosti. Najvišja ocena ISA za odnos je bila za naslednji dve trditvi: "*Tvegano je dostopati do občutljivih službenih datotek in podatkov na prenosnem računalniku, če nepooblaščene osebe vidijo računalniški zaslon*" in "*Tvegano je, da izven delovnega časa in moje navzočnosti (tudi čez noč) pustim dokumente, ki vsebujejo občutljive podatke, na vidni delovni površini*", s 100-odstotnim zavedanjem, da se zaposleni zavedajo posledic, ki jih lahko povzročijo, če nepooblaščene osebe vidijo zaupne podatke in tvegajo razkritje občutljivih informacij. Trditev "*Poteza deljenja službenih gesel s sodelavci je slaba ideja, čeprav me včasih za to prosijo*", je bila ocenjena z 99,00-odstotnim zavedanjem, trditvi "*To, da lahko v službi dostopam do določenega spletnega mesta, še ne pomeni, da je to tudi varno*" in

"*Objavljati določene informacije o mojem delu na družabnih omrežjih je tvegano dejanje*", pa z 98,10-odstotnim zavedanjem. Ta ocena ISA nakazuje, da se zaposleni prav tako odlično zavedajo informacijske varnosti in presojajo ter podvomijo o dostopanju in varnosti na določenih spletnih mestih ter tveganemu odnosu objavljanja službenih informacij o delu na družabnih omrežjih.

Trditev na podlagi odnosa z najnižjo oceno ISA "*Povezave v e-poštnih sporočilih ljudi, ki jih poznam je varno odpirati*" je imela 25,70 %. Ta ocena je 64,80 % pod povprečjem splošnega stanja ISA za odnos (90,50 %). Temu rezultatu prav tako velja nameniti pozornosti, ker je IS treba izboljšati s poudarkom na tehničnih tehnologijah izboljšanja varnosti e-pošte. Ta ocena ISA tudi kaže na potencialno slab odnos do zavedanja informacijske varnosti glede odpiranja sporočil poznanih pošiljatelje, kar je znak, da je odnos do klikanja na povezave v e-poštnih sporočilih varen z vidika zaposlenih do ljudi, ki jih poznajo. Lažna e-poštna sporočila danes popolnoma lažno predstavljajo in ponarejajo poznane e-poštne naslove. V tem primeru bi se v povezavo lažnega predstavljanja najverjetneje ujelo 74,30 % zaposlenih, kar predstavlja zaskrbljujoč podatek. Sledi trditev "*Nič slabega se ne more zgoditi, če odprem povezavo v e-poštnem sporočilu neznanega pošiljatelja*", s 85,70 %. Ta ocena je sicer dobra in razumna, vendar še vedno nakazuje na potencialno tveganje, da se nekateri izmed zaposlenih ne zavedajo nevarnosti spletnega kriminala, ki se lahko nahajajo v vsebinah povezav in priponkah e-poštnih sporočil. Zaupne in občutljive podatke je treba obravnavati z največjo možno varnostjo in poskusiti izničiti varnostna tveganja. Odnos zaposlenih do informacijske varnosti v splošnem je bil ugotovljen kot odličen (90,50 %), vendar se ga še vedno lahko izboljša z vsebinskim poudarkom varnosti e-poštnega komuniciranja. Smiselno je razmisliti o usposabljanju zaposlenih v smeri prepoznave e-poštnega socialnega inženiringa z izvajanjem simulacijskih vaj, z namenom preverjanja sposobnosti prepoznavanja nezaželene pošte, da se preveri sposobnost prepoznavanja lažnega predstavljanja in odziva nanj.

### 3.8.3 Ocena ISA za vedenje

Skupna ocena ISA razvidna iz priloge 20 za vprašanja, ki temeljijo na vedenju, znaša 87,00 %. Ocena je znak dobre in učinkovite ozaveščenosti in nakazuje, da so vedenjski nameni zaposlenih v organizaciji nenaklonjeni tveganju. Najvišja ocena ISA za vedenje po HAIS-Q okvirju je "*Če bi videl/a, da se v delovnem okolju nekdo vede sumljivo, bi o tem opozoril nadrejenega*", s 95,20 %. Ta ocena kaže na jasno nenaklonjenost tveganju do potencialnih varnostnih incidentov. Sledita vprašanji "*Pred vnosom podatkov ocenim varnost spletnega mesta*" in "*Ko je potrebno uničiti dokumente, ki vsebujejo občutljive podatke vedno poskrbim, da jih uničim s pomočjo rezalnika papirja (šreder)*", obe s po 94,30 %. To kaže, da 94,30 % (7,30 % nad povprečjem ocene ISA za vedenje) zaposlenih ve, da je pred vnosom podatkov potrebno oceniti varnost spletnega mesta in da je potrebno dokumente, ki vsebujejo občutljive podatke, uničiti s pomočjo rezalnika papirja.

To je znak dobre prakse varovanja informacij in izboljšuje splošno oceno stanja vedenja do varnosti informacij v organizaciji. Poleg tega varno vedenje ozaveščanja kaže tudi na dobro razumevanje ozaveščenosti o varovanju informacij, saj je bil najnižji vedenjsko usmerjen rezultat ISA pri trditvi "*Povezav v e-poštnih sporočilih ne odpiram vedno samo zato, ker prihaja od poznane osebe*", z 61,90 %. Ta ocena je nizka, vendar sprejemljiva in kaže, da se nekateri zaposleni zavedajo, da povezave v e-poštnih sporočilih niso vedno varne samo zato, ker prihajajo od poznane osebe. Tako je 61,90 % zaposlenih v vzorcu nenaklonjenih odpiranju povezav, preden jo ocenijo ali je varna, medtem ko jih ostalih 38,10 % zaposlenih povezavo odpre, ne da bi prej vsaj vizualno ocenili, ali je povezavo varno odpirati in da ne vsebuje znakov zlonamernih elementov. Sledijo trditve "*Če je povezava v e-poštnem sporočilu neznanega pošiljatelja videti zanimiva, to povezavo odprem*" in "*Med službenim časom z dostopom do spleta obiščem vsa spletna mesta, ki jih želim*" s po 81,00 %. Omeniti velja še trditev "*Če mi je pošiljatelj nepoznan, ne odpiram prilog v e-poštnem sporočilu*", z 80,00 %, saj se vsebinsko navezuje na trditvi "*Povezav v e-poštnih sporočilih ne odpiram vedno samo zato, ker prihaja od poznane osebe*" in "*Če je povezava v e-poštnem sporočilu neznanega pošiljatelja videti zanimiva, to povezavo odprem*". Ta ocena nakazuje na razmislek glede povečanja zaščite varnosti e-pošte z uporabo tehnologije za samodejno blokiranje e-poštnih sporočil in blokiranje zlonamernih povezav, če bi zaposleni nezavedno vseeno kliknil na povezavo.

# 4 OMEJITVE RAZISKOVANJA IN SMERNICE ZA NADALJNJE RAZISKOVANJE

Že med izvajanjem raziskave smo predpostavljali, da se bomo tekom raziskovanja srečevali z nekaterimi pomanjkljivostmi in omejitvami, ki so v magistrskem delu metodološke narave. Zaradi časovne dolžine anketnega vprašalnika se kaže, da je bilo v vzorec raziskave vključeno manjše število zaposlenih, ki so v celoti izpolnili vprašalnik, vendar vseeno dovolj, da je bil vzorec reprezentativen. Upoštevati je potrebno tudi omejitev morebitnega pristranskega odgovarjanja na trditve ter to, da so situacije v trditvah oblikovane na splošen kontekst, saj so resnične situacije bolj kompleksne. Včasih nastane situacija, ko prenosno napravo (pametni telefon ali prenosni računalnik) pustimo za trenutek brez nadzora, vendar je ta zaščiten s primernim geslom in ohranja delovno okolje varovano pred nepooblaščenim posegom. Upoštevati je potrebno tudi specifičnost meje med varnim in negotovim vedenjem. V realnih situacijah jih je včasih nemogoče določiti. Za objektivnejšo oceno bi bilo potrebno opraviti praktično preverjanje znanja vsakega zaposlenega s strani strokovno usposobljene osebe, vendar to glede na učinek največkrat ni ekonomsko upravičena metoda. Za bolj relevantne rezultate bi bilo smiselno raziskavo ponoviti na večjem vzorcu števila zaposlenih. V kolikor bi s ponovitvijo pridobili podobne rezultate, bi lahko z večjo gotovostjo govorili tudi o večji veljavnosti vprašalnika. Poudariti velja tudi glavno omejitev, ki jo predstavlja uporaba modela regresijske analize, tj. da je oblika povezave med spremenljivkami linearna. Pri izvedbi

empiričnega dela je imela anketa časovno omejeni okvir zaradi omejene dostopnosti spletnega vprašalnika. Anketiranje je potekalo šest tednov v začetku januarja do sredine februarja 2023. Z večjim deležem izpolnjenih anket izmed vseh zaposlenih bi lahko dosegli višjo stopnjo zanesljivosti empiričnega dela raziskave. Omeniti velja, da je bil vzorec omejen na točno določeni populaciji zaposlenih, zato rezultatov ni mogoče posploševati na splošno stanje ISA zaposlenih v slovenskih podjetjih.

Za nadaljnje raziskave bi bilo smiselno na podlagi pridobljenih rezultatov in ugotovitev faktorske analize, metode regresijske analize in ocen ISA, ki smo jih v zaključnem delu analizirali z namenom pridobitve osnovnih podatkov o zaposlenih glede stanja ISA, nadgradili z izvedbo praktične delavnice lažnega predstavljanja, ki temelji na tehnikah socialnega inženiringa preko e-pošte, saj je ocena ISA za uporabo elektronske pošte pokazala nizko raven ISA med zaposlenimi in jo velja spremljati tudi v nadaljnje. Po izvedbi praktične delavnice bi nato ponovili raziskavo z uporabo HAIS-Q ter ponovno izračunali ocene vrednosti ISA po dimenzijah in ciljnih pod-področjih ter dobljene rezultate primerjali z rezultati, dobljenimi iz raziskave v predstavljenem zaključnem delu. S tem bi pridobili zanimive rezultate, s katerimi bi lahko boljše ovrednotili učinkovitost izvajanj usposabljanj s področja informacijske varnosti. Rezultati lahko podajo usmeritve za usposabljanja v manjših skupinah glede na zaznane šibkosti pri ocenah zavedanja informacijske varnosti. Uspešnost praktične delavnice bi se morala pokazati v izboljšavi ocen ISA za vse tri dimenzije in po vseh sedmih ciljnih področjih. Za večjo objektivnost podanih odgovorov lahko v prihodnje izpustimo sklop demografskih vprašanj in dobimo realnejšo sliko ocen ISA zaposlenih pri ponovitvi raziskave s HAIS-Q.

Izračun vpliva znanja na odnos in vedenje, ki smo ga predstavili z dvema regresijskima modeloma, bi bilo v nadalje smiselno preveriti z modeliranjem strukturnih enačb, saj tovrstno modeliranje omogoča izločanje učinka kolinearnosti med neodvisnimi spremenljivkami in pomaga pri identifikaciji osnovnih konstruktov, ki so podvrženi med seboj podobnim spremenljivkam, ter tudi pri ocenjevanju moči povezav med dimenzijami/konstrukti. Strukturne enačbe omogočajo tudi možnost razlage posrednih in neposrednih vplivov posameznih spremenljivk, pri čemer ima tovrsten model v primerjavi z regresijsko analizo veliko večjo moč razlage in natančno definira neposredne in posredne vplive latentnih spremenljivk – faktorjev (Milfelner, Mumel & Snoj, 2006).

# SKLEP

Odtekanje zaupnih podatkov in informacij krši načelo zaupnosti in ogroža celovito informacijsko varnost. Da bi zagotovili najvišjo raven informacijske varnosti, mora organizacija krepiti organizacijsko kulturo ISA od najvišje ravni hierarhije – vrhnjega managementa do najnižje ravni – zaposlenih. Organizacija mora na vseh ravneh zagotavljati jasne in razumljive politike informacijske varnosti, da se prepreči zloraba informacijske varnosti in zavaruje poslovno vrednost informacij. Razumevanje ISA oz.

znanja, odnosa in vedenja do informacijske varnosti ter osredotočanje na človeški dejavnik omogoča izboljšavo obstoječih varnostnih okvirjev in prevzetih varnostnih standardov. Večina varnostnih incidentov in vdorov, do katerih pride, je posledica organizacijske klime in človeške interakcije, zato nam razumevanje dejavnikov človeškega vpliva na informacijsko varnost pomaga minimizirati tveganje, ki ga nosi organizacija z incidenti, s katerimi se sooča.

Tehnologiji AI in ML sta radikalno pripomogli k avtomatizaciji rutinskega dela z znanjem in ustvarjanjem poslovne vrednosti iz obstoječih podatkov, nista pa sposobni sklepanja, zavedanja, razmišljanja in ustvarjanja novih poslovnih modelov. Dejanska vrednost tehnologij AI in ML se kaže v vrednosti in celovitosti podatkov, s katerimi operira. Tehnologija AI ne bo nikoli imela intelektualnega kapitala, ki vključuje ustvarjalnost, vodenje, analiziranje, humor in izvirno razmišljanje. Zato je človeški dejavnik še kako pomemben pri učinkovitem delovanju kakršne koli tehnologije. Tehnologije AI in ML bodo v prihodnje postale bistvene pri zaščiti podatkov in obvladovanju vse bolj zapletenih groženj, saj algoritmi, ki delujejo v ozadju, v realnem času prepoznajo spremembe v vzorcih in nedovoljene posege v podatke.

Okvir HAIS-Q je bil preveden v slovenščino in končna različica je vključevala vseh sedem ciljnih področij s skupno 63 trditvami oz. indikatorji. V raziskavi smo notranjo konsistentnost ocenjevali na vzorcu 105 zaposlenih. Zanesljivost prevedenega vprašalnika smo ocenili z vidika notranje skladnosti s koeficientom Cronbach alfa za znanje, ki predstavlja poznavanje politik informacijske varnosti in znaša 0,828. Za dimenzijo odnosa, ki predstavlja odnos zaposlenih do informacijske varnosti, koeficient Cronbach alfa znaša 0,868. Za dimenzijo vedenje, ki predstavlja prakso zaposlenih do informacijske varnosti, Cronbach alfa znaša 0,946. Statistiko zanesljivosti smo izračunali tudi za ciljna področja, katerih Cronbach alfe zavzemajo interval od 0,744 do 0,894. Iz teh rezultatov lahko sklepamo, da je HAIS-Q notranje skladen.

Faktorska analiza je na predhodno uspešno izpolnjenih predpogojih za zmanjševanje dimenzij podatkov po pravokotni rotaciji Varimax podala za dimenzijo znanje šest faktorjev, s katerimi pojasnimo 57,38 % skupne variance. Za dimenzijo odnosa je faktorska analiza podala tri faktorje, s katerimi pojasnimo 49,68 % skupne variance, ter za dimenzijo vedenja prav tako tri faktorje, s katerimi pojasnimo 60,10 % skupne variance. S faktorsko analizo smo uspešno dosegli zmanjšanje števila merjenih spremenljivk (63) na 12 faktorjev. Z rezultati smo potrdili, da je preveden HAIS-Q še vedno veljaven. Izračun vpliva znanja na odnos in vedenje nakazuje, da tako dimenzija znanja ($\beta = 0{,}691$, $t = 4{,}532$, $p < 0{,}000$) kot odnos ($\beta = 0{,}449$, $t = 2{,}829$, $p < 0{,}006$) vplivata pozitivno na vedenje. Organizacija se mora osredotočiti na programe izboljšanja ozaveščenosti o informacijski varnosti, predvsem na dimenzijo znanja z interaktivnimi delavnicami, kot je lažno predstavljanje in drugimi usposabljanji, ki povečujejo zavedanje

do informacijske varnosti. Učinek izobraževanj lahko kasneje ocenimo s HAIS-Q in pridobijo informacijo, ali so dosegla svoj namen.

Končna splošna ocena ISA, pridobljena na vzorcu 105 zaposlenih, izračunana kot povprečje po dimenzijah znanja, odnosa in vedenja, velja za zelo dobro oceno zavedanja varnostnih groženj, s katerimi se sooča podjetje; ta znaša 88,30 %. Ocena ISA za dimenzijo znanje znaša 87,80 %, za dimenzijo odnosa 90,50 % ter za dimenzijo vedenja 87,00 %, kar pokaže zelo dobre ocene ISA za upoštevanje varnostnih politik, odnosa do varnostnih politik ter varnostne prakse. Varnostna ozaveščenost po ciljnih področjih kaže zelo podobne rezultate ocen kot za glavne tri dimenzije, tako da se ocene porazdeljujejo na intervalu od 66,90 % do 93,40 %. Najslabši rezultat predstavlja uporaba elektronske pošte (66,90 %), čemur velja posvetiti dodatno pozornost in to spremljati glede na to, v kolikšni meri imajo posamezne skupine po oddelkih stik z neznanimi pošiljatelji. Upoštevati je potrebno dejstvo, da je podjetje v tuji lasti in posluje globalno ter da zaposleni vsakodnevno komunicirajo z ljudmi, katerih niso še nikoli spoznali osebno. Slaba ocena ISA za uporabo elektronske pošte sama po sebi še ne pomeni slabega zavedanja, ampak je smiselno iskati logično razlago glede na visoke ocene ostalih področij Rezultati merjenja zavedanja kažejo, da rezultati uporabe e-pošte ne ustrezajo dobremu zavedanju po vseh treh dimenzijah znanja, odnosa in vedenja, kar nakazuje, da mora podjetje sprejeti potrebne ukrepe, kot je usposabljanje varne uporabe elektronske pošte s poudarkom na prepoznavi lažnih sporočil. Uporaba programov praktičnega usposabljanja je učinkovita metoda za izboljšanje znanja in zavedanja o potencialnih grožnjah ter tveganjih, saj je elektronska pošta še vedno najljubša tarča spletnega kriminala. Podjetje bi lahko izvedlo delavnico simulacije lažnega predstavljanja po e-pošti s souporabo HAIS-Q vprašalnika. Pridobljene rezultate bi primerjali z dobljenimi rezultati v tem magistrskem delu, tako bi lahko izmerili uspešnost usposabljanja, ki bi se moralo kazati v izboljšanju rezultatov po ciljnih področjih, predvsem pri uporabi e-pošte.

Ugotovitev raziskave, da je varno in sprejemljivo odpirati e-poštna sporočila, ker prihajajo od znanih pošiljateljev, predstavlja tveganje, saj so e-poštna sporočila lahko lažna. Podjetje se mora še posebej osredotočiti na zaposlene, ki imajo vsakodnevni stik z neznanimi ljudmi, kot so potencialni kupci ali predstavniki strank. Ti zaposleni predstavljajo večje tveganje do klikanja povezav, da bi obravnavali zahtevo pošiljatelja. Predvidevamo lahko, da bi se moralo to odražalo tudi pri odpiranju prilog. Kot tehnično izboljšavo bi podjetje lahko nadgradilo poštne strežnike s funkcijo karantene, ki nezaželeno in nevarno e-poštno sporočilo zaustavi že ob vstopu v sistem in v e-poštni predal pride samo preverjena e-sporočila brez zlonamernih vsebin. Tako bi zaposlenim ponudili dodatno varovalo, da v predogledu vidijo pošiljatelja in zadevo, kar je običajno dovolj, da prepoznajo izsiljevalsko sporočilo.

Dobljeni rezultati analize HAIS-Q in izračuni ocene ISA potrjujejo, da je merski inštrument stroškovno učinkovito orodje za ocenjevanje človeških vidikov zavedanja informacijske varnosti. Iz dobljenih rezultatov ocen ISA lahko razberemo, da podjetje

porabi precej sredstev za programe izobraževanja o informacijski varnosti. Instrument HAIS-Q v kombinaciji z ocenami ISA pa omogoča jasnejši vpogled v varnostno kulturo zavedanja zaposlenih in podaja rezultat v smernicah za učinkovitejšo organizacijo izobraževanj s področja informacijske varnosti. Rezultate raziskave je mogoče uporabiti tudi za načrtovanje in izboljšanje celostnih informacijsko varnostnih strategij ter omogočajo iskanje potencialnih nevarnosti za povzročitev varnostnega incidenta v IS.

Organizacija lahko z rednim spremljanjem ISA načrtuje individualne programe praktičnih usposabljanj. Lahko jih prilagaja posamezniku oz. manjšim skupinam glede na prepoznane šibkosti ter z ustreznimi ukrepi zmanjša človeške vplive in tvegano vedenje zaposlenih do celovite varnosti informacij in varnosti IS. Z izvajanjem praktičnega usposabljanja lažnega predstavljanja po elektronski pošti s simulacijo napada na IS, ki je sicer uspešno sredstvo za opazovanje vedenja zaposlenih, ko se dejansko soočijo z varnostnim incidentom v kombinaciji HAIS-Q, lahko organizacija ugotavlja napredovanje v vedenju, ki je posledica pozitivnega vpliva znanja in odnosa. ISA zaposlenih lahko podjetje izboljša tudi brez povečevanja finančnih sredstev v proračun, ki je namenjen informacijski varnosti. To lahko doseže tako, da prilagodi programe ozaveščanja glede na pridobljene ocene ISA namesto povečanja pogostosti izvajanja splošnih programov informacijske varnosti. V porastu uporabe vseh vrst IKT opreme pri izvajanju poslovnih procesov HAIS-Q nedvomno prispeva k raziskovanju teoretičnih izhodišč človeškega zavedanja in raziskovalnemu področju informacijske varnosti ter izboljšuje praktično uporabnost za katero koli organizacijo, še posebej v kombinaciji s souporabo metod simuliranih napadov.

## LITERATURA IN VIRI


1. Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179–211.
2. Al-Amri, B., Alsuwat, H. & Alsuwat, E. (2021). Human Factor & Artificial Intelligence: For future software security to be invincible, a confronting comprehensive survey. *IJCSNS International Journal of Computer Science and Network Security, 21*(6), 245–251.
3. Alassaf, M. & Alkhalifah, A. (2021). *Exploring the Influence of Direct and Indirect Factors on Information Security Policy Compliance: A Systematic Literature Review*. Pridobljeno 12. januarja 2023 iz https://www.researchgate.net/publication/356771487_Exploring_the_Influence_of_Direct_and_Indirect_Factors_on_Information_Security_Policy_Compliance_A_Systematic_Literature_Review.
4. Alavi, R., Islam, S., Jahankhani, H. & Al-Nemrat, A. (2013). Analyzing Human Factors for an Effective Information Security Management System. *International Journal of Secure Software Engineering (IJSSE), 4*(1), 50–74.

5. Alhogail, A. & Mirza, A. (2014). A framework of information security culture change. *Journal of Theoretical and Applied Information Technology, 64*(2), 540–549.
6. Arachchilage, A. G. & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspctive. *Computers in Human Behavior, 38*(1), 304–312.
7. Ashenden, D. (2008). Information Security Management: A human challenge? *Information Security Technical Report, 13*(4), 195–201.
8. Association of Change Management Professionals – ACMP. (2019). *Standard for Change Management and ACMP Change Management Code of Ethics*. Pridobljeno 10. januarja 2023 iz https://cdn.ymaws.com/www.acmpglobal.org/resource/resmgr/files/ACMP_Standard_2019_03_21.pdf.
9. Barolli, E., Hyra, A. & Tomco, V. (2022). *Impact of the General Data Protection Regulation (GDPR) on Cyber Security*. Pridobljeno 23. decembra 2022 iz https://www.researchgate.net/publication/362302903_Impact_of_the_General_Data_Protection_Regulation_GDPR_on_Cyber_Security/citation/download.
10. Bojanc, R., Jerman-Blažič B. & Tekavčič, M. (2014). *Informacijska varnost v podjetniškem okolju*. Ljubljana: Ekonomska fakulteta.
11. Brenner, J. (2007). ISO 27001 Risk management and compliance. *Risk management, 54*(1), 1–12.
12. Calder, A. & Watkins, S. G. (2019). *Information Security Risk Management for ISO 27001/ISO 27002* (8. izd). United Kingdom: IT Governance Publishing.
13. Chignell, M. H., Chung, M. H, Yang, Y., Cento, G. & Raman, A. (2021). Human Factors in Interactive Machine Learning: A Cybersecurity Case Study. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 65*(1), 1495–1499.
14. Choi, M. S., Levy, Y. & Hovav, A. (2013). *The role of user computer self-efficacy, cybersecurity countermeasures awareness, and cybersecurity skills influence on computer misuse*. Pridobljeno 29. decembra 2022 iz https://www.researchgate.net/publication/318710121_The_Role_of_User_Computer_SelfEfficacy_Cybersecurity_Countermeasures_Awareness_and_Cybersecurity_Skills_Influence_on_Computer_Misuse.
15. Conwill, C. (2010). Human factors in information security: The insider threat – Who can you trust these days? *Information security technical report, 14*(4), 1–11.
16. Culot, G., Nassimbeni, G., Podrecca,. M. & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. *TQM Journal 33*(7), 76–105.
17. Da Veiga, A. (2016). Comparing the information security culture of employees who had read the information security policy and those who had not: Illustrated through an empirical study. *Information & Computer Security, 24*(2), 139–151.
18. Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management, *Journal of Information Security 4*(1), 92–100.

19. Duffy, B., Smith, K., Terhanian, G. & Bremer, J. (2005). Comparing data from online and face-to-face surveys. *International Journal of Market Research, 47*(6), 615–639.
20. European Commission (2021, januar). *Study to support the review of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) - No. 2020– 665*. Pridobljeno 23. decembra 2022 iz https://www.ceps.eu/wp-content/uploads/2022/07/KK0921034ENN.en_compressed.pdf.
21. European Parliament & Council of the European Union. (2016a, 19. julij). *DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*. Pridobljeno 23. decembra 2022 iz https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&rid=1.
22. European Parliament & Council of the European Union. (2016b, 4. maj*). REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. Pridobljeno 23. decembra 2022 iz https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.
23. Evans, M., He, Y., Maglaras, L., Yevseyeva, I. & Janicke, H. (2019). Evaluating information security core human error causes (IS-CHEC) technique in public sector and comparison with the private sector. *International Journal of Medical Informatics, 127*(1), 109–119.
24. Ferreira Lopes, S. F. (2021). The importance of the ITIL framework in managing Information and Communication Technology Services. *International Journal of Advanced Engineering Research and Science (IJAERS), 8*(5), 292–296.
25. Fertig, T. & Schütz, E. A. (2020). *About the Measuring of Information Security Awareness: A Systematic Literature Review*. Pridobljeno 18. januarja 2023 iz https://www.researchgate.net/publication/338630876_About_the_Measuring_of_Information_Security_Awareness_A_Systematic_Literature_Review.
26. Fujs, D., Vrhovec, S. & Vaupotič, D. (2021). Kategorizacija uporabnikov na podlagi njihovega z informacijsko varnostjo povezanega znanja, stališč in vedenja: pilotna študija. *Uporabna informatika, 29*(3), 163–169.
27. Gnanabharathy, R. (2018). Artificial Intelligence Techniques for Information Security Risk Assessment. *International Journal of Innovattive Research Technology, (5)*6, 28–31.
28. Gratian, M., Bandi, S., Cukier, M., Dykstra, J. & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computer & Security, 73*(2), 345–358.

29. Hadlington, L. & Chivers, S. (2020). Segmentation Analysis of Susceptibility to Cybercrime: Exploring Individual Differences in Information Security Awareness and Personality Factors. *Journal of Policy and Practice, 14*(2), 479–492.
30. Hadlington, L., Popovac, M., Janicke, H., Yevseyeva, I. & Jones, K (2018). Exploring the role of work identity and work locus of control in information security awareness. *Psychology and Technology, 81*, 41–48.
31. Haeussinger, F. & Kranz, J. (2013). *Understanding the antecedents of information security awareness - An empirical study*. Pridobljeno 27. decembra 2022 iz https://www.researchgate.net/publication/286845668_Understanding_the_antecedents_of_information_security_awareness_-_An_empirical_study.
32. Hair, J. F., Black, W., Babin, B. & Anderson, R. E. (2014). *Multivariate Data Analysis* (7. izd.). Harlow: Pearson.
33. Hair, J. F., Celsi, M., Money, A., Samouel, P. & Page, M. (2016). *The Essentials of Business Research Methods* (3. izd.). New York: Routledge.
34. Helmke, S. & Uebel, M. (2013). *Managementorientiertes IT-Controlling und IT Governance*. Wiesbaden: Springer Gabler.
35. Hert, P. & Papakonstantinou, V. (2016). The new General Data Protection Regulation: Still a sound system for the protection of individuals? *Computer Law & Security Review, 32*(2), 179–194.
36. Herzog, P. (2010). *Security, trust, and how we are broken*. New York: ISECOM.
37. Hinson, G. (2003). *Human factors in Information security*. New Zealand: ISECT.
38. Horikawa, H., Ohtani, H., Takahashi, Y., Kato, T., Magata, F., Teshigawara, Y., Sasaki, R. & Nishigaki, M. (2023). Enhancement of a Company-Wide Information Security Management System Through Incident Learning. *SN Computer Science, 4*(3), 211–218.
39. Hughes-Lartey, K., Li, M., Botchey, E. F. & Qin, Z. (2021). Human factor, a critical weak point in the information security of an organization's Internet of things. *Heliyon 7*(1), 1–13.
40. Information Commissioner's office – ICO (2018, 2 avgust). *Guide to the General Data Protection Regulation (GDPR)*. Pridobljeno 26. decembra 2022 iz https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf.
41. ISACA. (2012). *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*. Pridobljeno 27. decembra 2022 iz https://www.mitigasibencana.bpbd.kotabogor.go.id/uploads/edukasi/COBIT5.pdf
42. ISO 27000. (brez datuma). *An Introduction To ISO 27001 (ISO27001)*. Pridobljeno 28. decembra 2022 iz https://www.iso.org/standard/27001.
43. Jahankhani, H., Fernando, S., Nkhoma, M. Z. & Mouratidis, H. (2007). Information systems security: Cases of network administrator threats. *International Journal of Information Security and Privacy (IJISP), 1*(3), 13–25.
44. Jaiswal, M. (2019). Risk Analaysis in Information Technology. *International Journal of Scientific research and Engineering Development, 2*(6), 857–860.

45. Kane M. T. (2016). Explicating validity. A*ssessment in Education: Principles, Policy & Practice, 4*(2), 198–211.
46. Kappel, K. (2020, 25. september). *Managing the Information Security impact of COVID-19* [KPMG]. Pridobljeno 21. novembra 2022 iz https://advisory.kpmg.us/articles/2020/covid-19-cio-cyber-security-risks.html.
47. Karabacak, B. & Sogukpinar, I. (2005), ISRAM: information security risk analysis method. *Computers & Security, 24*(2), 147–159.
48. Karjalainen, M., Siponen, M. & Sarker, S. (2020). Toward a stage theory of the development of employees' information security behavior, *Computers & Security 93*, 1–18.
49. Khando, K., Gao, S., Islam, M. S. & Salman, A. (2021). Enhancing Employees Information Security Awareness in Private and Public Organisations: A Systematic Literature Review. *Computers & Security, 106*, 1–22.
50. Knekta, E., Runyon, C., Eddy, S. & Brickman, P. (2019). One Size Doesn't Fit All: Using Factor Analysis to Gather Validity Evidence When Using Surveys in Your Research. *CBE–Life Science Education, 18*(1), 1–17.
51. Kraemer, S. & Carayon, P. (2006). *An Adversarial Viewpoint of Human and Organizational Factors in Computer and Information Security: Final Report.* Madison: University of Wisconsin.
52. Kritzinger, E., da Veiga, A. & van Staden, W. (2022). Measuring organizational information security awareness in South Africa. *Information Security Journal: A Global Perspective, 32*(2), 120–133.
53. Kruger, H. A. & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Journal of Computer Security, 25*(4), 289–296.
54. Marble, J., Lawless, W. F., Mittu, R., Coyne T. J., Abramson, M. & Sibley, C. (2015). *The Human Factor in Cybersecurity: Robust & Intelligent Defense*. Pridobljeno 11. januar 2023 iz https://www.researchgate.net/publication/281993134_The_Human_Factor_in_Cybersecurity_Robust_Intelligent_Defense.
55. McCormac, A., Zwaans, T., Parsons, K., Calić, D., Butavicius, M.A. & Pattinson, M.R. (2017a). Individual differences and Information Security Awareness. *Computers in Human behavior, 69*, 151–156.
56. McCormac, A., Calić, D., Butavicius, M., Parsons, K., Zwaans, T & Pattinson, M. (2017b). A reliable measure of information security awareness and the identification of bias in responses. *Australasian Journal of Information Systems, 21*, 1–11.
57. Meissner, P. & Keding, C. (2021, 21. oktober). *The Human Factor in AI-Based Decision-Making*. Pridobljeno 11. januarja 2023 iz https://sloanreview.mit.edu/article/the-human-factor-in-ai-based-decision-making/
58. Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C. & Giannakopoulos, G. (2014). The Human Factor of Information Security: Unintentional Damage Perspective. *Social and Behavioral Sciences, 147*(1), 424–428.

59. Milfelner, B., Mumel, D. & Snoj, B. (2006). Metaanaliza dveh pristopov k raziskovanju kompleksnih marketinških problemov. *Naše gospodarstvo, 52*(5), 37–51.
60. Mittal, S. & Ilavarasan, P. V. (2019). *Demographic Factors in Cyber Security: An Empirical Study*. Pridobljeno 2. junija 2023 iz https://www.researchgate.net/publication/350183501_Demographic_Factors_in_Cyber_Security_An_Empirical_Study
61. Mittu, R. & Lawless, W. F. (2015). *Human Factors in Cybersecurity and the Role for AI. Foundations of Autonomy and Its (Cyber) Threats: From Individuals to Interdependence*. Pridobljeno 19. januarja 2023 iz https://www.aaai.org/ocs/index.php/SSS/SSS15/paper/viewFile/10248/10054
62. Moretti, M. & Markič, M. (2017). *Organizacijska kultura in organizacijska klima: Teorija, praksa in raziskave v Sloveniji*. Koper: Založba Univerze na Primorskem.
63. Morgan, S (2020, 13. november). *Cybercrime To Cost The World $10.5 Trillion Annually By 2025.* Pridobljeno 23. decembra 2022 iz https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.
64. News in France (2022). *Cybercrime cost more than $6 trillion in 2021*. Pridobljeno 21. decembra 2022 iz https://newsinfrance.com/cybercrime-cost-more-than-6-trillion-in-2021/?utm_content=cmp-true.
65. Nieles, M., Dempsey, K. & Yan Pillitteri V. (2017). *An Introduction to information Security* (1. izd.). Maryland: NIST.
66. Nunnally, J. C. (1978). *Psychometric theory* (2. izd.). New York: McGraw-Hill.
67. Pan, L. & Tomlinson, A. (2016). A systematic review of information security risk assessment. *Internationl Journal of Safety and Security Engineering, 6*(2), 270–281.
68. Parsons, K., Calić, D., Pattinson, M. & Butavicius, M. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers & Security, 66*(2), 40–51.
69. Parsons, K., McCormac, A., Butavicius, M. & Ferguson, L. (2010). *Human Factors and Information Security: Individual, Culture and Security Environment.* Pridobljeno 14. februrja 2023 iz https://apps.dtic.mil/sti/pdfs/ADA535944.pdf.
70. Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. & Jerram, C. (2014). Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security 14*(1), 165–176.
71. Parsons, K., McCormac, A., Pattinson, M. R. Butavicius M. A. & Jerram, C. (2013). *An analysis of information security vulnerabilities at three Australian government organisations*. Pridobljeno 4 junija 2023 iz https://www.researchgate.net/publication/286612263_An_analysis_of_information_security_vulnerabilities_at_three_Australian_government_organisations.
72. Pattinson, M. R. & Anderson, G. (2007). How well are information risks being communicated to your computer end-users? *Information Management & Computer Security, 15*(5), 362–371.

73. Pattinson, M., Butavicius, M., Parsons, K., McCormac, A. & Calić, D. (2015). *Factors that Influence Information Security Behavior: An Australian Web-Based Study*. Pridobljeno 4. junija 2023 iz https://digital.library.adelaide.edu.au/dspace/handle/2440/108319.
74. Pattinson, M. R., Butavicius, M. A., Parsons, K., McCormac, A., Calić, D. & Jerram, C. (2016). The Information Security Awareness of Bank Employees. *International Journal of Computing, 3*(3), 189–198.
75. Pattinson, M., Butavicius M., Lilie, M., Ciccarello B., Parsons, K., Calić, D. & McCormac, A. (2020). Matching Training to individual Learning Styles Improves Information Security Awareness. *Information and Computer Security, 28*(1), 1–14.
76. Payne, S. (2006, 26. junij). *A Guide to Security Metrics*. Pridobljeno 14 januarja 2023 iz http://www.sans.org/reading_room/whitepapers/auditing/guide-security-metrics_55.
77. Petrov, I. & Janevski, T. (2020). Artificial Intelligence Techniques for Information Security in 5G IoT Environments. *European Journal of Engineering and Technology Research, 5*(1). 1328–1333.
78. Pham Cong, H., Brennan, L. & Furnell, S. (2019). Information security burnout: Identification of sources and mitigating factors from security demands and resources. *Journal of Information Security and Applications, 46*(1), 96–107.
79. Preethi, M. B. & Parameshvar, M. (2022). Comparative Analysis of Cryptographic Hash Algorithms. *International Journal for Research in Applied Science and Engineering technology, 10*(5), 4362–4368.
80. Prelesnik, M., Burnik, J., Brulc, U., Ivanc, T., Jerše, A., Kalan Logar, E., Kotnik Šumah, K., Merce, P., Pavšič, B., Sironič, M., Strekelj, P. & Tomšič A. (2023). *Zakon o varstvu osebnih podatkov (ZVOP-2) s komentarjem*. Ljubljana: GV Založba.
81. Proctor, W. R. & Van Zandt, T. (2018). *Human Factors in Simple and Complex Systems*. United Kingdom: Taylor & Francis Group.
82. Qadir, S. & Quadri, S. M. K. (2016). Information Availability: An Insight into the Most Important Attribute of Information Security. *Journal of Information Security 7*(1), 185–194.
83. Rahman Ahlan, A., Lubis, M. & Lubis Ridho, A. (2015). Information Security Awereness at the Knowledge – Based Institution: Its Antecedents and Measures. *Procedia Copmuter Science, 72*(1), 361–373.
84. Ramluckan, T. & van Niekerk, B. (2020). *A Change Management Perspective to Implementing a Cyber Security Culture*. Pridobljeno 10. januarja 2023 iz https://www.researchgate.net/publication/342501668_A_Change_Management_Perspective_to_Implementing_a_Cyber_Security_Culture.
85. Reason, J. & Hobbs, A. (2017). *Managing maintenance error*. NW: Taylor & Francis Group.
86. Redmill, F. (2002). Human factors in risk analysis. *Engineering Management Journal, 12*(4), 171–176.

87. Rožanc, A. & Lahajnar, S. (2017). Kultura informacijske varnosti kot ključni dejavnik zagotavljanja ustrezne ravni informacijske varnosti. *Revija za ekonomske in poslovne vede, 4*(2), 92–109.
88. Ruighaver, A.B., Maynard, S. B. & Chang, S. (2007). Organisational security culture: Extending the end-user perspective. *Computers & Security, 26*(1), 56–62.
89. Samonas, S. & Coss, D. (2014). The CIA Strikes Back: Redefining Confidentiality, Integrity And Availability In Security. *Journal of Information System Security 10*(3), 21–45.
90. Shedden, P., Smith, W. & Ahmad, A. (2010). *Information Security Risk Assessment: Towards a Business Practice Perspective*. Pridobljeno 30. decembra 2022 iz https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1097&context=ism.
91. Shedden, P., Ahmad, A., Smith, W., Tscherning, H. & Scheepers, R. (2016). Asset Identification in Information Security Risk Assessment: A Business Practice Approach. *Communications of the Association for Information Systems 39*(15), 297–320.
92. Smith, P. A. (2019). Strategy Development and Implementation in a Complex Multinational IT Organisation. *Information & Security, 49*, 13–32.
93. Soltanmohammadi, S., Asadi, S. & Ithnin, N. (2013). Main human factors affecting information system security. *Interdisciplinary Journal Of Contemporary Research In Business, 5*(7), 329–354.
94. Stickman Cyber (2021, 16. februar). *ISO 27001 controls - 14 domains & how it solves business challenges*. [objava na blogu]. Pridobljeno 29. decembra 2022 iz https://www.stickmancyber.com/cybersecurity-blog/iso-27001-controls-resolve-organisational-challenges.
95. Szmit, M. & Szmit, A. (2015). Risk Management in NIST and ISO/IEC 27K Information Security Management Standards' Family - a Brief Analysis. Mechanics *Transport Communications Academic Journal, 13*(3), 14–19.
96. Taherdoost, H. (2022). Understanding Cybersecurity Frameworks and Information Security Standards–A Review and Comprehensive Overview. *Electronics 11*(14), 1–20.
97. Talabis, M. & Martin, J. (2012) *Information Security Risk Assessment Toolkit* (1. izd.). Oxford: Syngress.
98. Talimonchik, V. P. (2019). *Legal Aspects of International Information Security*. Pridobljeno 21. decembra 2022 iz https://www.researchgate.net/publication/332838686_Legal_Aspects_of_International_Information_Security.
99. Thomson, K. & van Niekerk, J. (2012). Combating information security apathy by encouraging prosocial organisational behaviour. *Information Management & Computer Security, 20*(1), 39–46.
100. Tianshui, W., Gang, Z. (2014). *A new security and privacy risk assessment model for information system considering influence relation of risk elements*. Pridobljeno 29. decembra 2022 iz https://ieeexplore.ieee.org/document/7016074.

101. Tipton, F. & Krause, M. (2008). *Information Security Management Handbook*. NW: Auerbach Publication.
102. Von Solms, R. (1999). Information security management: Why standards are important. Information. *Management & Computer Security, 7*(1), 50–58.
103. Wei, Y. C., Wu, W. C. & Chu, Y. C. (2018). Performance evaluation of the recommendation mechanism of information security risk identification. *Neurocomputing, 279*, 48–53.
104. Werlinger, R., Hawkey, K. & Beznosov, K., (2009). An integrated view of human, organizational, and technological challenges of IT security management. *Information Management & Computer Security, 17*(1), 4–19.
105. Ye, J. H. & Jensen, M. (2022). Effects of introducing an online community in a crowdsourcing contest platform. *Information System Journal, 32*(6), 1203–1230.
106. Zhen, J., Dong, K., Xie, Z. & Chen, L. (2022). Factors Influencing Employees' Information Security Awareness in the Telework Environment. *Electronics, 11*, 1–14.

# PRILOGE

**Priloga 1: Faktorske uteži pridobljene z Varimax rotacijo za dimenzijo znanje**

| Rotirana faktorska matrika[a] | | | | | | |
|---|---|---|---|---|---|---|
| | Faktor | | | | | |
| | 1 | 2 | 3 | 4 | 5 | 6 |
| *Sprejemljivo je odpreti priloge e-poštnih sporočil neznanih pošiljateljev. | 0,807 | | | | | |
| *Na službeni računalnik lahko naložim katerekoli datoteke, če mi te pomagajo opraviti moje delo. | 0,770 | | | | | |
| *Na kateremkoli spletnem mestu lahko vnesem kakršnekoli podatke, če mi ti pomagajo pri opravljanju mojega dela. | 0,664 | | | | | |
| Povezave v e-poštnih sporočilih neznanega pošiljatelja ne odpiram. | 0,569 | | | | | |
| Med službenim časom, ne bi smel dostopati do določenih spletnih mest. | 0,562 | | | | | |
| *Za službene račune je primerno, da uporabljam enaka gesla, kot jih na osebnih profilih družabnih omrežij. | | 0,817 | | | | |
| *Gesla, ki jih uporabljam na delovnem mestu, lahko delim s sodelavci. | | 0,795 | | | | |
| Uporaba različnih simbolov, številk in črk je potrebna pri izbiri službenih gesel. | | 0,764 | | | | |
| Pri opravljanju dela na javnih mestih, moram imeti računalnik ves čas pod nadzorom. | | | 0,764 | 0,404 | | |
| Če najdem nosilec spomina (USB ključ) na javnem mestu, tega ne bi smel priključiti na službeni računalnik. | | | 0,644 | | | |

se nadaljuje

**Priloga 1: Faktorske uteži pridobljene z Varimax rotacijo za dimenzijo znanje (nad.)**

| | | | | | | |
|---|---|---|---|---|---|---|
| *Sprejemljivo je, da službene datoteke z občutljivimi podatki pošiljam tudi preko javnega omrežja Wi-Fi. | 0,473 | | 0,605 | | | |
| Pri delu z občutljivimi dokumenti in podatki moram zagotoviti, da nepooblaščene osebe ne vidijo mojega računalniškega zaslona. | | | | | | |
| *Z dokumenti, ki vsebujejo občutljive podatke lahko ravnam enako, kot z dokumenti, ki ne vsebujejo občutljivih podatkov. | | | | | | |
| *O službi in delu lahko na družabnih omrežjih objavim, kar želim. | | | | 0,632 | | |
| Slabega varnostnega vedenja sodelavcev ne smem prezreti. | | | | 0,592 | | |
| *Na delovni mizi lahko izven delovnega časa in moje navzočnosti (tudi čez noč), pustim dokumente, ki vsebujejo občutljive podatke. | | | | 0,419 | | |
| *Sprejemljivo je odpreti povezave v e-poštnih sporočilih ljudi, ki jih poznam. | | | | | | |
| *Poročanje o varnostnih incidentih nadrejenim, ni obvezno. | | | | | 0,732 | |
| Če opazim, da se nekdo v mojem delovnem okolju vede sumljivo, to sporočim nadrejenim. | | | | | 0,651 | |

se nadaljuje

**Priloga 1: Faktorske uteži pridobljene z Varimax rotacijo za dimenzijo znanje (nad.)**

| | | | | | | |
|---|---|---|---|---|---|---|
| *Ne morem biti odpuščen zaradi nečesa, kar objavim na družabnih omrežjih. | | | | | | 0,702 |
| Občasno moram pregledati nastavitve zasebnosti na računih družabnih omrežij. | | | | | | 0,555 |
| Metoda ekstrakcije: Metoda glavnih osi<br>Metoda vrtenja: Varimax s Kaiserjevo normalizacijo | | | | | | |
| a. Rotacija se je izvedla v 8 ponovitvah | | | | | | |

*Vir: lastno delo.*

**Priloga 2: Faktorske uteži pridobljene z Varimax rotacijo za dimenzijo odnosa**

| Rotirana faktorska matrika[a] | | | |
|---|---|---|---|
| | Faktor | | |
| | 1 | 2 | 3 |
| *Nič slabega se ne more zgoditi, če zanemarim sumljivo varnostno vedenje sodelavca. | 0,818 | | |
| *Nič slabega se ne more zgoditi, če odprem povezavo v e-poštnem sporočilu neznanega pošiljatelja. | 0,806 | | |
| * Službeno geslo, ki vsebuje samo črke je varno. | 0,770 | | |
| *Ni pomembno katere podatke sem delil na spletnem mestu, če mi pomagajo pri opravljanju mojega dela. | 0,652 | | |
| *Ni pomembno, če na družabnih omrežjih objavljam stvari, ki jih običajno ne bi povedal/a v javnosti. | 0,611 | | |
| *Če najdem nosilec spomina (USB ključ) na javnem mestu, se ne more zgoditi nič slabega, če ga priključim na službeni računalnik. | 0,576 | 0,504 | |
| *Če se nekdo v mojem delovnem okolju vede sumljivo in to zanemarim, se ne more zgoditi nič slabega. | 0,574 | | |

se nadaljuje

**Priloga 2: Faktorske uteži pridobljene z Varimax rotacijo za dimenzijo odnosa (nad.)**

| | | | |
|---|---|---|---|
| Odpiranje e-poštnih priponk od neznanega pošiljatelja je tvegano dejanje. | 0,542 | | |
| *Povezave v e-poštnih sporočilih ljudi, ki jih poznam je varno odpirati. | | | |
| Tvegano je prezreti varnostne incidente, čeprav mislim, da niso pomembni. | | | |
| Tvegano je dostopati do občutljivih službenih datotek in podatkov na prenosnem računalniku, če nepooblaščene osebe vidijo računalniški zaslon. | | 0,806 | |
| Tvegano je pošiljati občutljive datoteke z občutljivimi podatki, preko javnega Wi-Fi omrežja. | | 0,784 | 0,407 |
| Tvegano je, da izven delovnega časa in moje navzočnosti (tudi čez noč), pustim dokumente, ki vsebujejo občutljive podatke na vidni delovni površini. | | 0,740 | |
| Poteza deljenja službenih gesel s sodelavci je slaba ideja, čeprav me včasih za to prosijo. | | 0,708 | |
| Objavljati določene informacije o mojem delu na družabnih omrežjih je tvegano dejanje. | | 0,640 | |
| *Odlaganje nerazrezanih dokumentov v koš za papir, ki vsebujejo občutljive podatke je varno dejanje. | | 0,517 | |
| To, da lahko v službi dostopam do določenega spletnega mesta, še ne pomeni, da je to tudi varno. | | 0,484 | 0,470 |
| *Pri opravljanju dela na javnih mestih (kavarna, restavracija, knjižnica) je varno pustiti prenosni računalnik brez nadzora, čeprav samo za trenutek. | | 0,426 | |
| Prenos datotek na službeni računalnik je lahko tvegano. | | | 0,735 |

se nadaljuje

**Priloga 2: Faktorske uteži pridobljene z Varimax rotacijo za dimenzijo odnosa (nad.)**

| | | | |
|---|---|---|---|
| *Varno je uporabljati enaka gesla na družabnih omrežjih in službenih računih. | | | 0,701 |
| Priporočljivo je, da redno pregledujem nastavitve zasebnosti na družabnih omrežjih. | | 0,494 | 0,557 |
| Metoda ekstrakcije: Metoda glavnih osi<br>Metoda vrtenja: Varimax s Kaiserjevo normalizacijo | | | |
| a. Rotacija se je izvedla v 8 ponovitvah | | | |

*Vir: lastno delo.*

**Priloga 3*:* Faktorske uteži pridobljene z Varimax rotacijo za dimenzijo vedenja**

| Rotirana faktorska matrika[a] | | | |
|---|---|---|---|
| | Faktor | | |
| | 1 | 2 | 3 |
| *Med službenim časom z dostopom do spleta, obiščem vsa spletna mesta, ki jih želim. | 0,870 | | |
| *Na službeni računalnik naložim vse datoteke, ki mi omogočajo lažje opravljanje mojega dela. | 0,853 | | |
| *Če je povezava v e-poštnem sporočilu neznanega pošiljatelja videti zanimiva, to povezavo odprem. | 0,800 | | |
| *Datoteke z občutljivimi podatki, pošiljam tudi preko javnega Wi-Fi omrežja. | 0,767 | | 0,415 |
| V službenih geslih uporabljam kombinacijo številk, simbolov in črk (malih in velikih). | 0,759 | | |
| Če mi je pošiljatelj nepoznan, ne odpiram prilog v e-poštnem sporočilu. | 0,723 | | 0,455 |
| *S sodelavci delim svoja službena gesla. | 0,505 | | |

se nadaljuje

**Priloga 3*:* Faktorske uteži pridobljene z Varimax rotacijo za dimenzijo vedenja (nad.)**

| | | | |
|---|---|---|---|
| *Med delom na javnem mestu (kavarna, restavracija, knjižnica), včasih pustim prenosni računalnik brez nadzora. | 0,470 | | 0,458 |
| *Kadar nisem na delovnem mestu, včasih pustim na vidni delovni površini dokumente z občutljivimi podatki. | 0,462 | | 0,449 |
| *Če bi opazil/a, da sodelavec/ka ignorira varnostna pravila in politike, glede tega ne bi storil/a ničesar. | | 0,762 | |
| Če bi videl/a, da se v delovnem okolju nekdo vede sumljivo, bi o tem opozoril nadrejenega. | | 0,642 | |
| Ko je potrebno uničiti dokumente, ki vsebujejo občutljive podatke vedno poskrbim, da jih uničim s pomočjo rezalnika papirja (šreder). | | 0,631 | |
| V službeni računalnik ne bi priključeval nosilca spomina (USB ključ), ki ga najdem na javnem mestu. | | 0,600 | |
| Za družabna omrežja in službene račune uporabljam različna gesla. | 0,435 | 0,587 | |
| *Nastavitev zasebnosti na družabnih omrežjih ne pregledujem redno. | 0,468 | 0,498 | |
| Povezav v e-poštnih sporočilih ne odpiram vedno samo zato, ker prihajajo od poznanih oseb. | | | |
| Na družabnih omrežjih ne objavim ničesar, dokler ne premislim morebitnih negativnih posledic. | | | 0,725 |
| *O delu na družabnih omrežjih objavim, karkoli želim. | | | 0,718 |
| Ko delam z dokumenti, ki vsebujejo občutljive podatke, preverim da nepooblaščene osebe ne vidijo računalniškega zaslona. | 0,508 | | 0,628 |

se nadaljuje

**Priloga 3*:* Faktorske uteži pridobljene z Varimax rotacijo za dimenzijo vedenja (nad.)**

| | | | |
|---|---|---|---|
| Pred vnosom podatkov ocenim varnost spletnega mesta. | | | 0,489 |
| Če bi opazil/a varnostni incident, bi to nemudoma prijavil/a nadrejenemu. | | 0,429 | 0,455 |
| Metoda ekstrakcije: Metoda glavnih osi<br>Metoda vrtenja: Varimax s Kaiserjevo normalizacijo | | | |
| a. Rotacija se je izvedla v 7 ponovitvah | | | |

*Vir: lastno delo.*

**Priloga 4: Tabela komunalitet faktorskih analiz po KAB dimenzijah**

| KOMUNALITETE ZA DIMEZIJO ZNANJE | | | KOMUNALITETE ZA DIMENZIJO ODNOS | | | KOMUNALITETE ZA DIMENZIJO VEDENJE | | |
|---|---|---|---|---|---|---|---|---|
| | Začetne | Ekstrahirane | | Začetne | Ekstrahirane | | Začetne | Ekstrahirane |
| *Za službene račune je primerno, da uporabljam enaka gesla, kot jih na osebnih profilih družabnih omrežij. | 0,790 | 0,743 | *Varno je uporabljati enaka gesla na družabnih omrežjih in službenih računih. | 0,707 | 0,627 | Za družabna omrežja in službene račune uporabljam različna gesla. | 0,735 | 0,544 |
| *Gesla, ki jih uporabljam na delovnem mestu, lahko delim s sodelavci. | 0,837 | 0,757 | Poteza deljenja službenih gesel s sodelavci je slaba ideja, čeprav me včasih za to prosijo. | 0,645 | 0,518 | *S sodelavci delim svoja službena gesla. | 0,635 | 0,423 |
| Uporaba različnih simbolov, številk in črk je potrebna pri izbiri službenih gesel. | 0,693 | 0,793 | *Službeno geslo, ki vsebuje samo črke je varno. | 0,806 | 0,673 | V službenih geslih uporabljam kombinacijo številk, simbolov in črk (malih in velikih). | 0,795 | 0,736 |
| *Sprejemljivo je odpreti povezave v e-poštnih sporočilih ljudi, ki jih poznam. | 0,211 | 0,173 | *Povezave v e-poštnih sporočilih ljudi, ki jih poznam je varno odpirati. | 0,438 | 0,035 | Povezav v e-poštnih sporočilih ne odpiram vedno samo zato, ker prihajajo od poznanih oseb. | 0,464 | 0,095 |

se nadaljuje

**Priloga 4: Tabela komunalitet faktorskih analiz po KAB dimenzijah (nad.)**

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Povezave v e-poštnih sporočilih neznanega pošiljatelja ne odpiram. | 0,419 | 0,341 | *Nič slabega se ne more zgoditi, če odprem povezavo v e-poštnem sporočilu neznanega pošiljatelja. | 0,804 | 0,659 | *Če je povezava v e-poštnem sporočilu neznanega pošiljatelja videti zanimiva, to povezavo odprem. | 0,904 | 0,773 |
| *Sprejemljivo je odpreti priloge e-poštnih sporočil neznanih pošiljateljev. | 0,733 | 0,738 | Odpiranje e-poštnih priponk od neznanega pošiljatelja je tvegano dejanje. | 0,731 | 0,355 | Če mi je pošiljatelj nepoznan, ne odpiram prilog v e-poštnem sporočilu. | 0,922 | 0,787 |
| *Na službeni računalnik lahko naložim katerekoli datoteke, če mi te pomagajo opraviti moje delo. | 0,832 | 0,820 | Prenos datotek na službeni računalnik je lahko tvegano. | 0,820 | 0,631 | *Na službeni računalnik naložim vse datoteke, ki mi omogočajo lažje opravljanje mojega dela. | 0,875 | 0,814 |
| Med službenim časom, ne bi smel dostopati do določenih spletnih mest. | 0,710 | 0,486 | To, da lahko v službi dostopam do določenega spletnega mesta, še ne pomeni, da je to tudi varno. | 0,720 | 0,455 | *Med službenim časom z dostopom do spleta, obiščem vsa spletna mesta, ki jih želim. | 0,952 | 0,931 |

se nadaljuje

**Priloga 4: Tabela komunalitet faktorskih analiz po KAB dimenzijah (nad.)**

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| *Na kateremkoli spletnem mestu lahko vnesem kakršnekoli podatke, če mi ti pomagajo pri opravljanju mojega dela. | 0,628 | 0,622 | *Ni pomembno katere podatke sem delil na spletnem mestu, če mi pomagajo pri opravljanju mojega dela. | 0,682 | 0,513 | Pred vnosom podatkov ocenim varnost spletnega mesta. | 0,474 | 0,258 |
| Občasno moram pregledati nastavitve zasebnosti na računih družabnih omrežij. | 0,619 | 0,593 | Priporočljivo je, da redno pregledujem nastavitve zasebnosti na družabnih omrežjih. | 0,705 | 0,574 | *Nastavitev zasebnosti na družabnih omrežjih ne pregledujem redno. | 0,683 | 0,505 |
| *Ne morem biti odpuščen zaradi nečesa, kar objavim na družabnih omrežjih. | 0,593 | 0,613 | *Ni pomembno, če na družabnih omrežjih objavljam stvari, ki jih običajno ne bi povedal/a v javnosti. | 0,742 | 0,425 | Na družabnih omrežjih ne objavim ničesar, dokler ne premislim morebitnih negativnih posledic. | 0,797 | 0,736 |
| *O službi in delu lahko na družabnih omrežjih objavim, kar želim. | 0,605 | 0,609 | Objavljati določene informacije o mojem delu na družabnih omrežjih je tvegano dejanje. | 0,637 | 0,423 | *O delu na družabnih omrežjih objavim, karkoli želim. | 0,621 | 0,569 |

se nadaljuje

**Priloga 4: Tabela komunalitet faktorskih analiz po KAB dimenzijah (nad.)**

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Pri opravljanju dela na javnih mestih, moram imeti računalnik ves čas pod nadzorom. | 0,681 | 0,795 | *Pri opravljanju dela na javnih mestih (kavarna, restavracija, knjižnica) je varno pustiti prenosni računalnik brez nadzora, čeprav samo za trenutek. | 0,636 | 0,290 | *Med delom na javnem mestu (kavarna, restavracija, knjižnica), včasih pustim prenosni računalnik brez nadzora. | 0,774 | 0,515 |
| *Sprejemljivo je, da službene datoteke z občutljivimi podatki pošiljam tudi preko javnega omrežja Wi-Fi. | 0,706 | 0,696 | Tvegano je pošiljati občutljive datoteke z občutljivimi podatki, preko javnega Wi-Fi omrežja. | 0,870 | 0,792 | *Datoteke z občutljivimi podatki, pošiljam tudi preko javnega Wi-Fi omrežja. | 0,931 | 0,877 |
| Pri delu z občutljivimi dokumenti in podatki moram zagotoviti, da nepooblaščene osebe ne vidijo mojega računalniškega zaslona. | 0,454 | 0,245 | Tvegano je dostopati do občutljivih službenih datotek in podatkov na prenosnem računalniku, če nepooblaščene osebe vidijo računalniški zaslon. | 0,789 | 0,722 | Ko delam z dokumenti, ki vsebujejo občutljive podatke, preverim da nepooblaščene osebe ne vidijo računalniškega zaslona. | 0,807 | 0,757 |

se nadaljuje

**Priloga 4: Tabela komunalitet faktorskih analiz po KAB dimenzijah (nad.)**

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| *Z dokumenti, ki vsebujejo občutljive podatke lahko ravnam enako, kot z dokumenti, ki ne vsebujejo občutljivih podatkov. | 0,435 | 0,116 | *Odlaganje nerazrezanih dokumentov v koš za papir, ki vsebujejo občutljive podatke je varno dejanje. | 0,702 | 0,387 | Ko je potrebno uničiti dokumente, ki vsebujejo občutljive podatke vedno poskrbim, da jih uničim s pomočjo rezalnika papirja (šreder). | 0,789 | 0,618 |
| Če najdem nosilec spomina (USB ključ) na javnem mestu, tega ne bi smel priključiti na službeni računalnik. | 0,713 | 0,665 | *Čenajdem nosilec spomina (USB ključ) na javnem mestu, se ne more zgoditi nič slabega, če ga priključim na službeni računalnik. | 0,739 | 0,611 | V službeni računalnik ne bi priključeval nosilca spomina (USB ključ), ki ga najdem na javnem mestu. | 0,747 | 0,500 |
| *Na delovni mizi lahko izven delovnega časa in moje navzočnosti (tudi čez noč), pustim dokumente, ki vsebujejo občutljive podatke. | 0,440 | 0,228 | Tvegano je, da izven delovnega časa in moje navzočnosti (tudi čez noč), pustim dokumente, ki vsebujejo občutljive podatke na vidni delovni površini. | 0,757 | 0,659 | *Kadar nisem na delovnem mestu, včasih pustim na vidni delovni površini dokumente z občutljivimi podatki. | 0,740 | 0,503 |

se nadaljuje

**Priloga 4: Tabela komunalitet faktorskih analiz po KAB dimenzijah (nad.)**

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Če opazim, da se nekdo v mojem delovnem okolju vede sumljivo, to sporočim nadrejenim. | 0,758 | 0,728 | *Če se nekdo v mojem delovnem okolju vede sumljivo in to zanemarim, se ne more zgoditi nič slabega. | 0,770 | 0,384 | Če bi videl/a, da se v delovnem okolju nekdo vede sumljivo, bi o tem opozoril nadrejenega. | 0,634 | 0,556 |
| Slabega varnostnega vedenja sodelavcev ne smem prezreti. | 0,728 | 0,660 | *Nič slabega se ne more zgoditi, če zanemarim sumljivo varnostno vedenje sodelavca. | 0,886 | 0,673 | *Če bi opazil/a, da sodelavec/ka ignorira varnostna pravila in politike, glede tega ne bi storil/a ničesar. | 0,727 | 0,704 |
| *Poročanje o varnostnih incidentih nadrejenim, ni obvezno. | 0,590 | 0,628 | Tvegano je prezreti varnostne incidente, čeprav mislim, da niso pomembni. | 0,424 | 0,026 | Če bi opazil/a varnostni incident, bi to nemudoma prijavil/a nadrejenemu. | 0,551 | 0,418 |
| Metoda ekstrakcije: Metoda glavnih osi | | | | | | | | |

*Vir: lastno delo.*

**Priloga 5: instrument merjenja človeških vidikov na informacijsko varnost – HAIS-Q**

| **Ciljna področja** | **Podpodročje** | **Znanje**<br>**HAIS-Q od V1 do V21** | **Odnos**<br>**HAIS-Q od V22 do V42** | **Vedenje**<br>**HAIS-Q od V43 do V63** |
|---|---|---|---|---|
| Upravljanje gesel | Uporaba istega gesla | Za službene račune je primerno, da uporabljam enaka gesla, kot jih na osebnih profilih družabnih omrežij. * | Varno je uporabljati enaka gesla na družabnih omrežjih in službenih računih. * | Za družabna omrežja in službene račune uporabljam različna gesla. |
| | Skupna raba gesel | Gesla, ki jih uporabljam na delovnem mestu, lahko delim s sodelavci. * | Poteza deljenja službenih gesel s sodelavci je slaba ideja, čeprav me včasih za to prosijo. | S sodelavci delim svoja službena gesla. * |
| | Izbira primernega gesla | Uporaba različnih simbolov, številk in črk je potrebna pri izbiri službenih gesel. | Službeno geslo, ki vsebuje samo črke je varno. * | V službenih geslih uporabljam kombinacijo številk, simbolov in črk (malih in velikih). |
| Uporaba elektronske pošte | Odpiranje povezav v e-poštnih sporočilih neznanega pošiljatelja | Sprejemljivo je odpreti povezave v e-poštnih sporočilih ljudi, ki jih poznam. * | Povezave v e-poštnih sporočilih ljudi, ki jih poznam je varno odpirati. * | Povezav v e-poštnih sporočilih ne odpiram vedno samo zato, ker prihaja od poznane osebe. |
| | Odpiranje povezav v e-poštnih sporočil neznanih pošiljateljev | Povezave v e-poštnih sporočilih neznanega pošiljatelja ne odpiram. | Nič slabega se ne more zgoditi, če odprem povezavo v e-poštnem sporočilu neznanega pošiljatelja. * | Če je povezava v e-poštnem sporočilu neznanega pošiljatelja videti zanimiva, to povezavo odprem. * |
| | Odpiranje priponk v e-poštnih sporočilih neznanih pošiljateljev. | Sprejemljivo je odpreti priloge e-poštnih sporočil neznanih pošiljateljev. * | Odpiranje e-poštnih priponk od neznanega pošiljatelja je tvegano dejanje. | Če mi je pošiljatelj nepoznan, ne odpiram prilog v e-poštnem sporočilu. |

se nadaljuje

**Priloga 5: instrument merjenja človeških vidikov na informacijsko varnost – HAIS-Q (nad.)**

| | | | | |
|---|---|---|---|---|
| Uporaba interneta | Prenos datotek | Na službeni računalnik lahko naložim katerekoli datoteke, če mi te pomagajo opraviti moje delo. * | Prenos datotek na službeni računalnik je lahko tvegano. | Na službeni računalnik naložim vse datoteke, ki mi omogočajo lažje opravljanje mojega dela. * |
| | Dostop do spletnih mest | Med službenim časom, ne bi smel dostopati do določenih spletnih mest. | To, da lahko v službi dostopam do določenega spletnega mesta, še ne pomeni, da je to tudi varno. | Med službenim časom z dostopom do spleta, obiščem vsa spletna mesta, ki jih želim. * |
| | Vnos podatkov na spletna mesta | Na kateremkoli spletnem mestu lahko vnesem kakršnekoli podatke, če mi to pomaga pri opravljanju mojega dela. * | Ni pomembno katere podatke sem delil na spletnem mestu, če mi to poma pri opravljanju mojega dela.* | Pred vnosom podatkov ocenim varnost spletnega mesta. |
| Uporaba družabnih omrežij | Nastavitev zasebnosti družabnih omrežij | Občasno moram pregledati nastavitve zasebnosti na računih družabnih omrežij. | Priporočljivo je, da redno pregledujem nastavitve zasebnosti na družabnih omrežjih. | Nastavitev zasebnosti na družabnih omrežjih ne pregledujem redno. * |
| | Upoštevanje teže posledic | Ne morem biti odpuščen zaradi nečesa, kar objavim na družabnih omrežjih. * | Ni pomembno, če na družabnih omrežjih objavljam stvari, ki jih običajno ne bi povedal/a v javnosti. * | Na družabnih omrežjih ne objavim ničesar, dokler ne premislim morebitnih negativnih posledic. |
| | Objavljanje informacij o delu na družabnih omrežjih | O službi in delu lahko na družabnih omrežjih objavim, kar želim. * | Objavljati določene informacije o mojem delu na družabnih omrežjih je tvegano dejanje. | O delu na družabnih omrežjih objavim, karkoli želim. * |
| Mobilne naprave – delo na daljavo | Fizično varovanje osebnih elektronskih naprav | Pri opravljanju dela na javnih mestih, moram imeti računalnik ves čas pod nadzorom. | Pri opravljanju dela na javnih mestih (kavarna, restavracija, knjižnica) je varno pustiti prenosni računalnik brez nadzora, čeprav samo za trenutek. * | Med delom na javnem mestu (kavarna, restavracija, knjižnica), včasih pustim prenosni računalnik brez nadzora. * |

se nadaljuje

**Priloga 5: instrument merjenja človeških vidikov na informacijsko varnost – HAIS-Q (nad.)**

| | | | | |
|---|---|---|---|---|
| | Pošiljanje občutljivih informacij preko Wi-Fi omrežja. | Sprejemljivo je, da službene datoteke z občutljivimi podatki pošiljam tudi preko javnega omrežja Wi-Fi. * | Tvegano je pošiljati občutljive datoteke z občutljivimi podatki, preko javnega Wi-Fi omrežja. | Datoteke z občutljivimi podatki, pošiljam tudi preko javnega Wi-Fi omrežja. * |
| | Nadzor nad obdelavo podatkov na javnih mestih | Pri delu z občutljivimi dokumenti in podatki moram zagotoviti, da nepooblaščene osebe ne vidijo mojega računalniškega zaslona. | Tvegano je dostopati do občutljivih službenih datotek in podatkov na prenosnem računalniku, če nepooblaščene osebe vidijo računalniški zaslon. | Ko delam z dokumenti, ki vsebujejo občutljive podatke, preverim da nepooblaščene osebe ne vidijo računalniškega zaslona. |
| Ravnanje z informacijami | Obdelava občutljivih podatkov | Z dokumenti, ki vsebujejo občutljive podatke lahko ravnam enako, kot z dokumenti, ki ne vsebujejo občutljivih podatkov. * | Odlaganje nerazrezanih dokumentov v koš za papir, ki vsebujejo občutljive podatke je varno dejanje. * | Ko je potrebno uničiti dokumente, ki vsebujejo občutljive podatke vedno poskrbim, da jih uničim s pomočjo rezalnika papirja (šreder). |
| | Vstavljanje prenosnih medijev (npr. USB ključ) | Če najdem nosilec spomina (USB ključ) na javnem mestu, tega ne bi smel priključiti na službeni računalnik | Če najdem nosilec spomina (USB ključ) na javnem mestu, se ne more zgoditi nič slabega, če ga priključim na službeni računalnik. * | V službeni računalnik ne bi priključeval nosilca spomina (USB ključ), ki ga najdem na javnem mestu. |
| | Obdelava občutljivih informacij | Na delovni mizi lahko izven delovnega časa in moje navzočnosti (tudi čez noč), pustim dokumente, ki vsebujejo občutljive podatke. * | Tvegano je, da izven delovnega časa in moje navzočnosti (tudi čez noč), pustim dokumente, ki vsebujejo občutljive podatke na vidni delovni površini. | Kadar nisem na delovnem mestu, včasih pustim na vidni delovni površini dokumente z občutljivimi podatki. * |

se nadaljuje

**Priloga 5: instrument merjenja človeških vidikov na informacijsko varnost – HAIS-Q (nad.)**

| | | | | |
|---|---|---|---|---|
| Poročanje o incidentih | Poročanje o sumljivem vedenju | Če opazim, da se nekdo v mojem delovnem okolju vede sumljivo, to sporočim nadrejenim. | Če se nekdo v mojem delovnem okolju vede sumljivo in to zanemarim, se ne more zgoditi nič slabega. * | Če bi videl/a, da se v delovnem okolju nekdo vede sumljivo, bi o tem opozoril nadrejenega. |
| | Prezrtje slabega vedenja sodelavcev | Slabega varnostnega vedenja sodelavcev ne smem prezreti. | Nič slabega se ne more zgoditi, če zanemarim sumljivo varnostno vedenje sodelavca. * | Če bi opazil/a, da sodelavec/ka ignorira varnostna pravila in politike, glede tega ne bi storil/a ničesar. * |
| | Poročanje o vseh varnostnih incidentih | Poročanje o varnostnih incidentih nadrejenim, ni obvezno. * | Tvegano je prezreti varnostne incidente, čeprav mislim, da niso pomembni. | Če bi opazil/a varnostni incident, bi to nemudoma prijavil/a nadrejenemu. |
| Anketiranci na vsako trditev odgovorijo na 5 stopenjski Likertovi lestvici od “Sploh se ne strinjam” do “Popolnoma se strinjam”;<br>Za trditev se uporablja obratno točkovanje * | | | | |

*Prirejeno po Parsons in drugi (2017).*

**Priloga 6: Celotna pojasnitev variance za dimenzijo znanje**

| CELOTNA POJASNITEV VARIANCE – ZNANJE | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Faktorji | Začetna lastna vrednost | | | Začetna vsota kvadratov | | | Rotirana vsota kvadratov | | |
| | Skupaj | % variance | Komulativa % | Skupaj | % variance | Komulativa % | Skupaj | % variance | Komulativa % |
| 1 | 6,566 | 31,268 | 31,268 | 6,235 | 29,691 | 29,691 | 3,055 | 14,547 | 14,547 |
| 2 | 2,372 | 11,295 | 42,563 | 2,029 | 9,663 | 39,354 | 2,420 | 11,525 | 26,072 |
| 3 | 1,609 | 7,660 | 50,223 | 1,197 | 5,699 | 45,054 | 2,023 | 9,636 | 35,708 |
| 4 | 1,521 | 7,241 | 57,464 | 1,100 | 5,240 | 50,294 | 1,715 | 8,166 | 43,874 |
| 5 | 1,366 | 6,506 | 63,970 | 0,910 | 4,331 | 54,625 | 1,593 | 7,584 | 51,458 |
| 6 | 1,059 | 5,041 | 69,011 | 0,577 | 2,748 | 57,373 | 1,242 | 5,915 | 57,373 |
| 7 | 0,944 | 4,497 | 73,508 | | | | | | |
| 8 | 0,872 | 4,153 | 77,661 | | | | | | |
| 9 | 0,797 | 3,794 | 81,455 | | | | | | |
| 10 | 0,672 | 3,199 | 84,654 | | | | | | |
| 11 | 0,598 | 2,846 | 87,500 | | | | | | |
| 12 | 0,531 | 2,528 | 90,028 | | | | | | |
| 13 | 0,431 | 2,050 | 92,079 | | | | | | |
| 14 | 0,362 | 1,725 | 93,804 | | | | | | |
| 15 | 0,323 | 1,538 | 95,341 | | | | | | |
| 16 | 0,274 | 1,306 | 96,647 | | | | | | |
| 17 | 0,193 | 0,917 | 97,565 | | | | | | |
| 18 | 0,176 | 0,839 | 98,403 | | | | | | |
| 19 | 0,163 | 0,777 | 99,180 | | | | | | |
| 20 | 0,109 | 0,520 | 99,700 | | | | | | |
| 21 | 0,063 | 0,300 | 100,000 | | | | | | |
| Metoda ekstrakcije: Metoda glavnih osi | | | | | | | | | |

*Vir: lastno delo.*

**Priloga 7: Celotna pojasnitev variance za dimenzijo odnosa**

| CELOTNA POJASNITEV VARIANCE – ODNOS | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Faktorji | Začetna lastna vrednost | | | Začetna vsota kvadratov | | | Rotirana vsota kvadratov | | |
| | Skupaj | % variance | Komulativa % | Skupaj | % variance | Komulativa % | Skupaj | % variance | Komulativa % |
| 1 | 7,041 | 33,528 | 33,528 | 6,606 | 31,455 | 31,455 | 4,164 | 19,827 | 19,827 |
| 2 | 3,107 | 14,796 | 48,324 | 2,694 | 12,830 | 44,285 | 4,129 | 19,661 | 39,488 |
| 3 | 1,546 | 7,364 | 55,688 | 1,133 | 5,395 | 49,681 | 2,140 | 10,193 | 49,681 |
| 4 | 1,275 | 6,071 | 61,759 | | | | | | |
| 5 | 1,056 | 5,026 | 66,786 | | | | | | |
| 6 | 1,000 | 4,763 | 71,548 | | | | | | |
| 7 | 0,929 | 4,425 | 75,974 | | | | | | |
| 8 | 0,828 | 3,941 | 79,914 | | | | | | |
| 9 | 0,794 | 3,781 | 83,695 | | | | | | |
| 10 | 0,703 | 3,349 | 87,044 | | | | | | |
| 11 | 0,514 | 2,446 | 89,489 | | | | | | |
| 12 | 0,460 | 2,191 | 91,681 | | | | | | |
| 13 | 0,427 | 2,035 | 93,716 | | | | | | |
| 14 | 0,291 | 1,385 | 95,101 | | | | | | |
| 15 | 0,262 | 1,247 | 96,348 | | | | | | |
| 16 | 0,208 | 0,989 | 97,337 | | | | | | |
| 17 | 0,184 | 0,875 | 98,211 | | | | | | |
| 18 | 0,156 | 0,744 | 98,956 | | | | | | |
| 19 | 0,095 | 0,454 | 99,410 | | | | | | |
| 20 | 0,081 | 0,383 | 99,793 | | | | | | |
| 21 | 0,043 | 0,207 | 100,000 | | | | | | |
| Metoda ekstrakcije: Metoda glavnih osi | | | | | | | | | |

*Vir: lastno delo.*

**Priloga 8: Celotna pojasnitev variance za dimenzijo vedenja**

| CELOTNA POJASNITEV VARIANCE - VEDENJE | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Faktorji | Začetna lastna vrednost | | | Začetna vsota kvadratov | | | Rotirana vsota kvadratov | | |
| | Skupaj | % variance | Komulativa % | Skupaj | %variance | Komulativa % | Skupaj | % variance | Komulativa % |
| 1 | 10,640 | 50,665 | 50,665 | 10,315 | 49,120 | 49,120 | 5,646 | 26,887 | 26,887 |
| 2 | 1,625 | 7,738 | 58,403 | 1,280 | 6,096 | 55,216 | 3,536 | 16,838 | 43,725 |
| 3 | 1,497 | 7,128 | 65,531 | 1,024 | 4,878 | 60,094 | 3,437 | 16,369 | 60,094 |
| 4 | 1,101 | 5,243 | 70,774 | | | | | | |
| 5 | 0,938 | 4,465 | 75,239 | | | | | | |
| 6 | 0,831 | 3,957 | 79,196 | | | | | | |
| 7 | 0,684 | 3,257 | 82,454 | | | | | | |
| 8 | 0,665 | 3,167 | 85,620 | | | | | | |
| 9 | 0,537 | 2,558 | 88,178 | | | | | | |
| 10 | 0,465 | 2,216 | 90,394 | | | | | | |
| 11 | 0,384 | 1,828 | 92,222 | | | | | | |
| 12 | 0,311 | 1,483 | 93,705 | | | | | | |
| 13 | 0,290 | 1,380 | 95,085 | | | | | | |
| 14 | 0,271 | 1,293 | 96,378 | | | | | | |
| 15 | 0,220 | 1,046 | 97,424 | | | | | | |
| 16 | 0,175 | 0,835 | 98,259 | | | | | | |
| 17 | 0,120 | 0,573 | 98,832 | | | | | | |
| 18 | 0,105 | 0,501 | 99,333 | | | | | | |
| 19 | 0,063 | 0,301 | 99,633 | | | | | | |
| 20 | 0,046 | 0,221 | 99,855 | | | | | | |
| 21 | 0,031 | 0,145 | 100,000 | | | | | | |
| Metoda ekstrakcije: Metoda glavnih osi | | | | | | | | | |

*Vir: lastno delo.*

**Priloga 9: Rezultati Cronbach alfe za notranjo konsistentnost HAIS-Q instrumenta po ciljnih področjih**

| Statistika zanesljivosti podpodročji HAIS-Q vprašalnika | | |
|---|---|---|
| Ciljno področje | Cronbach alfa (α) | Število indikatorjev |
| Upravljanje z gesli | 0,894 | 9 |
| Uporaba elektronske pošte | 0,803 | 9 |
| Uporaba interneta | 0,874 | 9 |
| Uporaba družabnih omrežji | 0,788 | 9 |
| Mobilne naprave – delo na daljavo | 0,797 | 9 |
| Ravnanje z informacijami | 0,744 | 9 |
| Poročanje o incidentih | 0,811 | 9 |

*Vir: lastno delo.*

**Priloga 10: Rezultati Cronbach alfe za notranjo konsistentnost dobljenih faktorjev s faktorsko analizo za dimenzijo znanja**

| Statistika zanesljivosti faktorjev za dimenzijo znanje | | |
|---|---|---|
| Faktor | Cronbach alfa (α) | Število indikatorjev |
| F1 – Znanje o odpiranju prilog e-poštnih sporočil, prenosu datotek ter vnašanje podatkov | 0,820 | 5 |
| F2 – Znanje z upravljanjem gesel | 0,854 | 3 |
| F3 – Znanje pri delu na daljavo | 0,868 | 3 |
| F4 – znanje o varovanju službenih informacij | 0,820 | 3 |
| F5 – znanje o varnostnih incidentih | 0,820 | 2 |
| F6 – znanje o zasebnosti | 0,785 | 2 |

*Vir: lastno delo.*

**Priloga 11: Rezultati Cronbach alfe za notranjo konsistentnost dobljenih faktorjev s faktorsko analizo za dimenzijo odnosa**

| Statistika zanesljivosti faktorjev za dimenzijo odnos | | |
|---|---|---|
| Faktor | Cronbach alfa (α) | Število indikatorjev |
| F1 – Odnos do varne obdelave podatkov in informacij, ki prihajajo od drugih oseb | 0,874 | 8 |
| F2 – Odnos do obdelave občutljivih podatkov in informacij | 0,793 | 8 |
| F3 – Odnos do zasebnosti in varovanje službenih informacijskih sredstev | 0,818 | 3 |

*Vir: lastno delo.*

**Priloga 12: Rezultati Cronbach alfe za notranjo konsistentnost dobljenih faktorjev s faktorsko analizo za dimenzijo vedenja**

| Statistika zanesljivosti faktorjev za dimenzijo vedenje | | |
|---|---|---|
| Faktor | Cronbach alfa (α) | Število indikatorjev |
| F1 – Vedenje do izbire primernega gesla ter dostopanje in varovanje občutljivih podatkov in informacij | 0,947 | 9 |
| F2 – Vedenje do varnstnih incidentov ter zaščita občutljivih podatkov pred nepooblaščenim dostopom | 0,860 | 6 |
| F3 – Vedenje do obdelave in objave občutljivih podatkov ter informacij | 0,821 | 5 |

*Vir: lastno delo.*

**Priloga 13: Analiza variance odvisne spremenljivke odnos**

| Model | | Vsota kvadratov | Stopinje prostosti | Ocena Variance | F–preizkus | Statistična značilnost (p) |
|---|---|---|---|---|---|---|
| 1 | Regresija | 6,091 | 1 | 6,091 | 285,505 | .000[b] |
| | Ostanek | 2,197 | 103 | 0,021 | | |
| | Skupaj | 8,288 | 104 | | | |
| a Odvisna spremenljivka: Odnos | | | | | | |
| b (Konstanta), Znanje | | | | | | |

*Vir: lastno delo.*

**Priloga 14: Ocene koeficientov regresijske funkcije**

| Model | | Nestandardiziran koeficient | | Standardiziran koeficient | t | Statistična značilnost (p) |
|---|---|---|---|---|---|---|
| | | B | Standardna napaka | Beta | | |
| 1 | Konstanta | 0,752 | 0,196 | | 3,843 | 0,000 |
| | Znanje | 0,823 | 0,049 | 0,857 | 16,897 | 0,000 |
| a Odvisna spremenljivka: Odnos | | | | | | |

*Vir: lastno delo.*

**Priloga 15: Analiza variance odvisne spremenljivke vedenja**

| Model | | Vsota kvadratov | Stopinje prostosti | Ocena variance | F–preizkus | Statistična značilnost (p) |
|---|---|---|---|---|---|---|
| 1 | Regresija | 10,558 | 2 | 5,279 | 95,305 | .000[b] |

se nadaljuje

**Priloga 15: Analiza variance odvisne spremenljivke vedenje (nad.)**

| | | | | | | |
|---|---|---|---|---|---|---|
| | Ostanek | 5,650 | 102 | 0,055 | | |
| | Skupaj | 16,208 | 104 | | | |
| a Odvisna spremenljivka: Vedenje | | | | | | |
| b (Konstanta): Odnos, Znanje | | | | | | |

*Vir: lastno delo.*

**Priloga 16: Ocene koeficientov regresijske funkcije**

| Model | | Nestandardiziran koeficient | | Standardiziran koeficient | t | Statistična značilnost (p) |
|---|---|---|---|---|---|---|
| | | B | Standardna napaka | Beta | | |
| 1 | (Konstanta) | -0,636 | 0,337 | | -1,887 | 0,062 |
| | Znanje | 0,691 | 0,152 | 0,515 | 4,532 | 0,000 |
| | Odnos | 0,449 | 0,159 | 0,321 | 2,829 | 0,006 |
| Odvisna spremenljivka: Vedenje | | | | | | |

*Vir: lastno delo.*

**Priloga 17: Oblikovanje spremenljivk za regresijski analizi**

Dimenzija znanje

| | | N | % |
|---|---|---|---|
| Primeri | Veljavnih | 105 | 100,0 |
| | Izključenih[a] | 0 | 0,0 |
| | Skupaj | 105 | 100,0 |
| a. Brisanje po seznamu glede na vse spremenljivke v postopku | | | |

| **Statistika zanesljivosti** | |
|---|---|
| Cronbach alfa (α) | Število indikatorjev |
| 0,744 | 6 |

Dimenzija odnos

| | | N | % |
|---|---|---|---|
| Primeri | Veljavnih | 105 | 100,0 |
| | Izključenih[a] | 0 | 0,0 |
| | Skupaj | 105 | 100,0 |
| a. Brisanje po seznamu glede na vse spremenljivke v postopku. | | | |

| **Statistika zanesljivosti** | |
|---|---|
| Cronbach alfa (α) | Število indikatorjev |
| 0,840 | 3 |

Dimenzija vedenje

| | | N | % |
|---|---|---|---|
| Primeri | Veljavnih | 105 | 100,0 |
| | Izključenih[a] | 0 | 0,0 |
| | Skupaj | 105 | 100,0 |
| a. Brisanje po seznamu glede na vse spremenljivke v postopku | | | |

| **Statistika zanesljivosti** | |
|---|---|
| Cronbach alfa (α) | Število indikatorjev |
| 0,712 | 3 |

*Vir: lastno delo.*

## Priloga 18: Ocena ISA za dimenzijo znanja

| **OCENA ISA ZA ZNANJE** | | |
|---|---|---|
| številka indikatorja iz HAIS-Q | Vprašanja o znanju | Ocena zavedanje informacijske varnosti - ISA v % |
| HAIS-Q: V1 | Za službene račune je primerno, da uporabljam enaka gesla, kot jih na osebnih profilih družabnih omrežij. | 96,2 |
| HAIS-Q: V2 | Gesla, ki jih uporabljam na delovnem mestu, lahko delim s sodelavci. | 95,2 |
| HAIS-Q: V3 | Uporaba različnih simbolov, številk in črk je potrebna pri izbiri službenih gesel. | 94,4 |
| HAIS-Q: V4 | Sprejemljivo je odpreti povezave v e-poštnih sporočilih ljudi, ki jih poznam. | 25,7 |
| HAIS-Q: V5 | Povezave v e-poštnih sporočilih neznanega pošiljatelja ne odpiram. | 70,5 |
| HAIS-Q: V6 | Sprejemljivo je odpreti priloge e-poštnih sporočil neznanega pošiljatelja. | 79,0 |
| HAIS-Q: V7 | Na službeni računalnik lahko naložim katerekoli datoteke, če mi te pomagajo opraviti moje delo. | 81,9 |
| HAIS-Q: V8 | Med službenim časom, ne bi smel dostopati do določenih spletnih mest. | 93,3 |
| HAIS-Q: V9 | Na kateremkoli spletnem mestu lahko vnesem kakršnekoli podatke, če mi ti pomagajo pri opravljanju mojega dela. | 83,8 |
| HAIS-Q: V10 | Občasno moram pregledati nastavitve zasebnosti na računih družabnih omrežij. | 96,2 |
| HAIS-Q: V11 | Ne morem biti odpuščen zaradi nečesa, kar objavim na družabnih omrežjih. | 78,1 |
| HAIS-Q: V12 | O službi in delu lahko na družabnih omrežjih objavim, kar želim. | 91,4 |

se nadaljuje

**Priloga 18: Ocena ISA za dimenzijo znanja (nad.)**

| | | |
|---|---|---|
| HAIS-Q: V13 | Pri opravljanju dela na javnih mestih, moram imeti računalnik ves čas pod nadzorom. | 99,0 |
| HAIS-Q: V14 | Sprejemljivo je, da službene datoteke z občutljivimi podatki pošiljam tudi preko javnega omrežja Wi-Fi. | 93,3 |
| HAIS-Q: V15 | Pri delu z občutljivimi dokumenti in podatki moram zagotoviti, da nepooblaščene osebe ne vidijo mojega računalniškega zaslona. | 96,2 |
| HAIS-Q: V16 | Z dokumenti, ki vsebujejo občutljive podatke lahko ravnam enako, kot z dokumenti, ki ne vsebujejo občutljivih podatkov. | 91,4 |
| HAIS-Q: V17 | Če najdem nosilec spomina (USB ključ) na javnem mestu, tega ne bi smel priključiti na službeni računalnik. | 96,2 |
| HAIS-Q: V18 | Na delovni mizi lahko izven delovnega časa in moje navzočnosti (tudi čez noč), pustim dokumente, ki vsebujejo občutljive podatke. | 94,3 |
| HAIS-Q: V19 | Če opazim, da se nekdo v mojem delovnem okolju vede sumljivo, to sporočim nadrejenim. | 97,1 |
| HAIS-Q: V20 | Slabega varnostnega vedenja sodelavcev ne smem prezreti. | 97,1 |
| HAIS-Q: V21 | Poročanje o varnostnih incidentih nadrejenim, ni obvezno. | 93,3 |
| | **OCENA ISA SPLOŠNO STANJE ZA ZNANJE** | **87,8** |

*Vir: lastno delo.*

**Priloga 19: Ocena ISA za dimenzijo odnosa**

| **OCENA ISA ZA ODNOS** | | |
|---|---|---|
| številka indikatorja | Vprašanja o odnosu | Ocena zavedanja informacijske varnosti - ISA v % |
| HAIS-Q: V22 | Varno je uporabljati enaka gesla na družabnih omrežjih in službenih računih. | 93,3 |
| HAIS-Q: V23 | Poteza deljenja službenih gesel s sodelavci je slaba ideja, čeprav me včasih za to prosijo. | 99,0 |
| HAIS-Q: V24 | Službeno geslo, ki vsebuje samo črke je varno. | 86,7 |
| HAIS-Q: V25 | Povezave v e-poštnih sporočilih ljudi, ki jih poznam je varno odpirati. | 25,7 |
| HAIS-Q: V26 | Nič slabega se ne more zgoditi, če odprem povezavo v e-poštnem sporočilu neznanega pošiljatelja. | 85,7 |
| HAIS-Q: V27 | Odpiranje e-poštnih priponk od neznanega pošiljatelja je tvegano dejanje. | 92,4 |
| HAIS-Q: V28 | Prenos datotek na službeni računalnik je lahko tvegano. | 96,2 |

se nadaljuje

**Priloga 19: Ocena ISA za dimenzijo odnosa (nad.)**

| | | |
|---|---|---|
| HAIS-Q: V29 | To, da lahko v službi dostopam do določenega spletnega mesta, še ne pomeni, da je to tudi varno. | 98,1 |
| HAIS-Q: V30 | Ni pomembno katere podatke sem delil na spletnem mestu, če mi pomaga pri opravljanju mojega dela. | 89,5 |
| HAIS-Q: V31 | Priporočljivo je, da redno pregledujem nastavitve zasebnosti na družabnih omrežjih. | 96,2 |
| HAIS-Q: V32 | Ni pomembno, če na družabnih omrežjih objavljam stvari, ki jih običajno ne bi povedal/a v javnosti. | 88,6 |
| HAIS-Q: V33 | Objavljati določene informacije o mojem delu na družabnih omrežjih je tvegano dejanje. | 98,1 |
| HAIS-Q: V34 | Pri opravljanju dela na javnih mestih (kavarna, restavracija, knjižnica) je varno pustiti prenosni računalnik brez nadzora, čeprav samo za trenutek. | 95,2 |
| HAIS-Q: V35 | Tvegano je pošiljati občutljive datoteke z občutljivimi podatki, preko javnega Wi-Fi omrežja. | 97,1 |
| HAIS-Q: V36 | Tvegano je dostopati do občutljivih službenih datotek in podatkov na prenosnem računalniku, če nepooblaščene osebe vidijo računalniški zaslon. | 100,0 |
| HAIS-Q: V37 | Odlaganje nerazrezanih dokumentov v koš za papir, ki vsebujejo občutljive podatke je varno dejanje. | 96,2 |
| HAIS-Q: V38 | Če najdem nosilec spomina (USB ključ) na javnem mestu, se ne more zgoditi nič slabega, če ga priključim na službeni računalnik. | 93,3 |
| HAIS-Q: V39 | Tvegano je, da izven delovnega časa in moje navzočnosti (tudi čez noč), pustim dokumente, ki vsebujejo občutljive podatke na vidni delovni površini. | 100,0 |
| HAIS-Q: V40 | Če se nekdo v mojem delovnem okolju vede sumljivo in to zanemarim, se ne more zgoditi nič slabega. | 88,6 |
| HAIS-Q: V41 | Nič slabega se ne more zgoditi, če zanemarim sumljivo varnostno vedenje sodelavca. | 87,6 |
| HAIS-Q: V42 | Tvegano je prezreti varnostne incidente, čeprav mislim, da niso pomembni. | 92,4 |
| | **OCENA ISA SPLOŠNO STANJE ZA ODNOS** | **90,5** |

*Vir: lastno delo.*

**Priloga 20: Ocena ISA za dimenzijo vedenja**

| **OCENA ISA ZA VEDENJE** | | |
|---|---|---|
| številka indikatorja | Vprašanja o vedenju | Ocena zavedanje informacijske varnosti - ISA v % |

se nadaljuje

**Priloga 20: Ocena ISA za dimenzijo vedenja (nad.)**

| | | |
|---|---|---|
| HAIS-Q: V43 | Za družabna omrežja in službene račune uporabljam različna gesla. | 91,4 |
| HAIS-Q: V44 | S sodelavci delim svoja službena gesla. | 91,4 |
| HAIS-Q: V45 | V službenih geslih uporabljam kombinacijo številk, simbolov in črk (malih in velikih). | 85,7 |
| HAIS-Q: V46 | Povezav v e-poštnih sporočilih ne odpiram vedno samo zato, ker prihaja od poznane osebe. | 61,9 |
| HAIS-Q: V47 | Če je povezava v e-poštnem sporočilu neznanega pošiljatelja videti zanimiva, to povezavo odprem. | 81,0 |
| HAIS-Q: V48 | Če mi je pošiljatelj nepoznan, ne odpiram prilog v e-poštnem sporočilu. | 80,0 |
| HAIS-Q: V49 | Na službeni računalnik naložim vse datoteke, ki mi omogočajo lažje opravljanje mojega dela. | 81,9 |
| HAIS-Q: V50 | Med službenim časom z dostopom do spleta, obiščem vsa spletna mesta, ki jih želim. | 81,00 |
| HAIS-Q: V51 | Pred vnosom podatkov ocenim varnost spletnega mesta. | 94,3 |
| HAIS-Q: V52 | Nastavitev zasebnosti na družabnih omrežjih ne pregledujem redno. | 85,7 |
| HAIS-Q: V53 | Na družabnih omrežjih ne objavim ničesar, dokler ne premislim morebitnih negativnih posledic. | 91,4 |
| HAIS-Q: V54 | O delu na družabnih omrežjih objavim, karkoli želim. | 92,4 |
| HAIS-Q: V55 | Med delom na javnem mestu (kavarna, restavracija, knjižnica), včasih pustim prenosni računalnik brez nadzora. | 88,6 |
| HAIS-Q: V56 | Datoteke z občutljivimi podatki, pošiljam tudi preko javnega Wi-Fi omrežja. | 83,8 |
| HAIS-Q: V57 | Ko delam z dokumenti, ki vsebujejo občutljive podatke, preverim da nepooblaščene osebe ne vidijo računalniškega zaslona. | 85,7 |
| HAIS-Q: V58 | Ko je potrebno uničiti dokumente, ki vsebujejo občutljive podatke vedno poskrbim, da jih uničim s pomočjo rezalnika papirja (šreder). | 94,3 |
| HAIS-Q: V59 | V službeni računalnik ne bi priključeval nosilca spomina (USB ključ), ki ga najdem na javnem mestu. | 91,4 |
| HAIS-Q: V60 | Kadar nisem na delovnem mestu, včasih pustim na vidni delovni površini dokumente z občutljivimi podatki. | 83,8 |
| HAIS-Q: V61 | Če bi videl/a, da se v delovnem okolju nekdo vede sumljivo, bi o tem opozoril nadrejenega. | 95,2 |
| HAIS-Q: V62 | Če bi opazil/a, da sodelavec/ka ignorira varnostna pravila in politike, glede tega ne bi storil/a ničesar. | 92,4 |
| HAIS-Q: V63 | Če bi opazil/a varnostni incident, bi to nemudoma prijavil/a nadrejenemu. | 93,3 |
| | **OCENA ISA SPLOŠNO STANJE ZA VEDENJE** | **87,0** |

*Vir: lastno delo.*