ELEKTROTEHNIŠKI VESTNIK 88(4): 174–182, 2021
IZVIRNI ZNANSTVENI ČANEK

Zaznavanje tveganj pri sprejemanju tehnoloških vsadkov

Lara Klemenc[1], **Simon Vrhovec**[1], **Anže Mihelič**[1,*]

[1] *Univerza v Mariboru, Fakulteta za varnostne vede*
Kotnikova ul. 8, 1000 Ljubljana, Slovenija

[*] *E-naslov: anze.mihelic@um.si*

Povzetek. Potrošniki tehnoloških novosti ne sprejmejo vedno dobro, prav oni pa odločajo, ali bodo izdelek uporabljali ali bo šel v pozabo. V prispevku predstavljamo uporabo tehnoloških vsadkov, ki jih delimo na dve vrsti: (1) raba tehnoloških vsadkov za zdravstvene namene, (2) raba za namene olajševanja vsakdanjega življenja. Da bi odgovorili na vprašanje, kateri dejavniki napovedujejo sprejemanje vstavljivih tehnologij, smo razvili raziskovalni model, ki temelji na modelu sprejemanja tehnologije in obenem vsebuje tudi varnostne vidike. Za testiranje modela smo uporabili spletni vprašalnik ($N = 243$). Stališča do tehnoloških vsadkov najbolje napovedujeta enostavnost uporabe in zaznana uporabnost, v manjšem obsegu pa tudi zaznana varnost podatkov in subjektivna norma. Skrb glede nadzora nad uporabniki in glede zasebnosti statistično značilno ne napoveduje stališč do tehnoloških vsadkov. Namero uporabe tehnoloških vsadkov statistično značilno napovedujejo stališča do tehnoloških vsadkov.

Ključne besede: vstavljive naprave, tehnološki vsadki, dejavniki tveganja, model sprejemanja tehnologij, TAM

Risk perception in adopting technological implants

Technological novelties are not always well adopted by consumers. They decide whether to use a product or consign it to oblivion. The paper addresses adoption of two types of technological implants in turns of their intended use, i.e., either for or to facilitate the human's everyday life. To answer the question which factors predict adoption of implantable technologies, a research model is developed based on a technology acceptance model with a due consideration of security aspects. An online survey ($n = 243$) is conducted to test the model showing that implantable technologies are most affected by the ease of their use and perceived usefulness and less by the perceived data security and subjective norm. Surveillance and privacy concerns do not significantly affect the attitude towards implantable technologies adoption. The behavioral intention is statistically significantly predicted by attitude towards implantable technologies.

Keywords: insideable devices, insideables, technological implants, risk factors, technology acceptance model, TAM

1 UVOD

Vstavljive naprave (angl. *insideable devices*, *insideables*) oz. tehnološki vsadki (angl. *technological implants*) so elektronske naprave, ki so vgrajene v človekovo telo [1]. Razdelimo jih lahko na naprave, ki odpravljajo telesne okvare ali zdravstvene težave (terapevtski vsadki), in tiste, ki povečujejo prirojene človeške sposobnosti, kot so duševna okretnost, spomin in fizična moč [2]. Poleg omenjenega lahko omogočijo nove sposobnosti, kot je daljinsko upravljanje strojev [1]. V svetu se vstavljiva tehnologija že razvija, tehnološki razvoj pa spodbuja k razmisleku o uporabi vstavljivih naprav. Gre za potencialno zelo invazivno tehnologijo, kljub temu pa je ljudem mamljiva, saj lahko z njeno pomočjo izboljšajo svoje čute ali celo možgansko moč [3]. Za premagovanje človeških telesnih okvar je tehnologija dobro sprejeta [1]. Naprave se povezujejo z internetom, zato lahko postanejo tarče kibernetskih napadov, ti pa lahko pomenijo precejšnje tveganje [4]. Smo ljudje res pripravljeni posegati v svoje telo in ga s tem modificirati?

Raziskave so pokazale, da je pomemben dejavnik pri sprejemanju novih tehnologij naše stališče do te tehnologije [5], [6], [7]. Ljudje v splošnem vstavljive naprave podpirajo [8], predvsem za zdravstvene namene [9]. V veliko raziskavah o vstavljivih napravah je izpostavljeno vprašanje, ali je uporaba vstavljivih naprav etična [8], [1], [10]. Med vsemi raziskavami so le v eni izpostavljena tveganja, ki jih vstavljiva tehnologija prinaša [8]. Vstavljivim napravam, ki odpravljajo zdravstvene težave [9], so ljudje etično veliko bolj naklonjeni, kot napravam, ki bi uporabnikom omogočale udobje [8].

Ker lahko tehnološki vsadki prinašajo različna varnostna tveganja [4], se v pričujočem prispevku osredotočamo predvsem na tiste napovedne dejavnike sprejemanja tehnoloških vsadkov, ki so povezani z varnostjo. Čeprav so pri sprejemanju novih tehnologij tovrstni dejavniki izjemnega pomena, tega v literaturi ni mogoče zaslediti,

Prejet 25. april 2021
Odobren 20. julij, 2021

razen v primeru tehnoloških vsadkov za medicinsko uporabo [11].

2 TEHNOLOŠKI VSADKI

Z vsakim dnem se kaže trend oziroma želja po izboljšanju našega telesa s sodobno tehnologijo. Za potrebe medicine so milijoni ljudi po svetu opremljeni s protetičnimi napravami, ki pomagajo obnoviti izgubljene telesne funkcije [12]. Narašča tudi gibanje, usmerjeno v samoizboljšanje telesa, ustvarjanje novih čutov ali izboljšanje trenutnih čutov, ki presegajo običajno raven naših zmogljivosti [12]. Poznamo protetične okončine, umetne srčne spodbujevalnike, defibrilatorje, vsadke, ki ustvarjajo vmesnike med možgani in računalnikom, ušesne vsadke, proteze mrežnice (proteze oči), magnete kot vsadke in številne druge izboljšave. Tako postaja človeško telo bolj mehansko in računalniško, a z vsako tehnologijo tudi manj biološko. Ta trend se bo še naprej krepil, saj se bo telo preoblikovalo v tehnologijo za obdelavo informacij, ki bo ne nazadnje izzvala čut za identiteto, torej, kaj sploh pomeni biti človek [12].

2.1 Tehnološki vsadki za medicinsko uporabo

Uporaba tehnoloških vsadkov za reševanje življenj ni etično sporna, saj so vsadki dobro sprejeti, in sicer tudi tiste oblike najbolj invazivnih tehnologij, kot sta izboljšanje vida in sluha ter uravnavanje srčnega ritma [1]. Tehnološki vsadki za medicinske namene spremljajo in zdravijo fiziološke razmere v telesu. Te naprave, vključno s srčnimi spodbujevalniki, vsadljivimi srčnimi defibrilatorji, sistemi za distribucijo zdravil in nevrostimulatorji, lahko pomagajo obvladovati širok spekter bolezni, kot so srčna aritmija, sladkorna bolezen in Parkinsonova bolezen [11]. Z internetom stvari (angl. *internet of things* – IoT) se spremlja paciente in zdravstvene storitve, ki so jih deležni [13].

Na podlagi nosljivih medicinskih pripomočkov, ki spremljajo mobilnost bolnikov po bolj zapletenih posegih [14], so se razvili tudi tehnološki vsadki za samonadzor na osnovi informacijske tehnologije za obvladovanje kroničnih bolezni. So zaznavne naprave, ki jih pacientom lahko vstavijo v telo, ter tako lažje spremljajo njihove vitalne znake [9]. Za spremljanje na daleč pa je potrebna povezava z internetom, kar omogoča, da se težave lahko hitro identificirajo [11]. S tem bi se lahko reaktivna oskrba pacientov spremenila v preventivno [15].

2.2 Tehnološki vsadki za olajševanje vsakdanjega življenja

Tehnološki vsadki za olajševanje vsakdanjega življenja so v resnici že del naših življenj, saj uporabljamo pripomočke za boljši sluh, srčne spodbujevalnike, umetne okončine in druge vgradljive naprave [16]. Številni jih vidijo kot naravno razširitev sodobne inovacije – nosljive tehnologije (angl. *wearable technology*, *wearables*), ki omogoča spremljanje zdravja in kondicije posameznikov. Nekateri posamezniki že uporabljajo tehnologijo čipov RFID, kot so vstopni ključi stanovanj, brezstične plačilne kartice, kartice za javni prevoz, zdravstvene kartice (krvna skupina, alergije, drugi zdravstveni podatki), osebne izkaznice (kartice z osebnimi podatki) in drugi čipi, ki vsebujejo občutljive podatke (gesla, osebne informacije ...) [16].

Uporabnike privlači tudi navidezna resničnost, ki bi zadovoljila njihove potrebe [17]. Po mnenju nevroznanstvenikov bi se napredek v prihodnosti lahko odražal s kupovanjem popolnoma novih in tujih spominov, ki bi si jih lahko posamezniki vgradili v možgane. Predvidevajo tudi, da bi lahko bilo celotno življenje zaživeto v trenutku. S tehnološkimi vsadki bi bilo mogoče ustvarjanje novih čutil. Obstaja tudi možnost, da bomo lahko informacije v možgane vsadili neposredno, urejali spomine in se brezžično povezali med možgani (povezava misel – misel) ter tako izkusili širok spekter senzoričnih informacij [12].

Tako bi lahko spremenili svoje spomine in ostal bi nam občutek zavedanja, ločen od spominov, ki izhaja iz interakcije s svetom [12]. Znanstveniki z instituta Massachusetts Institute of Technology (MIT) so pred nekaj leti v možgane miši vsadili lažne spomine in dokazali, da so nevrološke sledi teh spominov po naravi enake kot pravi oz. verodostojni spomini. Če je uspelo spremeniti mišje spomine, lahko predvidevamo, da nismo daleč od dneva, ko bo človeški spomin mogoče spremeniti ali izboljšati s tehnološkimi vsadki [16]. Na robu sprememb je tudi naš um oz. naši možgani. Možganski vsadki, ki obnavljajo poškodovane spomine, lahko nekoč privedejo do ustvarjanja novih spominov ali telepatske komunikacije. Če lahko prilagodimo svoja telesa in spomine, lahko spremenimo tudi svoje čute in način življenja. Bistveno človeško zavedanje se bo spremenilo, morda celo do točke nerazpoznavnosti. Vprašali bi se lahko, kaj sploh reči o človeški naravi, če je bilo vse, kar imamo za resnično, predmet spremembe ali celo (kibernetskega) napada [12].

2.3 Pomisleki o varnosti in zasebnosti

Pametne naprave se hitro razvijajo, uporablja pa jih vedno več ljudi [18]. Prav tako narašča raba interneta, zato se je razvilo drugo področje uporabe, imenovano internet stvari [19]. Omogoča medsebojno komunikacijo, računanje in usklajevanje neposredno med stroji in predmeti. Varnost in zasebnost sta dve od ključnih vprašanj, povezanih s široko uporabo interneta stvari [15]. Naprave med seboj komunicirajo s podatki, ki so bili zbrani iz različnih naprav, ki dovoljujejo internetno povezavo. Ponudnikom nudijo priročne in pametne storitve, hkrati pa vnašajo potencialne pomisleke glede zasebnosti. Zasebne informacije lahko uhajajo v katerikoli fazi življenjskega cikla podatkov v okoljih interneta stvari [20].

Življenjski cikel podatkov predstavlja celoten podatkovni proces v sistemu. Obsega ustvarjanje, shranjevanje, uporabnost skupne rabe ter arhiviranje in uničenje v sistemu in aplikacijah [21]. Poleg posameznih podatkov, kot so prstni odtisi in srčni utrip, ki so neposredno povezani s posameznikovo zasebnostjo, se lahko nekatere okoljske informacije, ki jih zaznavajo naprave, uporabijo za pridobivanje dodatnih informacij, npr. o uporabnikovih željah in gibanju. Združeni podatki različnih naprav lahko prispevajo k vseobsežnemu nadzoru našega življenja [22]. Uporabnik je lahko hkrati prejemnik podatkov ali storitev in predmet zbiranja podatkov s pametnimi stvarmi. V primerjavi z internetom, kjer morajo uporabniki prevzeti aktivno vlogo, da ogrozijo svojo zasebnost [23], [24], se veliko podatkov o uporabnikih zbira in prenaša v računalniške oblake brez njihove ozaveščenosti. Velik obseg podatkov se generira samodejno in z večjo hitrostjo kot kadarkoli prej, vse kršitve varnosti pa vplivajo na osebno varnost in zasebnost posameznika [25]. Zaradi povezanosti z internetom uporabnikom teh naprav grozijo kibernetski napadi ter zasebnostne in druge varnostne grožnje [18], [26], [27].

Varnost je pomemben dejavnik zaupanja. Ker je zaupanje subjektivno in je varnost objektivna, lahko varnost razumemo kot predhodnico namere pri uporabnikih [28]. Vpliv varnosti na stališča do novih tehnologij je močnejši pri tistih, ki niso imeli preteklih izkušenj z njimi [28]. Poleg varnosti je pomembno tudi zaupanje, kar še zlasti vpliva na vedenjske namere posameznika [28]. Na človekovo negativno sprejetje tehnologije vplivajo pomisleki glede zasebnosti [16], vendar le takrat, ko je občutljivost informacij velika [29]).

Če se ljudje zaradi prilagojenih informacij čutijo izkoriščene, se počutijo tudi ranljive, kar sproži posameznikove pomisleke glede zasebnosti [30]. Ljudje s splošnim dojemanjem tveganj zasebnosti tudi na spletnih mestih in v spletnem okolju poskrbijo za svojo zasebnost [31], želeli pa bi imeti večji nadzor nad osebnimi podatki, ki jih uporabljajo na spletu [32]. Uporabniki na spletu ne razkrivajo več toliko osebnih podatkov [33] ali pa jih delno zakrijejo oziroma uporabijo izmišljene podatke [32], [34]. Čeprav vemo, da smo nadzorovani, nas ta nadzor ne skrbi, saj gre za javno oz. družbeno korist [35]. Na splošno pa je dokazano, da so ženske bolj dovzetne za spletne napade kot moški [36].

Uporaba vstavljivih elektronskih naprav pomeni nastajajoče tvegano vedenje s potencialnimi negativnimi posledicami za zdravje in varnost, čeprav naj bi prinašale koristi. Tveganja postajajo večja v nekonvencionalnih okoljih, kjer se samoimplementacije izvajajo brez ocene tveganja in preventivnih ukrepov strokovnjakov [4]. Čeprav so po namenu uporabe vsadki podobni nosljivi tehnologiji, je pri njih stopnja tveganja za uporabnike večja in zaradi tega je tudi njihova zaskrbljenost glede zasebnosti večja, kar otežuje sprejemanje tehnoloških vsadkov [16]. Uravnoteženje zasebnosti z varnostjo in učinkovitostjo bo z razvojem tehnologij postajala vse bolj pomembna [11].

Implantacija sproža tudi pomisleke glede varnosti. Vstavitev čipa je invaziven postopek, ki lahko privede do trajnih sprememb telesa ne glede na to, ali se izvaja v profesionalni ali domači oskrbi. Težko je oceniti zdravstvena tveganja, povezana s tehnološkimi vsadki. Rana se lahko okuži, okužba pa je velikokrat odvisna od tega, za katere vrste vsadek gre (srčne zaklopke, vaskularni presadki, srčni spodbujevalniki, sklepne proteze ...). Odziv telesa je odvisen tudi od [4]: lastnosti pacienta (debelost, diabetes), lastnosti vsadka (material vsadka, biološka kompatibilnost), lastnosti operacije (dobro steriliziran pribor, ki onemogoča kontaminacijo).

Poleg zdravstvenih zapletov so tehnološki vsadki dovzetni za kibernetske napade. Ti so lahko prav tako škodljivi kot tisti v materialnem svetu, čeprav jih je v kibernetskem prostoru včasih težko zaznati kot take [37]. Veliko naprav povezavo zahteva ali jo dovoljuje. Povezljivost lahko ogrozi fizično in psihološko varnost, saj so naprave različne ranljivosti (npr. srčni spodbujevalniki so lahka tarča napadalcev) [4]. Ti napadi pa so, še zlasti v primeru tehnoloških vsadkov za medicinsko uporabo, za posameznika veliko hujši in bolj neposredni v primerjavi z napadi na drugo tehnologijo [15]. Ne nazadnje je zasebnost lahko ogrožena pri vseh ljudeh, ne samo pri tistih, ki imajo vgrajene tehnološke vsadke. Povezani vsadki se včasih uporabljajo za spremljanje in shranjevanje zdravstvenega stanja ali telesnih funkcij (spremljanje sladkorja v krvi, razpoloženja ...), pa tudi človekove dejavnosti (geografska lokacija in podatki o vsakodnevnem življenju). Osebne, zaupne in občutljive informacije so lahko v nevarnosti, da jih tretje osebe ukradejo in uporabijo v zle namene (npr. protetična kamera za oči, ki lahko beleži dejavnosti tretjih oseb). Snemanje ljudi brez vednosti in dovoljenja ter nadaljnje upravljanje podatkov pomeni tveganje za zasebnost in sproža etična vprašanja [4]. Od vseh podatkov so najbolj občutljivi ravno podatki o zdravstvenem stanju posameznika [38].

Tehnološki vsadki so povezani tudi z osebno varnostjo. Ljudje, ki bi sami imeli vsadke, svojim otrokom tega večinoma ne bi priporočili, razen za medicinske namene [2]. Kot že omenjeno, so od vseh podatkov najbolj občutljivi ravno podatki o zdravstvenem stanju posameznika [38]. Napadi, ki jih ogrožajo, pa so za posameznika veliko hujši in bolj neposredni v primerjavi z napadi na drugo tehnologijo [15]. Ugotovljeno je bilo, da potrošniki zelo veliko uporabljajo različne aplikacije, od katerih pa nimajo vedno le koristi, ampak tudi tvegajo razkritje svojih osebnih podatkov. Ljudje aplikacije uporabljajo množično, saj njihova uporaba prinese veliko več koristi, kot je zaznanih tveganj [39]. Uporabniki se zavedajo različnih tveganj, kot so njihova zasebnost na spletu, transakcije in nevarnost kraje osebnih podatkov [40].

Zaradi precejšnjih koristi pa so uporabniki velikokrat

pripravljeni deliti svoje osebne podatke na spletu ali v drugih aplikacijah [41], saj z izmenjavo osebnih podatkov prejmejo hitrejše in bolj prilagojene storitve [42]. Napadalci pogosto uporabijo osebno komunikacijo, ki je zelo podobna vsakdanji (uporaba čustvenih simbolov), da se tako približajo žrtvi in lažje od nje pridobijo podatke [43]. Uporabniki so motivirani in nova tehnologija jih spodbuja k telesni aktivnosti, vendar obenem te podatke delijo v medmrežju in tekmujejo z vrstniki [44]. Ravno zato se z varnostjo in zaščito zasebnosti spodbuja ljudi k sprejemanju novejših tehnologij [45].

3 Razvoj raziskovalnega modela

Da bi poiskali odgovor na raziskovalno vprašanje, smo oblikovali raziskovalni model, ki se osredotoča na pomembne dejavnike sprejemanja tehnologij in varnostne dejavnike. Izvirni model sprejemanja tehnologij, od katerega smo obdržali zaznano uporabnost, enostavnost uporabe, subjektivno normo in namero za uporabo, smo uporabili kot temelj našega raziskovalnega modela. Model smo dopolnili z dejavniki, ki odražajo različna tveganja, povezana s tehnološkimi vsadki.

Prvi sklop hipotez se osredotoča na varnost tehnologije in uporabnika. Zaupanje v tehnologijo se izrazi kot prepričanje, da uporabniki lahko postanejo ranljivi, to pa vpliva tudi na uporabnikovo mnenje o varnosti tehnologije [46]. Zaupanje v varnost tehnologije je pomembna za rabo te tehnologije v prihodnosti [47]. Na tem mestu je treba poudariti tudi zaskrbljenost glede nadzora nad zasebnostjo posameznika oz. ozaveščenost o takem nadzoru in njegovo občutljivost za informacije, ki zelo pomembno vpliva na sprejemljivost nadzora pri ljudeh [35], [48], [49]. Skrbi glede zasebnosti pomembno vplivajo na uporabnikovo motivacijo za samozaščito, saj meni, da če se zaščitijo drugi, mora za to obstajati resna grožnja [50], [51]. Na osnovi tega izpeljemo naslednje hipoteze.

H1a: Zaznana varnost podatkov je pozitivno povezana s stališčem do tehnoloških vsadkov.

H1b: Skrb glede nadzora je negativno povezana s stališčem do tehnoloških vsadkov.

H1c: Skrb glede zasebnosti je negativno povezana s stališčem do tehnoloških vsadkov.

Splošno stališče potencialnega uporabnika do določenega sistema vpliva na njegovo namero uporabe tega sistema [5]. Zaznana uporabnost je pomemben dejavnik pri sprejemanju informacijskih sistemov. Do te stopnje človek verjame, da uporaba določenega sistema poveča koristnost njihovega dela. Tudi enostavnost uporabe je pomemben dejavnik, ki vpliva na sprejemanje informacijskega sistema, saj oseba verjame, da bo uporaba sistema brez napora. Tako bo tehnologija, ki je lažja za uporabo, veliko bolje sprejeta med njenimi uporabniki [52], [53]. Dokazana je tudi povezanost med uporabnostjo in enostavnostjo uporabe, saj enostavnost uporabe vpliva na zaznano uporabnost [6]. V praksi je ljudem pomembneje, da je tehnologijo lažje uporabljati, kot njena koristnost [54]. Pomembno vlogo igra tudi subjektivna norma, ki se nanaša na zaznani družbeni pritisk, ki vpliva na posameznikovo vedenje [55]. Obstoječe raziskave močno podpirajo obstoj povezave med uporabnostjo, enostavnostjo uporabe in subjektivno normo ter namero uporabe nove tehnologije [56]. Na osnovi tega izpeljemo naslednje hipoteze.

H2a: Enostavnost uporabe je pozitivno povezana s stališčem do tehnoloških vsadkov.

H2b: Subjektivna norma je pozitivno povezana s stališčem do tehnoloških vsadkov.

H2c: Zaznana uporabnost je pozitivno povezana s stališčem do tehnoloških vsadkov.

Človeška stališča do uporabe tehnologij temeljijo na naših prepričanjih. Ta izhajajo iz našega znanja [6]. Zato lažje proučujemo stališče do uporabe in namero uporabe kot dejansko uporabo naprav, saj tiste vstavljive naprave, ki so v uporabi, večinoma niso povezane v medmrežje [60]. Na osnovi tega izpeljemo naslednjo hipotezo.

H3: Stališče do tehnoloških vsadkov je pozitivno povezano z namero uporabe.

4 Metoda

Vprašalnik je temeljil na indikatorjih, preverjenih v že opravljenih raziskavah, ki so tematsko ustrezale področju sprejemanja novih tehnologij. Indikatorje smo najprej prilagodili v angleškem jeziku, nato pa prevedli v slovenščino. Prevod iz angleščine v slovenščino sta opravila dva neodvisna prevajalca. Da bi preverili ohranitev pomena prevedenih indikatorjev, je bil opravljen tudi povratni prevod v angleščino. Tabela 1 prikazuje akronim, ime konstrukta, definicijo konstrukta in vir indikatorjev.

Vprašalnik je vseboval osem sklopov vprašanj, po enega za vsak konstrukt iz raziskovalnega modela. Vsak sklop je vseboval po tri indikatorje. Pri konstruktih namera uporabe in enostavnost uporabe smo uporabili sedemstopenjsko Likertovo lestvico, pri čemer je 1 pomenilo *močno se ne strinjam* in 7 *močno se strinjam*. Petstopenjsko Likertovo lestvico smo uporabili pri konstruktih za zaznano uporabnost, skrb glede zasebnosti in zaznane varnosti podatkov, pri čemer je 1 pomenilo *močno se ne strinjam* in 5 *močno se strinjam*. Pri konstruktih stališče do tehnoloških vsadkov, subjektivna norma in

Tabela 1: Teoretični konstrukti

Akronim	Naziv	Definicija	Vir
BI	Namera za uporabo	Ali so uporabniki pripravljeni uporabljati tehnološke vsadke in v kolikšni meri.	[57]
AtTI	Stališče do tehnoloških vsadkov	Kaj uporabniki na splošno menijo o tehnoloških vsadkih.	[58]
PU	Zaznana uporabnost	V kolikšni meri bi bili tehnološki vsadki uporabni v vsakodnevnem življenju uporabnika.	[55]
EoU	Enostavnost uporabe	Ali bi bila uporaba tehnoloških vsadkov uporabniku enostavna za uporabo in v kolikšni meri.	[55]
SN	Subjektivna norma	Kakšno bi bilo mišljenje uporabniku pomembnih ljudi do njegove uporabe tehnoloških vsadkov.	[44]
SC	Skrb glede nadzora	V kolikšni meri uporabnika skrbi, da ga država nadzoruje.	[35]
PDS	Zaznana varnost podatkov	V kolikšni meri uporabnik meni, da je na tehnoloških podatkih varno shranjevati podatke.	[28]
PC	Skrb za zasebnost	V kolikšni meri uporabnika skrbi, da bi bile njegove informacije na tehnoloških vsadkih ogrožene.	[59]

Tabela 2: Demografski podatki

	Število	Delež
Formalna izobrazba		
Končana srednja šola ali manj	88	36,2
Končana 1. bolonjska stopnja	93	38,3
Končana 2. bolonjska stopnja	50	20,6
Končana 3. bolonjska stopnja	10	4,1
Zaposlitveni status		
Dijak/študent	75	30,9
Zaposlen	156	64,2
Nezaposlen	8	3,3
Upokojen	1	0,4
Življenjsko okolje		
Urbano/mestno	138	56,8
Ruralno/podeželje	103	42,4

skrb glede nadzora smo uporabili lestvico petstopenjskega semantičnega diferenciala.

Podatke smo zbirali s spletnim vprašalnikom, merili pa smo na populacijo slovensko govorečih prebivalcev Slovenije, ki so aktivni uporabniki interneta, elektronske pošte ali družbenih omrežij. Pri vzorčenju smo uporabili priložnostno vzorčenje, podatke pa smo zbirali s pomočjo spletnega orodja za anketiranje (https://1ka.arnes.si). Povezavo do ankete smo delili po tematsko različnih skupinah na družbenem omrežju Facebook, prav tako pa tudi preko elektronske pošte v podjetjih in šolah. Na Ministrstvu za notranje zadeve so anketo objavili tudi na njihovem intranetu. Poudarjeno je bilo, da je anketa prostovoljna in anonimna, podatki pa bodo zbrani izključno v raziskovalne namene. Podatke smo zbirali novembra 2020.

Vprašalnik je izpolnilo 249 anketirancev, od tega smo jih šest izločili, saj so bili le delno izpolnjeni. V vzorec smo tako zajeli 243 enot. Povprečna starost med anketiranimi je bila 33 let, stari so bili od 17 do 62 let. Prikaz demografskih podatkov je viden v spodnjih tabelah. Več kot polovica (60,1 odstotka) anketirancev je bila ženskega spola. V tabeli 2 so prikazani preostali demografski podatki anketirancev. Največ jih je končalo prvo bolonjsko stopnjo oz. diplomiralo, več kot polovica anketirancev je zaposlenih.

5 REZULTATI

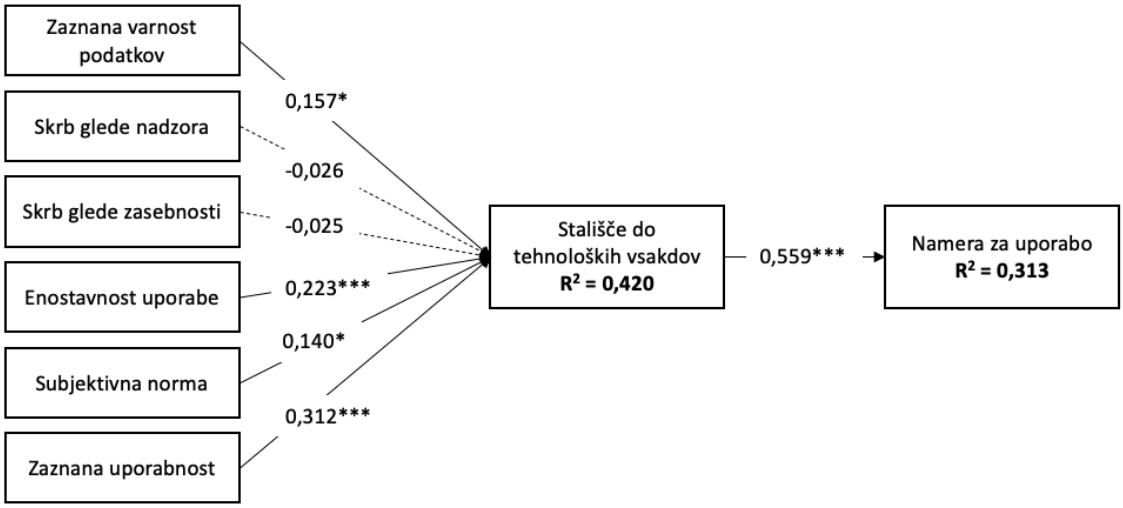
Zanesljivost vprašalnika smo merili s koeficientom Cronbach alfa – CA (Tabela 3). V vsakem od merjenih konstruktov so bile tri spremenljivke. Vse vrednosti so višje od 0,80, zato sklepamo, da je zanesljivost vprašalnika visoka. Tabela 3 prav tako prikazuje rezultate opisne statistike: aritmetično sredino (M), standardni odklon (SD) in mediano (Me). Rezultati nakazujejo, da v tem trenutku respondenti niso naklonjeni uporabi tehnoloških vsadkov in jih ne zaznavajo kot zelo uporabne. Prav tako ne izražajo velike skrbi, da bi bili preko vsadkov nadzorovani. Bolj kot skrb glede na nadzora jih skrbi njihova zasebnost, a aritmetična sredina in mediana nakazujeta na nevtralno vrednost.

Ustreznost vzorca smo preverili s Kaiser-Meyer-Olkinovo (KMO) mero ustreznosti, ki nakazuje, da je vzorec ustrezen ($KMO > 0,877$). Bartlettov test je potrdil homogenost varianc ($p < 0,001$). Faktorska analiza (*Principal Axis Factoring*) s poševnokotno rotacijo (*Direct Oblimin*) je potrdila razporeditev indikatorjev po osmih konstruktih. Z osmimi faktorji je mogoče pojasniti 83,2 odstotka variance. Za izvedbo večkratne linearne regresije so izpolnjene vse predpostavke (linearnost, homoskedastičnost, multikolinearnost, normalnost porazdelitve ostankov).

Model smo testirali z dvema linearnima regresijskima modeloma. Oba sta bila statistično značilna ($p < 0,001$). V prvem modelu smo testirali, kako neodvisne

Tabela 3: Zanesljivost vprašalnika in opisna statistika

Konstrukt	CA	M	SD	Me	Lestvica
Namera uporabe	0,97	2,34	1,60	2,00	Likert 1–7
Enostavnost uporabe	0,95	4,52	1,92	5,00	Likert 1–7
Zaznana uporabnost	0,91	2,37	1,13	2,33	Likert 1–5
Zaznana varnost podatkov	0,92	1,97	0,97	2,00	Likert 1–5
Skrb za zasebnost	0,96	4,04	1,11	4,33	Likert 1–5
Subjektivna norma	0,94	2,07	1,00	2,00	Semantični diferencial
Skrb glede nadzora	0,93	2,94	1,25	3,00	Semantični diferencial
Stališče do tehnoloških vsadkov	0,80	2,63	1,01	2,67	Semantični diferencial



Slika 1: Model z rezultati linearne regresije (vrednostmi β: * $p < 0,05$; *** $p < 0.001$)

spremenljivke, zaznana varnost podatkov, skrb glede nadzora, skrb glede zasebnosti, enostavnost uporabe, subjektivna norma in zaznana uporabnost napovedujejo stališče do tehnoloških vsadkov. V drugem modelu smo testirali, kako stališče do tehnoloških vsadkov napoveduje namero uporabe. Slika 1 prikazuje rezultate obeh linearnih regresijskih modelov. Hipoteze H1a, H2a, H2b, H2c, H3 potrdimo, medtem ko hipotezi H1b in H1c ne moremo niti potrditi niti ovreči.

6 RAZPRAVA

Namen pričujočega prispevka je bilo ugotoviti, katera tveganja vplivajo na sprejemanje vstavljivih tehnologij. Primerjamo lahko uporabo nosljivih naprav, ki so pred dobrim desetletjem pomenile "znanstveno fantastiko", vendar danes predstavljajo ogromen trg, ki se še vedno širi. Vstavljive tehnologije bi prav tako lahko sledile podobnemu razvoju. Vstavljive naprave že pomenijo ogromno prednost na področju zdravstva, saj se v telesa vgrajuje veliko naprav, ki lahko pomagajo pri zagotavljanju zdravja ljudi, npr. za uravnavanje srčnega ritma, izboljšanje vida, sluha in izboljšanje možganske aktivnosti [61].

V zadnjem obdobju se pogosto srečujemo z varnostnimi grožnjami, ki nam pretijo na spletu. Uporabniki se sicer zavedajo spletnih tveganj, kot so kraje osebnih podatkov in nevarne transakcije [40]. Kljub temu pa z uporabo raznih aplikacij in družbenih omrežij uporabniki pogosto delijo svoje osebne podatke [41], saj to pripomore k večji koristi za uporabnika in tudi k hitrejšim in bolj prilagojenim storitvam [42]. V tem primeru uporabniki ne morejo kriviti nikogar drugega kot samega sebe. Popolnoma drugače je v primeru nadzora državnih organov. V zadnjem obdobju se veliko pozornosti posveča prav nadzoru državnih organov in organov pregona nad državljani. To vključuje sprotno geografsko označevanje lokacije in dejavnosti posameznika v realnem času. Naprave, ki se vgradijo v človeško telo, bi lahko v bližnji prihodnosti postale nevarno orodje državnih organov. Leta 2017 je bil Ross Campton iz Ohia v Združenih državah Amerike obsojen zaradi požiga in zavarovalniške prevare, potem ko so organi kazenskega pregona uporabili podatke o delovanju njegovega srčnega spodbujevalnika kot ključni dokaz. Zaradi mogočega nadzora državnih organov so v Združenih državah Amerike v nekaterih zveznih državah (Wisconsin, Severna Dakota in Kalifornija) že uzakonili uporabo čipov. Tako svoje državljane varujejo pred neprostovoljno implementacijo tehnoloških vsadkov [13].

Dosedanje raziskave so pokazale, da mladi odločitve za uporabo tehnoloških vsadkov ne dojemajo kot tvegane

[8]. Ne glede na visoko komercialno rast pa obstajajo ovire pri sprejemanju tehnoloških vsadkov pri starejši populaciji [62]. Starost ljudi sama po sebi ne vpliva na namero uporabe pametnih naprav, ampak je ta odvisna od njihovega subjektivnega počutja. Starost ljudi presenetljivo povečuje naklonjenost uporabi [63], poleg tega pa so starejši dokaj naklonjeni temu, da avtomatizirane naprave skrbijo za njihovo varnost [62]. Po mnenju respondentov v naši raziskavi lahko sklepamo, da tehnološki vsadki v očeh ljudi niso zaznani kot varno sredstvo za shranjevanje podatkov in se ne bi počutili povsem varne, če bi imeli v tehnoloških vsadkih shranjene osebne podatke. V raziskavi smo ugotovili, da nadzor državnih organov uporabnikov ne moti preveč in glede tega niso pretirano zaskrbljeni. Skrb glede nadzora nad uporabniki in skrb glede zasebnosti ne napovedujeta stališč do tehnoloških vsadkov, zaznana varnost podatkov pa pozitivno vpliva na stališče do tehnoloških vsadkov. Naše ugotovitve kažejo tudi, da v splošnem ljudje ne menijo, da uporaba tehnoloških vsadkov pripore k olajševanju življenja, povečevanju njihovih zmožnosti in olajševanju vsakodnevnih dejavnosti. Čeprav skoraj nihče nima izkušenj z vstavljivo tehnologijo, menijo, da uporaba naprav zanje ne bi bila težavna oz. da bi bila preprosta. Enostavnost uporabe in zaznana uporabnost tudi v našem primeru najbolj vplivata na stališče do tehnoloških vsadkov. Na sprejemanje tehnologije pa pomembno vpliva tudi subjektivna norma. Večina ljudi je zaskrbljenih glede tega, kaj bi o njihovi uporabi tehnoloških vsadkov menile osebe, ki so jim pomembne.

Ljudje na splošno tehnološke naprave uporabljajo, če so udobne, saj jih nosijo zaradi funkcionalnosti, in ne zaradi tega, ker bi bile modne [57]. Rezultati naše raziskave kažejo, da stališče do tehnoloških vsadkov pozitivno napoveduje namero njihove uporabe. Ni pa videti, da bi bili respondenti tehnološke vsadke že pripravljeni širše uporabljati, čeprav tega ni mogoče izključiti za prihodnost. Na tem mestu je pomembno opozoriti na dejstvo, da družbena sprejemljivost ni statična, ampak je zelo dinamična in se lahko spreminja glede na nacionalni in mednarodni okvir ter trenutne razmere [64].

7 Omejitve in nadaljnje delo

Ta raziskava ima nekatere omejitve, na katere morajo biti bralci pozorni. Prvič, vzorec je bil priložnostni, saj nismo mogli zagotoviti enostavnega naključnega vzorčenja. Posploševanje rezultatov na populacijo zato zahteva previdnost. Prav tako smo v vzorcu zajeli več žensk kakor moških, povprečna starost respondentov v vzorcu pa ne odraža povprečne starosti prebivalstva v Sloveniji. Drugič, raziskovalni model je zajemal samo izbrane vidike tveganj in varnosti, in tako ne zagotavlja popolnega pregleda nad vsemi tveganji, ki bi jih respondenti zaznavali ob morebitni uporabi tehnoloških vsadkov. Kljub omenjenim omejitvam menimo, da rezultati nudijo dober vpogled v problematiko in vsaj deloma odražajo vlogo tveganj pri sprejemanju tehnoloških vsadkov med populacijo.

V nadaljnjih raziskavah bi se bilo smiselno osredotočiti na dodatne vidike tveganj, ki so povezani s tehnološkimi vsadki. Prav tako bi bilo treba raziskati razlike med zaznavami tveganj vsadkov za olajševanje življenj in vsadkov za medicinsko uporabo. Zaznave tveganj bi bile lahko različne glede na to delitev. Ne nazadnje bi bila smiselna tudi primerjava med državami, kjer so tehnološki vsadki za olajševanje življenj že (bili) prisotni, in državami, kjer takšnih vsadkov še ni mogoče zaslediti na trgu.

References

[1] O.-P. Cristina, P.-B. Jorge, R.-L. Eva, and A.-O. Mario, "From wearable to insideable: Is ethical judgment key to the acceptance of human capacity-enhancing intelligent technologies?" *Computers in Human Behavior*, vol. 114, p. 106559, jan 2021. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0747563220303095

[2] J. Pelegrín-Borondo, E. Reinares-Lara, C. Olarte-Pascual, and M. Garcia-Sierra, "Assessing the moderating effect of the end user in consumer behavior: The acceptance of technological implants to increase innate human capacities," *Frontiers in Psychology*, vol. 7, no. February, pp. 1–13, 2016.

[3] K. Murata, Y. Fukuta, Y. Orito, and A. Adams, "Cyborg Athletes or Technodoping," in *ETHICOMP 2018*, 2018, pp. 1–22.

[4] J. Giger and R. Gaspar, "A look into future risks: A psychosocial theoretical framework for investigating the intention to practice body hacking," *Human Behavior and Emerging Technologies*, vol. 1, no. 4, pp. 306–316, 2019.

[5] F. D. Davis, "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," *MIS Quarterly*, vol. 13, no. 3, pp. 319–340, 1989.

[6] M. T. Dishaw and D. M. Strong, "Extending the technology acceptance model with task–technology fit constructs," *Information & Management*, vol. 36, no. 1, pp. 9–21, 1999.

[7] J. Lu, C. S. Yu, C. Liu, and J. E. Yao, "Technology acceptance model for wireless Internet," *Internet Research*, vol. 13, no. 3, pp. 206–222, 2003.

[8] M. Arias-Oliva, J. Pelegrín-Borondo, A. M. Lara-Palma, and E. Juaneda-Ayensa, "Emerging cyborg products: An ethical market approach for market segmentation," *Journal of Retailing and Consumer Services*, vol. 55, no. May, p. 102140, 2020. [Online]. Available: https://doi.org/10.1016/j.jretconser.2020.102140

[9] J. Jiang and A.-F. Cameron, "IT-Enabled Self-Monitoring for Chronic Disease Self-Management: An Interdisciplinary Review," *MIS Quarterly*, vol. 44, no. 1, pp. 451–508, jan 2020.

[10] S. Gauttier, "'I've got you under my skin' – The role of ethical consideration in the (non-) acceptance of insideables in the workplace," *Technology in Society*, vol. 56, pp. 93–108, feb 2019.

[11] D. Halperin, T. S. Heydt-Benjamin, K. Fu, T. Kohno, and W. H. Maisel, "Security and Privacy for Implantable Medical Devices," *IEEE Pervasive Computing*, vol. 7, no. 1, pp. 30–39, jan 2008.

[12] W. Barfield and A. Williams, "Cyborgs and Enhancement Technology," *Philosophies*, vol. 2, no. 4, p. 4, 2017.

[13] A. K. Yetisen, "Biohacking," *Trends in Biotechnology*, vol. 36, no. 8, pp. 744–747, 2018.

[14] L. S. Hogaboam, "Assessment of Technology Adoption Potential of Medical Devices: Case of Wearable Sensor Products for Pervasive Care in Neurosurgery and Orthopedics," Ph.D. dissertation, Portland State University, Portland, OR, 2018.

[15] Y. Sun, F. P.-W. Lo, and B. Lo, "Security and Privacy for the Internet of Medical Things Enabled Healthcare Systems: A Survey," *IEEE Access*, vol. 7, pp. 183 339–183 355, 2019.

[16] H. Gangadharbatla, "Biohacking: An exploratory study to understand the factors influencing the adoption of embedded technolo-

gies within the human body," *Heliyon*, vol. 6, no. 5, p. e03931, 2020.

[17] S. Bueno, M. D. Gallego, and J. Noyes, "Uses and Gratifications on Augmented Reality Games: An Examination of Pokémon Go," *Applied Sciences*, vol. 10, no. 5, p. 1644, mar 2020.

[18] E. Lutolli and S. L. R. Vrhovec, "Adoption of smarthome devices: Blinded by benefits, ignoring the dangers?" *Elektrotehniški vestnik / Electrotechnical Review*, vol. 86, no. 5, pp. 267–273, 2019.

[19] Y. Meidan, V. Sachidananda, H. Peng, R. Sagron, Y. Elovici, and A. Shabtai, "A novel approach for detecting vulnerable IoT devices connected behind a home NAT," *Computers & Security*, vol. 97, p. 101968, oct 2020. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0167404820302418

[20] F. Alsubaei, A. Abuhussein, V. Shandilya, and S. Shiva, "IoMT-SAF: Internet of Medical Things Security Assessment Framework," *Internet of Things*, vol. 8, p. 100123, dec 2019.

[21] K. Rahul and R. K. Banyal, "Data Life Cycle Management in Big Data Analytics," *Procedia Computer Science*, vol. 173, no. 2019, pp. 364–371, 2020. [Online]. Available: https://doi.org/10.1016/j.procs.2020.06.042

[22] M. Chamikara, P. Bertok, I. Khalil, D. Liu, and S. Camtepe, "Privacy Preserving Face Recognition Utilizing Differential Privacy," *Computers & Security*, vol. 97, p. 101951, oct 2020. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0167404820302273

[23] A. Mihelič, M. Jevšček, S. Vrhovec, and I. Bernik, "Testing the human backdoor: Organizational response to a phishing campaign," *Journal of Universal Computer Science*, vol. 25, no. 11, pp. 1458–1477, 2019.

[24] S. AlGhamdi, K. T. Win, and E. Vlahu-Gjorgievska, "Information security governance challenges and critical success factors: Systematic review," *Computers & Security*, vol. 99, p. 102030, dec 2020. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0167404820303035

[25] J. Hou, L. Qu, and W. Shi, "A survey on internet of things security from data perspectives," *Computer Networks*, vol. 2019, no. 148, pp. 295–306, 2019. [Online]. Available: https://doi.org/10.1016/j.comnet.2018.11.026

[26] S. Vrhovec, "Safe mobile device use in the cyberspace / Varna uporaba mobilnih naprav v kibernetskem prostoru," *Elektrotehniški vestnik / Electrotechnical Review*, vol. 83, no. 3, pp. 144–147, 2016.

[27] S. L. R. Vrhovec, "Safe use of mobile devices in the cyberspace," in *39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO 2016)*. Opatija, Croatia: Croatian Society for Information and Communication Technology, Electronics and Microelectronics, 2016, pp. 1639–1643.

[28] J. Khalilzadeh, A. B. Ozturk, and A. Bilgihan, "Security-related factors in extended UTAUT model for NFC based mobile payment in the restaurant industry," *Computers in Human Behavior*, vol. 70, pp. 460–474, may 2017.

[29] L. Jelovčan, D. Fujs, S. Vrhovec, and A. Mihelič, "The role of information sensitivity in adoption of E2EE communication software," in *European Interdisciplinary Cybersecurity Conference (EICC 2020)*. Rennes, France: ACM, 2020, pp. 13:1–2.

[30] Q. Chen, Y. Feng, L. Liu, and X. Tian, "Understanding consumers' reactance of online personalized advertising: A new scheme of rational choice from a perspective of negative effects," *International Journal of Information Management*, vol. 44, pp. 53–64, feb 2019.

[31] Y. Li, "A multi-level model of individual information privacy beliefs," *Electronic Commerce Research and Applications*, vol. 13, no. 1, pp. 32–44, 2014. [Online]. Available: http://dx.doi.org/10.1016/j.elerap.2013.08.002

[32] I.-D. Anic, V. Škare, and I. Kursan Milaković, "The determinants and effects of online privacy concerns in the context of e-commerce," *Electronic Commerce Research and Applications*, vol. 36, p. 100868, jul 2019.

[33] Á. Herrero, H. San Martín, and M. d. M. Garcia-De los Salmones, "Explaining the adoption of social networks sites for sharing user-generated content: A revision of the UTAUT2," *Computers in Human Behavior*, vol. 71, pp. 209–217, jun 2017.

[34] J. Huang, S. Kumar, and C. Hu, "Does Culture Matter? A Comparative Study on the Motivations for Online Identity Reconstruction Between China and Malaysia," *SAGE Open*, vol. 10, no. 2, p. 215824402092931, apr 2020.

[35] T. Nam, "Untangling the relationship between surveillance concerns and acceptability," *International Journal of Information Management*, vol. 38, no. 1, pp. 262–269, 2018.

[36] M. Abdelhamid, "The Role of Health Concerns in Phishing Susceptibility: Survey Design Study," *Journal of Medical Internet Research*, vol. 22, no. 5, p. e18394, 2020.

[37] D. Fujs, S. Vrhovec, and A. Mihelič, "What drives the motivation to self-protect on social networks? The role of privacy concerns and perceived threats," in *Central European Cybersecurity Conference 2018 (CECC 2018)*. Ljubljana, Slovenia: ACM, 2018, pp. 11:1–6.

[38] E. M. Schomakers, C. Lidynia, and M. Ziefle, "Listen to My Heart? How Privacy Concerns Shape Users' Acceptance of e-Health Technologies," *International Conference on Wireless and Mobile Computing, Networking and Communications*, vol. 2019-Octob, pp. 306–311, 2019.

[39] J. W. Kang and Y. Namkung, "The role of personalization on continuance intention in food service mobile apps: A privacy calculus perspective," *International Journal of Contemporary Hospitality Management*, vol. 31, no. 2, pp. 734–752, 2019.

[40] J. H. Wu and S. C. Wang, "What drives mobile commerce? An empirical evaluation of the revised technology acceptance model," *Information and Management*, vol. 42, no. 5, pp. 719–729, 2005.

[41] G. Pizzi and D. Scarpi, "Privacy threats with retail technologies: A consumer perspective," *Journal of Retailing and Consumer Services*, vol. 56, p. 102160, sep 2020.

[42] N. Shaw and K. Sergueeva, "The non-monetary benefits of mobile commerce: Extending UTAUT2 with perceived value," *International Journal of Information Management*, vol. 45, no. October 2018, pp. 44–55, 2019.

[43] D. Fujs, S. L. R. Vrhovec, and A. Mihelič, "The role of emojis and emoticons in social engineering / Vloga čustvenčkov in čustvenih simbolov pri socialnem inženiringu," *Psihološka obzorja / Horizons of Psychology*, vol. 29, pp. 134–142, 2020.

[44] Y. Zhu, S. L. Dailey, D. Kreitzberg, and J. Bernhardt, ""Social Networkout": Connecting Social Features of Wearable Fitness Trackers with Physical Exercise," *Journal of Health Communication*, vol. 22, no. 12, pp. 974–980, dec 2017.

[45] V. Venkatesh, J. Y. L. Thong, F. K. Y. Chan, P. J.-H. Hu, and S. A. Brown, "Extending the two-stage information systems continuance model: incorporating UTAUT predictors and the role of context," *Information Systems Journal*, vol. 21, no. 6, pp. 527–555, nov 2011.

[46] P. A. Pavlou, "Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model," *International Journal of Electronic Commerce*, vol. 7, no. 3, pp. 101–134, 2003.

[47] S. Ha and L. Stoel, "Consumer e-shopping acceptance: Antecedents in a technology acceptance model," *Journal of Business Research*, vol. 62, no. 5, pp. 565–571, 2009. [Online]. Available: http://dx.doi.org/10.1016/j.jbusres.2008.06.016

[48] D. Fujs and S. L. R. Vrhovec, "Cyber Landscape of Trust, Fear and Surveillance Concerns: How Slovenians Around the Globe Perceive the Cyberspace," *Varstvoslovje / Journal of Criminal Justice and Security*, vol. 21, no. 4, pp. 333–345, 2019.

[49] K. van der Schyff, S. Flowerday, and S. Furnell, "Duplicitous social media and data surveillance: An evaluation of privacy risk," *Computers & Security*, vol. 94, p. 101822, jul 2020. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0167404820300961

[50] D. Fujs, A. Mihelič, and S. Vrhovec, "Social Network Self-Protection Model: What Motivates Users to Self-Protect?" *Journal of Cyber Security and Mobility*, vol. 8, no. 4, pp. 467–492, 2019.

[51] S. Vrhovec and B. Markelj, "Relating Mobile Device Use and Adherence to Information Security Policy with Data Breach Consequences in Hospitals," *Journal of Universal Computer Science*, vol. 24, no. 5, pp. 634–645, 2018.

[52] T. Pikkarainen, K. Pikkarainen, H. Karjaluoto, and S. Pahnila, "Consumer acceptance of online banking: An extension of the

technology acceptance model," *Internet Research*, vol. 14, no. 3, pp. 224–235, 2004.
[53] A. Mihelič and S. Vrhovec, "A model of self-protection in the cyberspace / Model samozaščite v kibernetskem prostoru," *Elektrotehniški vestnik / Electrotechnical Review*, vol. 85, no. 1–2, pp. 13–22, 2018.
[54] T. Ramayah, "The role of voluntariness in distance education students' usage of a course website," *Turkish Online Journal of Educational Technology*, vol. 9, no. 3, pp. 96–105, 2010.
[55] J. Pelegrín-Borondo, E. Reinares-Lara, and C. Olarte-Pascual, "Assessing the acceptance of technological implants (the cyborg): Evidences and challenges," *Computers in Human Behavior*, vol. 70, pp. 104–112, 2017.
[56] A. Murko and S. L. R. Vrhovec, "Bitcoin adoption: Scams and anonymity may not matter but trust into Bitcoin security does," in *Central European Cybersecurity Conference (CECC 2019)*. Munich, Germany: ACM, 2019, pp. 15:1–6.
[57] H. S. Chang, S. C. Lee, and Y. G. Ji, "Wearable device adoption model with TAM and TTF," *International Journal of Mobile Communications*, vol. 14, no. 5, p. 518, 2016.
[58] J. T. Siegel, M. A. Navarro, C. N. Tan, and M. K. Hyde, "Attitude–behavior consistency, the principle of compatibility, and organ donation: A classic innovation." *Health Psychology*, vol. 33, no. 9, pp. 1084–1091, 2014.
[59] A. Marakhimov and J. Joo, "Consumer adaptation and infusion of wearable devices for healthcare," *Computers in Human Behavior*, vol. 76, pp. 135–148, nov 2017.
[60] C. Rijcken, *Rainforests of wearables and insideables*. Elsevier Inc., 2019. [Online]. Available: http://dx.doi.org/10.1016/B978-0-12-817638-2.00010-9
[61] C. Olarte-Pascual, J. Pelegrín-Borondo, and E. Reinares-Lara, "Implants to increase innate capacities: Integrated vs. apocalyptic attitudes. Is there a new market?" *Universia Business Review*, vol. 2015, no. 48, pp. 86–117, 2015.
[62] S. Arthanat, H. Chang, and J. Wilcox, "Determinants of information communication and smart home automation technology adoption for aging-in-place," *Journal of Enabling Technologies*, vol. 14, no. 2, pp. 73–86, may 2020.
[63] S. Farivar, M. Abouzahra, and M. Ghasemaghaei, "Wearable device adoption among older adults: A mixed-methods study," *International Journal of Information Management*, vol. 55, no. April, p. 102209, dec 2020.
[64] I. Georgieva, E. Beaunoyer, and M. J. Guitton, "Ensuring social acceptability of technological tracking in the COVID-19 context," *Computers in Human Behavior*, vol. 116, no. November 2020, p. 106639, 2020. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0747563220303861

Lara Klemenc je magistrirala na Fakulteti za varnostne vede Univerze v Mariboru. Zaposlena je na Ministrstvu za notranje zadeve.

Simon Vrhovec je docent na Univerzi v Mariboru. Doktorat iz računalništva in informatike Univerze v Ljubljani je prejel leta 2015. Leta 2018 in 2019 je sopredsedoval konferenci Central European Cybersecurity Conference (CECC). Od leta 2019 je v usmerjevalnem odboru konference European Interdisciplinary Cybersecurity Conference (EICC). Je član uredniških odborov revij Journal of Cyber Security and Mobility, Frontiers in Computer Science, EUREKA: Social and Humanities in International Journal of Cyber Forensics and Advanced Threat Investigations. Je ali je bil gostujoči urednik posebnih izdaj revij IEEE Security & Privacy, Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA) in Journal of Universal Computer Science (J.UCS). Njegovi glavni raziskovalni interesi so človeški dejavniki v kibernetski varnosti, razvoj varne programske opreme, agilne metode in management sprememb.

Anže Mihelič je leta 2016 magistriral na Fakulteti za varnostne vede Univerze v Mariboru. Je doktorski kandidat na Fakulteti za računalništvo in informatiko ter na Pravni fakulteti Univerze v Ljubljani. Kot asistent je zaposlen na Fakulteti za varnostne vede Univerze v Mariboru, kot raziskovalec pa na Fakulteti za matematiko in računalništvo na FernUniversität in Hagen. Njegovi raziskovalni interesi obsegajo tehnične in človeške informacijske in kibernetske varnosti ter agilen razvoj varne programske opreme.