Kompetenčne vrzeli in kadrovski izzivi na področju informacijske in kibernetske varnosti: analiza stanja v Sloveniji

Andreja Markun, Alenka Brezavšček
Fakulteta za organizacijske vede, Univerza v Mariboru, Kidričeva cesta 55a,4000 Kranj
andreja.markun@student.um.si, alenka.brezavscek@um.si

Izvleček

V času hitro rastoče digitalizacije postaja vprašanje kadrovskih kompetenc in zagotavljanja ustrezno usposobljenih in kompetentnih kadrov na področju informacijske in kibernetske varnosti vse bolj ključno za dolgoročno digitalno odpornost organizacij. V prispevku predstavljamo rezultate nedavne raziskave, ki je bila izvedena med slovenskimi organizacijami. Raziskava razkriva izrazite kompetenčne vrzeli na področju informacijske in kibernetske varnosti, pri čemer je bila kot glavna ovira za tako stanje izpostavljeno pomanjkanje usposobljenega kadra na trgu. Ugotovljeno je bilo, da organizacije, ki varnost vključujejo v strateške cilje, prej prepoznajo potrebe po kadrovskem razvoju, proaktivno načrtujejo izobraževanja ter bolj sistematično gradijo kompetenčne baze. Zaznani so bili tudi začetni učinki sprememb v zakonodajnih okvirih ZInfV-1 in NIS2, predvsem v obliki večjih vlaganj v usposabljanje in sodelovanje z zunanjimi izvajalci. Prispevek ponuja empirično podlago za oblikovanje sistemskih ukrepov in podpira strateško načrtovanje razvoja kadrov na področju informacijske in kibernetske varnosti za učinkovito obvladovanje digitalnih tveganj v slovenskem prostoru.

Ključne besede: kompetence, zagotavljanje kadrov, informacijska varnost, kibernetska varnost, digitalna odpornost, slovensko gospodarstvo

Skills gaps and workforce challenges in information and cyber security: Insights from Slovenia

Abstract

In the age of rapidly advancing digitalisation, the issue of workforce skills and the availability of appropriately trained and qualified information and cyber security professionals is becoming increasingly important for the long-term digital resilience of organisations. This paper presents the results of a recent study conducted among Slovenian organisations. The research reveals significant skill gaps in the area of information and cyber security, with the lack of qualified professionals in the labour market seen as the main obstacle. It was found that companies which integrate security into their strategic objectives recognise staff development needs earlier, plan training proactively, and build a skill base more systematically. Initial effects of the changes to the ZInfV-1 and NIS2 legal frameworks were also observed, particularly in the form of increased investment in training and collaboration with external providers. The paper provides an empirical basis for the development of systemic measures and supports strategic workforce planning for effective digital risk management in Slovenia.

Keywords: Competencies, workforce development, information security, cyber security, digital resilience, Slovenian economy

1 UVOD

Informacijska varnost (angl. information security) in kibernetska varnost (angl. cyber security) sta postali ključen dejavnik digitalne operativne odpornosti organizacij [1]. Čeprav se pojma v praksi pogosto (neupravičeno) uporabljata kot sinonima, med njima obstajajo pomembne razlike: informacijska varnost zajema zaščito vseh informacij, ne glede na obliko ali medij, kibernetska varnost pa kot njen ožji podsklop obsega predvsem varovanje digitalnih sistemov in omrežij ter s tem podatkov in informacij, ki se v njih obdelujejo. Hitro napredujoča digitalizacija poslovnih procesov, razpršena informacijsko-komunikacijska infrastruktura ter vse pogostejši napredni kibernetski napadi povečujejo tveganja in organizacije silijo v sistematičen pristop k varovanju informacijskih sredstev, kar obema področjema daje vse večjo težo. V ospredje zato stopa potreba po strokovnjakih, ki poleg tehničnih obvladujejo tudi organizacijske, pravne in komunikacijske vidike varnosti [2].

Na ravni Evropske unije sta kot odziv na zaznane primanjkljaje kompetenc na področju informacijske in kibernetske varnosti nastala dva ključna okvira: European e-Competence Framework (e-CF) in European Cybersecurity Skills Framework (ECSF). Prvi opredeljuje 41 IKT kompetenc, razporejenih v pet procesnih področij in pet stopenj zahtevnosti, drugi pa zajema 12 poklicnih profilov s področja kibernetske varnosti z natančno določenimi znanji, spretnostmi in odgovornostmi [3, 4]. Kljub temu se zdi, da številne organizacije nimajo pregleda nad ključnimi kompetencami, ki jih potrebujejo, niti ne izvajajo sistematičnih pristopov k njihovemu razvoju [5].

Podatki SI-CERT-a kažejo, da se v praksi kibernetske grožnje še vedno pogosto kažejo v obliki ciljnih napadov na uporabnike, pri čemer so napadi vse bolj izpopolnjeni, odzivni časi pa pogosto nezadostni [6]. V takšnem okolju postaja ključno, da organizacije krepijo svojo notranjo odpornost ne le z vlaganjem v tehnologijo, temveč tudi s kadrovskimi ukrepi [7].

Poleg tega v letošnjem letu sprejeti Zakon o informacijski varnosti (ZInfV-1) in evropska direktiva Network and information systems directive (NIS2) uvajata obveznosti za zavezance glede zagotavljanja ustreznih varnostnih ukrepov, postopkov obvladovanja tveganj in usposobljenosti osebja [8, 9]. Nova zakonodaja tako vpliva na organizacijsko strukturo, opredeljevanje vlog ter strateško umeščanje informacijske/kibernetske varnosti na strateško raven. Po drugi strani pa analize opozarjajo na praktične izzive, ki spremljajo implementacijo zakonodaje in zajemajo dejavnike od nejasnosti glede izvedbe in obsega zahtev, pri čemer se pomanjkanje usposobljenega kadra izpostavlja kot pomemben dejavnik [10, 11]. Ob tem se vse bolj poudarja tudi potreba po razvoju celostnih kompetenc na področju informacijske/kibernetske varnosti, ki poleg tehničnih znanj vključujejo tudi mehke veščine, razumevanje poslovnega konteksta, upravljanje tveganj in skladnost z zakonodajo [12, 13]. Raziskave kažejo tudi, da organizacije pogosto investirajo v tehnologijo, a zanemarjajo vlaganje v človeški kapital, ki je ključen za učinkovito delovanje varnostnih mehanizmov [14, 15].

Kljub številnim evropskim pobudam, kot so ECSF, e-CF in strategije ENISA, se zdi, da problematika zagotavljanja kompetentnih kadrov na področju informacijske/kibernetske varnosti ostaja pereč problem tako v Evropi kot širše. Najnovejša študija organizacije ISC2 opozarja, da v Evropi primanjkuje več kot 390.000 strokovnjakov s področja kibernetske varnosti, globalno pa več kot štiri milijone, pri čemer se vrzel ne zmanjšuje temveč celo povečuje [16]. Kot poročajo strokovni krogi, Slovenija pri tem ni nobena izjema [17, 18]. Avtorji opozarjajo na razmeroma nizko zanimanje mladih za poklicne poti v tej panogi in posledično na pomanjkanje ustrezno usposobljenih kadrov na trgu dela [19]. Kljub zaznanemu problemu pa na podlagi pregleda literature in dostopnih virov nismo zasledili nobene celovite raziskave, ki bi sistematično prikazala dejansko stanje na ravni slovenskih organizacij. S pričujočim prispevkom želimo to raziskovalno vrzel zapolniti.

V prispevku predstavljamo del rezultatov empirične raziskave, ki je bila izvedena sredi leta 2025 na vzorcu slovenskih organizacij [20]. Namen raziskave je bil prepoznati tista znanja in kompetence s področja informacijske in kibernetske varnosti, ki jih slovenske organizacije prepoznavajo kot ključne, oceniti njihovo aktualno pokritost in identificirati glavne ovire pri nadaljnjem razvoju kadrovskega potenciala na tem področju. Poleg tega smo želeli celovito analizirati povezavo med zaznanimi kompetenčnimi vrzelmi, organizacijskimi ukrepi in vplivom zakonodaje na kadrovske strategije. Rezultati in ugotovitve prispevajo k razumevanju stanja na ravni slovenskega gospodarstva in prikazujejo smernice za sistemska priporočila v smeri krepitve nacionalne kibernetske odpornosti.

2 METODOLOGIJA

2.1 Ozadje problema

Potreba po usposobljenem kadru na področju informacijske in kibernetske varnosti se v zadnjih letih uveljavlja kot ena ključnih razvojnih prioritet organizacij. Strateška umeščenost informacijske/kibernetske varnosti v poslovne cilje ni le odraz zrelosti organizacij, temveč vpliva tudi na oblikovanje kadrovskih politik, postopkov in struktur. Raziskave kažejo, da organizacije, ki informacijsko/kibernetsko varnost obravnavajo kot sestavni del strateškega upravljanja, bistveno pogosteje izvajajo načrtovan razvoj kompetenc in zagotavljajo notranje procese za krepitev varnostne kulture [21, 22]. Pri tem se kompetenčne vrzeli ne kažejo le v tehničnem znanju, temveč v širšem neskladju med potrebami delodajalcev, ponudbo izobraževalnega sistema in dejansko razpoložljivostjo kadra na trgu dela [23, 24].

V zadnjem desetletju so se oblikovali tudi teoretični modeli, ki sistematizirajo kibernetske kompetence in poklicne vloge. Med najpomembnejšimi sta ECSF, ki ga je razvila agencija ENISA, in ameriški National Initiative for Cybersecurity Education (NICE) Framework, ki je standardiziran pod okriljem NIST [25, 26]. Oba okvirja poudarjata potrebo po strukturiranem povezovanju delovnih mest, znanj in spretnosti, kar omogoča boljšo primerljivost, razvoj kadrov in načrtovanje izobraževanj. ECSF posebej izpostavlja pomen strokovne specializacije, obenem pa prepoznava tudi mehke in organizacijske kompetence, kar je pogosto zapostavljeno v tradicionalnih pristopih k izobraževanju [27].

Raziskave v zadnjih letih vse bolj opozarjajo na pomen človeškega dejavnika v informacijski/kibernetski varnosti. Nezadostno zavedanje zaposlenih, pomanjkanje vodstvene podpore in odsotnost celovite kompetenčne strategije pogosto vodijo do neučinkovitosti tudi pri sicer tehnično ustrezno vzpostavljenih varnostnih sistemih [28, 29]. S tem postaja razumevanje organizacijske kulture, notranje komunikacije in vloge vodstva neločljiv del učinkovitega obvladovanja tveganj.

Pomemben segment teoretičnega okvira predstavlja tudi vpliv zakonodaje na oblikovanje kadrovskih ukrepov. Direktiva NIS2 in nedavno sprejeti ZInfV-1 namreč zavezancem nalagata obveznost zagotavljanja ne le tehničnih temveč tudi kadrovskih in organizacijskih ukrepov. Odgovornost za izvajanje teh ukrepov je pogosto porazdeljena med več deležnikov znotraj organizacije, kar zahteva jasno opredeljene vloge in trajno izobraževanje zaposlenih [30, 11]. Vendar izkušnje iz prakse kažejo, da implementacija zakonodaje pogosto naleti na omejitve. Številne organizacije nimajo zadostnih resursov za izvajanje potrebnih usposabljanj, pogosto pa se soočajo tudi s pomanjkanjem usmeritev in nejasnostmi glede zahtev za implementacijo kakor tudi z visokimi stroški, ki jih implementacija prinese [30, 16].

V tem kontekstu je preučevanje kompetenčnih potreb, ovir in vpliva zakonodaje na kadrovske politike ključno za razumevanje, kako lahko organizacije dolgoročno krepijo svojo kibernetsko odpornost. Raziskava tako temelji na presečišču sodobnih kompetenčnih modelov, strateškega upravljanja varnosti in regulativnih zahtev, ob upoštevanju značilnosti slovenskega institucionalnega in tržnega okolja.

2.2 Načrt in izvedba raziskave

Osnovni namen raziskave je preučiti kompetenčne potrebe slovenskih organizacij na področju informacijske/kibernetske varnosti, zaznane ovire pri razvoju kadrovskih virov ter vpliv aktualne zakonodaje na izvajanje kadrovskih ukrepov. Za potrebe raziskave je bil razvit namenski vprašalnik, ki pokrival različne tematske sklope, povezane s strateškim pristopom k varnosti, oceno pomembnosti in pokritosti znanj in kompetenc, zaznanimi ovirami ter vplivom zakonodaje. Celoten vprašalnik je dostopen v [20]. Ciljna populacija so bile slovenske organizacije, ki se na kakršenkoli način srečujejo z informacijsko/kibernetsko varnostjo, pri čemer je bile k izpolnjevanju ankete povabljene predvsem osebe, odgovorne za informacijsko/kibernetsko varnost, kadrovski razvoj ali strateško upravljanje. Tak izbor je omogočil pridobivanje podatkov z visoko vsebinsko relevantnostjo in zajem različnih vidikov obravnavanega problema.

V sklopu raziskave smo želeli odgovoriti na več raziskovalnih vprašanj, pri čemer se v pričujočem članku osredotočamo na naslednja raziskovalna vprašanja:

RV1: Ali lahko trdimo, da je splošno stanje na področju zagotavljanja kompetentnega kadra za informacijsko/kibernetsko varnost v Sloveniji ocenjeno kot slabo?

RV2: Ali lahko trdimo, da se večina slovenskih organizacij sooča s pomanjkanjem ustrezno usposob-

ljenega in kompetentnega kadra s področja informacijske/kibernetske varnosti?

RV3: Ali obstajajo statistično značilne razlike v zaznavanju pomanjkanja ustrezno usposobljenega in kompetentnega kadra glede na lastništvo organizacije (javno, zasebno, mešano)?

RV4: Ali organizacije, ki informacijsko/kibernetsko varnost obravnavajo kot strateško prioriteto, v večji meri zaznavajo pomanjkanje ustrezno usposobljenega in kompetentnega kadra na tem področju?

RV5: Katere ovire zaznavajo slovenske organizacije kot najbolj kritične pri razvoju kompetenc na področju informacijske/kibernetske varnosti?

RV6: Ali zavezanost organizacije zakonodajnem okviru ZInfV-1 in NIS2 vpliva na izvajanje dodatnih kadrovskih ukrepov na področju informacijske/kibernetske varnosti?

Raziskava je bila izvedena v maju in juniju 2025 preko orodja za spletno anketiranje 1KA (https://www.1ka.si/). Podatki so bili analizirani s programom IBM SPSS Statistics in Microsoft Excel.

3 REZULTATI

V nadaljevanju najprej predstavimo osnovne značilnosti vzorca sodelujočih organizacij, temu pa sledijo rezultati analize posameznih raziskovalnih vprašanj.

3.1 Predstavitev vzorca

Anketni vprašalnik je v celoti izpolnilo 235 organizacij iz različnih sektorjev slovenskega gospodarstva. Ključne lastnosti vzorca sodelujočih organizacij so strnjene v tabeli 1.

Razvidno je, da so v raziskavi sodelovale organizacije vseh velikostnih razredov, pri čemer prevladujejo velike, večinoma zasebne organizacije iz osrednjeslovenske regije. Dejavnost organizacij je raznolika. Največji delež predstavljajo organizacije iz sektorja informacijskih in komunikacijskih dejavnosti, sledijo jim organizacije iz finančnega sektorja, javne uprave, izobraževanja ter strokovnih in tehničnih storitev. Na 5-stopneski lestvici je bila ocenjena stopnja digitalizacije procesov v organizacijah večinoma srednja do visoka (M=3,4; SD=0,9), kar nakazuje na razmeroma visoko tehnološko zrelost sodelujočih organizacij. Glede statusa po zakonodaji ZInfV-1 in NIS2 se je približno polovica sodelujočih opredelila kot pomembni ali bistveni (skupaj 46 %) subjekt, medtem ko 27 % organizacij ni zavezancev. Prav tolikšen delež (27 %) pa se glede tega vprašanja ni znalo jasno opredeliti.

Tabela 1: **Struktura vzorca sodelujočih organizacij (n=235)**

Značilnost organizacije	Kategorija	Št. odgovorov (n)	Delež (%)
velikost	mikro (do 10 zaposlenih)	42	18
	mala (do 50 zaposlenih)	51	22
	srednja (do 250 zaposlenih)	55	23
	velika (nad 250 zaposlenih)	87	37
vrsta lastništva / financiranja	javno	73	31
	zasebno	125	53
	mešano	37	16
regija sedeža	Osrednjeslovenska	119	51
	Gorenjska	49	21
	ostale regije	67	28
glavna dejavnost po SKD	informacijske in komunikacijske dejavnosti	69	29
	finančne in zavarovalniške dejavnosti	18	8
	dejavnost javne uprave, obrambe, izobraževanja, zdravstva ipd.	59	25
	ostale dejavnosti	89	38
stopnja digitalizacije procesov	zelo nizka/nizka (1–2)	27	11
	srednja (3)	101	43
	visoka/zelo visoka (4–5)	107	46
status po ZInfV-1/NIS2	ni zavezanec	64	27
	pomembni subjekt	58	25
	bistveni subjekt	49	21
	ne vem	64	27

3.2 Ocena splošnega stanja na področju zagotavljanja kompetentnega kadra za informacijsko/kibernetsko varnost v Sloveniji

Organizacije, ki so v raziskavi sodelovale, so splošno stanje na področju zagotavljanja kompetentnega kadra za informacijsko/kibernetsko varnost v Sloveniji ocenjevale na lestvici od 1 do 5, pri čemer je 1 pomenilo »zelo slabo«, 5 pa »zelo dobro«. Povprečna ocena je bila 2,74 (*SD*=0,84), porazdelitev odgovorov pa je prikazana na sliki 1.

Da bi odgovorili na RV1, smo izvedli enostranski *t*-test, s katerim smo želeli preveriti, če je povprečna ocena splošnega stanja na področju zagotavljanja kompetentnega kadra za informacijsko/kibernetsko varnost v Sloveniji statistično značilno nižja od sredinske vrednosti 3 na ocenjevalni lestvici. Rezultati testa, predstavljeni v tabeli 2, so slednje potrdili ($t(234)=4{,}69$, $p<0{,}001$). Trditi torej smemo, da je povprečna ocena splošnega stanja na področju zagotavljanja kompetentnega kadra za informacijsko/kibernetsko varnost v Sloveniji statistično značilno nižja od sredinske vrednosti na ocenjevalni lestvici. Velikost učinka, izražena s Cohenovim *d* (–0,31), kaže na majhen do srednje majhen učinek, kar pomeni, da je razlika med ocenjenim stanjem in sredinsko vrednostjo sicer zanesljiva, a v praktičnem smislu zmerno izrazita. Na raziskovalno vprašanje RV1 tako lahko odgovorimo pritrdilno.

Tabela 2: **Rezultati t-testa za potrebe analize RV1**

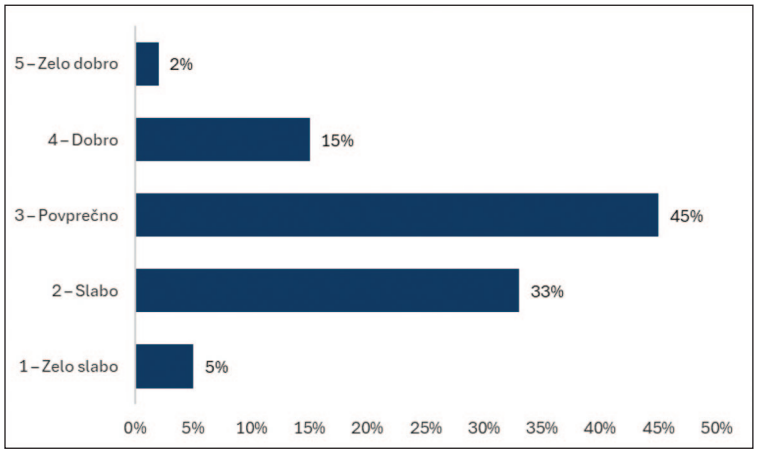
M	*SD*	*t*	*df*	*p*	Cohenov *d*
2,74	0,83	–4,694	234	<0,001	–0,306

Takšna ocena ni nepričakovana. Izkušnje iz prakse kažejo, da se organizacije že več let soočajo z izzivi pri zaposlovanju kadra, zlasti na področjih, ki zahtevajo specifična tehnična znanja, razumevanje regulatornega okvira (npr. ZInfV-1, NIS2) in sposobnost delovanja v visoko dinamičnem okolju. Razkorak med pričakovanji delodajalcev in dejansko razpoložljivostjo kadra se kaže ne le v številu razpoložljivih kandidatov temveč tudi v kakovosti njihovih znanj, kompetenc in izkušenj.

Zato nizka povprečna ocena ne odraža zgolj trenutnega stanja, temveč predstavlja jasno opozorilo o potrebi po dolgoročnem in usklajenem sistemskem ukrepanju. Ključno postaja vprašanje, ali trenutni izobraževalni sistem in obstoječe pobude za razvoj kadrov zmorejo ustrezno odgovoriti na identificirane potrebe. Rešitev ne tiči v kratkoročnih projektih ali posamičnih iniciativah, temveč v celoviti strategiji, ki vključuje:

- usklajevanje izobraževalnih programov s potrebami trga dela,
- stalno strokovno izpopolnjevanje na področju informacijske in kibernetske varnosti,
- razvoj nacionalnih standardov znanj in certifikacij,
- ter intenzivnejše povezovanje med gospodarstvom, državo in akademsko sfero.

V razmerah, kjer regulativni pritiski naraščajo, kibernetska odpornost pa postaja ključna za poslovno kontinuiteto, to vprašanje ni več zgolj razvojna prioriteta temveč osnovni pogoj za dolgoročno preživetje na trgu.



Slika 1: **Porazdelitev ocen o splošnem stanju zagotavljanja kadra za informacijsko/kibernetsko varnost v Sloveniji (n = 235).**

Ugotovitve o nizki zaznani razpoložljivosti strokovnjakov za kibernetsko varnost imajo neposredne implikacije za kadrovske in strateške politike slovenskih organizacij. Vodstva bi morale to zaznavo razumeti kot poziv k proaktivnemu upravljanju s talenti, intenzivnejšemu razvoju notranjih usposabljanj ter oblikovanju partnerstev z izobraževalnimi ustanovami. V pogojih omejene ponudbe se bodo konkurenčne prednosti gradile tudi na sposobnosti organizacij, da same razvijajo potrebne kompetence in ustvarjajo okolje, ki spodbuja zadrževanje ključnega kadra.

3.3 Soočanje s pomanjkanjem ustrezno usposobljenega in kompetentnega kadra v organizacijah

Za potrebe analize RV2 smo uporabili naslednje vprašanje iz anketnega vprašalnika: *»Ali v vaši organizaciji zaznavate pomanjkanje ustrezno usposobljenega in kompetentnega kadra s področja informacijske/kibernetske varnosti?«*. Porazdelitev odgovorov ponazarja slika 2, iz katere je razvidno, da večina organizacij zaznava vsaj delno pomanjkanje kadra (ocena 2 ali 3).

Razvidno je, da je vzorčni delež organizacij, ki so na naše vprašanje odgovorili z oceno vsaj 2, kar 70,6 %. Da bi dobili celovit odgovor na RV2, smo izvedli binomski test deleža, kjer smo kot testno vrednost izbrali 0,5. Rezultati, podani v tabeli 3, nakazujejo, da je rezultat testa statistično značilen, saj je $p<0{,}001$. Na podlagi tega torej lahko trdimo, da večina slovenskih organizaciji (več kot 50 % le-teh) zaznava pomanjkanje ustrezno usposobljenega in kompetentnega kadra s področja informacijske/kibernetske varnosti, kar pomeni, da na RV2 lahko odgovorimo pritrdilno.

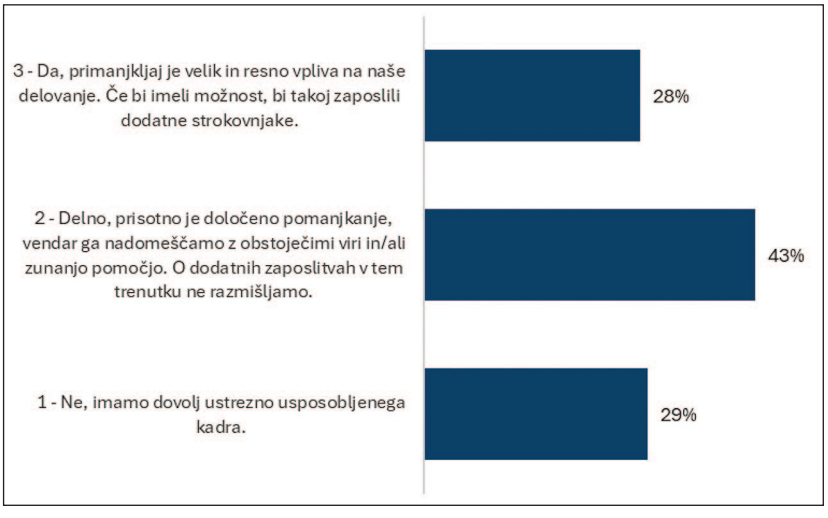
Tabela 3: **Rezultati binomskega testa za potrebe analize RV2**

Skupina	Št. odgovorov	Delež (%)	Testna vrednost	*p*
zaznavajo pomanjkanje (vsaj delno)	166	70,6	0,5	<0,001
ne zaznavajo pomanjkanja	69	29,4		

Ugotovitev, da je zaznavanje pomanjkanja splošna značilnost slovenskega organizacijskega prostora, je skladna z evropskimi analizami, kot je npr. ECSF [4], ki opozarjajo, da gre za strukturni in ne zgolj začasni primanjkljaj.

Z vidika kadrovske politike rezultati jasno nakazujejo, da posamezne organizacije same ne bodo mogle preseči vrzeli med potrebami in ponudbo. Potrebni so usklajeni sistemski ukrepi, ki vključujejo sodelovanje izobraževalnega sistema, državnih organov in gospodarstva. Dolgoročna kadrovska strategija mora obsegati usmerjeno krepitev strokovnih kompetenc, večjo prepoznavnost kibernetskih poklicev med mladimi ter prilagajanje izobraževalnih programov dejanskim potrebam trga.

Ker zaznano pomanjkanje presega posamezne sektorje in tipe organizacij, predstavlja le-to horizontalen problem slovenskega gospodarstva. To razu-



Slika 2: **Porazdelitev odgovorov na vprašanje »Ali v vaši organizaciji zaznavate pomanjkanje ustrezno usposobljenega in kompetentnega kadra s področja informacijske/kibernetske varnosti?« (n = 235).**

mevanje mora postati izhodišče za oblikovanje ukrepov, ki bodo omogočili stabilno in dolgoročno vzdržno kompetenčno osnovo za kibernetsko varnost.

3.4 Razlike v zaznavanju pomanjkanja ustrezno usposobljenega in kompetentnega kadra glede na lastništvo organizacije

V sklopu RV3 smo nadalje želeli ugotoviti, ali se povprečna ocena zaznave pomanjkanja ustrezno usposobljenega in kompetentnega kadra s področja informacijske/kibernetske varnosti razlikuje glede na tip lastništva organizacije (javno, zasebno, mešano). Za analizo smo uporabili isto vprašanje iz anketnega vprašalnika kot pri analizi RV2 v prejšnjem poglavju.

Opisne statistike (tabela 4) kažejo, da so javne organizacije v povprečju višje ocenile zaznano pomanjkanje kadra (M=2,45; SD=0,75) kot zasebne (M=1,79; SD=0,69) in mešane (M=1,73; SD=0,61) organizacije. Tudi 95 % intervali zaupanja nakazujejo, da so razlike med javnimi organizacijami in ostalimi tipi organizacij precej izrazite.

Tabela 4: **Opisne statistike za oceno zaznavanja pomanjkanja kadra glede na lastništvo organizacije (n = 235).**

Lastništvo organizacije	*n*	*M*	*SD*	95% interval zaupanja
javna	73	2,45	0,75	2,28 – 2,63
zasebna	125	1,79	0,69	1,67 – 1,91
mešana	37	1,73	0,61	1,53 – 1,93
skupaj	**235**	**1,99**	**0,76**	**1,89 – 2,08**

Da bi preverili, če so zaznane razlike med skupinami statistično značilne, smo uporabili enosmerno analizo variance (ANOVA). Pred izvedbo ANOVE smo preverili predpostavko homogenosti varianc s pomočjo Levenovega testa homogenosti varianc. Rezultati testa homogenosti varianc (F(2,232)=2,467, p=0,087>0,05) so pokazali, da ničelne domneve o enakosti varianc ne moremo zavrniti pri 5% tveganju, kar pomeni, da lahko nadaljujemo z interpretacijo tabele ANOVA (tabela 5).

Tabela 5: **Rezultati enosmerne analize variance ANOVA za potrebe analize RV3**

	Vsota kvadratov	*df*	Povprečni kvadrat	*F*	*p*	η^2
med skupinami	22,990	2	11,495	23,82	<0,001	0,17
znotraj skupin	111,971	232	0,483			
skupaj	**134,962**	**234**				

Rezulati analize ANOVA potrdjujo, da so razlike v povprečnih ocenah zaznavanja pomanjkanja kadra v proučevanih organizacijah statistično značilne, saj je p<0,001. Vrednost koeficienta η^2=0,17 kaže na srednje velik učinek, kar pomeni, da lastništvo organizacije razmeroma močno vpliva na zaznavanje kadrovskega pomanjkanja. Na podlagi teh rezultatov na RV3 lahko odgovorimo pritrdilno.

Rezultati torej dokazujejo, da je pomanjkanje usposobljenega kadra najbolj izrazito v javnem sektorju, kar lahko odraža omejitve v fleksibilnosti zaposlovanja, dolgotrajne postopke in manj konkurenčne plače v primerjavi z zasebnim sektorjem.

Ugotovitve tako odpirajo pomembna strateška vprašanja. Če lastniška struktura organizacije pomembno vpliva na zaznavanje razpoložljivosti kadrov, potem je treba pri oblikovanju ukrepov za reševanje kadrovske vrzeli upoštevati heterogenost organizacijskega okolja. Sistemski ukrepi naj bodo diferencirani glede na tip organizacije in naj vključujejo podporne mehanizme za tiste, ki imajo pri dostopu do kadrov večje omejitve. Le tako bo mogoče ustvariti pravične in učinkovite pogoje za dolgoročno kadrovsko vzdržnost slovenskega digitalnega prostora.

3.5 Povezanost strateškega pristopa k informacijski/kibernetski varnosti in zaznavanja pomanjkanja ustreznega kadra na tem področju

RV4 temelji na predpostavki, da organizacije, ki informacijsko/kibernetsko varnost razumejo kot strateško prioriteto, bolje razumejo potrebe po zagotavljanju kompetentnega kadra, so na tem področju bolj proaktivne in posledično v večji meri zaznavajo pomanjkanje ustreznega in kompetentnega kadra.

Da bi naše predvidevanja preverili, smo izvedli analizo, ki je temeljila na preseku dveh dimenzij: (1) oceni, v kolikšni meri vodstvo organizacije obravna-

va varnost kot strateško pomembno temo, ter (2) stopnji zaznanega pomanjkanja usposobljenega kadra s področja informacijske/kibernetske varnosti. Za preverjanje povezanosti med spremenljivkama smo uporabili hi-kvadrat (χ^2) test.

Kot je povedano že v poglavju 3.2, so anketirani na vprašanje, če v organizaciji zaznavajo pomanjkanje ustrezno usposobljenega in kompetentnega kadra s področja informacijske/kibernetske varnosti, odgovarjali na 3 - stopenjski lestvici (1 – ne, 2 - delno, 3 - da). Na vprašanje, če vodstvo njihove organizacije obravnava informacijsko/kibernetsko varnost kot strateško pomembno področje, pa so anketiranci odgovarjali na 5 stopenjski lestvici:

1. Ne, informacijska/kibernetska varnost nista obravnavani kot strateška tema.
2. Deloma, o informacijski/kibernetski varnosti se pri nas občasno razpravlja, a področji nista vključeni v strateške dokumente.
3. Zmerno, informacijska/kibernetska varnost ima nekaj strateške teže, vendar (še) ni integrirana v širše poslovne cilje organizacije.
4. V veliki meri, vodstvo priznava pomen informacijske/kibernetske varnosti in ju vključuje v strateške razprave.
5. V celoti, informacijska/kibernetska varnost je jasno prepoznana kot strateška prioriteta in redno vključena v odločanje na najvišji ravni.

Kontingenčno tabelo kakor tudi rezultate χ^2 testa prikazuje tabela 6. Razvidno je, da organizacije, ki v celoti (kategorija 5) razumejo informacijsko/kibernetsko varnost kot strateško prioriteto, v polovici primerov (50,0 %) poročajo o vsaj delnem pomanjkanju kadra, medtem ko jih 50,0 % meni, da pomanjkanja ni. Pri organizacijah, ki varnost obravnavajo v veliki meri (kategorija 4), je delež organizacij z vsaj delnim pomanjkanjem nekoliko višji (52,0 %). Organizacije, ki varnost obravnavajo zmerno ali manj, pogosteje poročajo, da pomanjkanja ni ali da je le delno prisotno. Najmanj zaznanega pomanjkanja je pri organizacijah, ki varnosti ne obravnavajo strateško (kategorija 1). Rezultati χ^2 testa nadalje kažejo na statistično značilno povezanost med proučevanima veličinama ($\chi^2 = 59, 417$; $df = 8$; $p < 0{,}001$). Za oceno moči povezanosti smo izračunali še Cramérjev V, ki je enak 0,36. Ta vrednost kaže na zmerno močno povezavo med izbranima spremenljivkama.

Tabela 6: **Kontingenčna tabela in rezultati χ^2-testa za potrebe analize RV4**

		Zaznavanje pomanjkanja ustrezno usposobljenega in kompetentnega kadra s področja informacijske/kibernetske varnosti			
		1 – ne	2 – delno	3 – da	skupaj
Strateški pristop k informacijski/ kibernetski varnosti	1 – ne	7	10	1	18
	2 – deloma	4	8	14	26
	3 – zmerno	2	17	27	46
	4 – v veliki meri	21	36	18	75
	5 – v celoti	35	29	6	70
	skupaj	69	100	66	235

Rezultati χ^2-testa: $\chi^2 = 59{,}417$; $df = 8$; $p < 0{,}001$

Povzamemo torej lahko, da strateški pristop organizacij k informacijski/kibernetski varnosti vpliva na njihovo zaznavanje kadrovskih vrzeli. Bolj kot je varnost razumljena kot strateška prioriteta, večja je verjetnost, da organizacije zaznajo vsaj delno pomanjkanje ustrezno usposobljenega kadra. Ugotovitve torej kažejo, da je strateški odnos do informacijske/kibernetske varnosti več kot zgolj izraz zrelosti organizacijskega upravljanja, gre tudi za pomemben dejavnik pri oblikovanju in ohranjanju notranjih kadrovskih zmogljivosti. Organizacije, ki varnost integrirajo v strateške cilje, prej prepoznajo potrebe po kadrovskem razvoju, proaktivno načrtujejo izobraževanja ter bolj sistematično gradijo kompetenčne baze. Po drugi strani organizacije z manj razvitim strateškim pristopom tega pomanjkanja bodisi ne zaznavajo bodisi ga zaznavajo le delno, morda zaradi manjše osredotočenosti na kadrovske vidike varnosti. Tudi na RV4 torej lahko odgovorimo pritrdilno.

Naše ugotovitve imajo pomembne implikacije za slovenski kontekst, kjer večina organizacij deluje v okoljih z omejenimi viri in pomanjkanjem specializiranega kadra. Rezultati nakazujejo, da je eden izmed načinov za ublažitev kadrovske vrzeli ravno v tem, da se varnost ne obravnava zgolj kot tehnična naloga, temveč kot integralni del organizacijske strategije.

3.6 Ključne ovire pri razvoju kompetenc na področju informacijske in kibernetske varnosti

V sklopu analize RV5 smo želeli proučiti, katere zaviralne dejavnike organizacije zaznavajo kot najbolj problematične pri zagotavljanju, usposabljanju in ohranjanju kompetentnega kadra. Anketirancem smo ponudili 8 možnih odgovorov, pri čemer so anketiranci lahko izbrali največ 3 možnosti.

Rezultati deskriptivne analize odgovorov so prikazani v tabeli 7 in kažejo, da organizacije najpogosteje prepoznavajo naslednje tri ovire:

- pomanjkanje ustrezno usposobljenega kadra na trgu dela (64,4 % primerov),
- pomanjkanje sredstev za kadrovanje ali najem zunanjih strokovnjakov (50,6 %),
- velika fluktuacija in težave pri zadrževanju kadrov (47,8 %).

Manj pogosto so bile izpostavljene ovire, kot so nezadostna ponudba ali visoka cena izobraževanj ter nizka ozaveščenost vodstva.

Da bi bolje razumeli medsebojne povezave med ovirami, je bila izvedena faktorska analiza (metoda glavnih komponent z Varimax rotacijo), ki je potrdila prisotnost štirih latentnih dimenzij:

- **Faktor 1:** Organizacijska podpora in kultura, ki vključuje ovire, kot sta pomanjkanje načrtnega razvoja kompetenc znotraj organizacije in nizka ozaveščenost vodstva o pomenu kibernetske varnosti.
- **Faktor 2:** Zunanji viri in stroški, kamor sodijo visoki stroški ali nezadostna ponudba zunanjih izobraževanj.
- **Faktor 3:** Nestabilnost kadra, ki zajema pomanjkanje strokovnega kadra na trgu dela in visoko fluktuacijo zaposlenih.
- **Faktor 4:** Šibka notranja motivacija, ki odraža predvsem nizko motivacijo zaposlenih za pridobivanje dodatnih znanj.

Kaiser-Meyer-Olkinov indikator je bil 0,388, kar opozarja na šibkejšo povezljivost spremenljivk, vendar je Bartlettov test sferičnosti bil statistično značilen ($\chi^2 = 127{,}14$; $df=28$; $p<0{,}001$), kar upravičuje izvedbo faktorske analize. Identificirani faktorji pojasnjujejo 66,5 % skupne variance. Celotni rezultati faktorske analize so podani v magistrski nalogi [20].

Ugotovitve potrjujejo, da so ovire pri razvoju kompetenc na področju informacijske/kibernetske varnosti večdimenzionalne in pogosto medsebojno prepletene. To pomeni, da se organizacije ne soočajo zgolj z enim tipom izzivov temveč s kombinacijo ekonomskih, organizacijskih in kulturnih dejavnikov. Takšen vpogled ponuja uporabno osnovo za oblikovanje ukrepov na ravni organizacij, sektorjev in državnih politik.

Tabela 7: **Zaznane ovire pri razvoju kompetenc na področju informacijske in kibernetske varnosti**

Ovire pri razvoju kompetenc na področju informacijske in kibernetske varnosti	Št. odgovorov (n)	Delež glede na vse odgovore (%)	Delež anketirancev, ki so izbrali to možnost (%)
pomanjkanje ustrezno usposobljenega kadra na trgu dela	116	25,8	64,4
pomanjkanje sredstev za kadrovanje ali najem zunanjih strokovnjakov	91	20,3	50,6
velika fluktuacija strokovnjakov, težave pri zadrževanju kompetentnih kadrov (npr. majhno podjetje, neatraktivna regija ipd.)	86	19,2	47,8
pomanjkanje motivacije zaposlenih za pridobivanje dodatnih znanj	48	10,7	26,7
pomanjkanje načrtnega pristopa k lastnemu razvoju kompetenc znotraj organizacije	48	10,7	26,7
predraga ponudba zunanjih izobraževanj	26	5,8	14,4
nizka ozaveščenost vodstva o pomenu kibernetske varnosti	20	4,5	11,1
nezadostna ponudba zunanjih izobraževanj	14	3,1	7,8
skupaj	**449**	**100**	**249,4***

Opomba: Ker je bilo možnih več odgovorov, skupni % primerov presega 100 % Posamezni anketiranec je lahko označil več različnih ovir, zato je vključen v izračun odstotkov pri več postavkah.

3.7 Vpliv regulative na dodatne kadrovske ukrepe na področju informacijske in kibernetske varnosti

Uvedba nacionalnega ZInfV-1 in evropske Direktive NIS2 predstavlja pomemben institucionalni okvir za dvig ravni informacijske/kibernetske varnosti v slovenskih organizacijah [32]. Oba predpisa določata obveznosti za tako imenovane »zavezance«, ki so glede na svojo vlogo v digitalni družbi dolžni izvajati konkretne tehnične, organizacijske in kadrovske ukrepe. V tem kontekstu zakonodaja ne deluje le kot normativna zahteva, temveč vse bolj kot dejanski dejavnik oblikovanja kadrovskih strategij.

V sklopu RV6 smo tako želeli preveriti, ali sta status zavezanca po ZInfV-1 ali NIS2 in izvajanje dodatnih kadrovskih ukrepov na področju informacijske/kibernetske varnosti povezani veličini. Primerjali smo organizacije, ki so se identificirale kot zavezanci po ZInfV-1/NIS2 (pomembni ali bistveni subjekti), z organizacijami, ki tega statusa nimajo.

Za preverjanje povezanosti med statusom zavezanca in potrebo po izvajanju dodatnih kadrovskih ukrepov smo uporabili χ^2 test povezanosti. Rezultati, prikazani v tabeli 8, kažejo, da se je statistično značilna povezanost (p=0,022<0,05) pokazala le pri povečani potrebi po dodatnih znanjih in usposabljanjih obstoječih zaposlenih. To pomeni, da organizacije, ki spadajo med zavezance po ZInfV-1/NIS2, pogosteje občutijo potrebo po izvajanju ciljno usmerjenih internih izobraževanj za izboljšanje kompetenc obstoječega kadra. Da bi ugotovili moč povezanosti, smo izračunali še Cramérjev V, ki je enak 0,22 in dokazuje šibko do zmerno povezanost. Pri vseh ostalih navedenih potencialnih kadrovskih ukrepih (širitev ekipe, uvedba novih vlog, zunanje partnerstvo in okrepljena vloga vodstva) statistično značilne povezanosti nismo mogli potrditi. Na podlagi teh rezultatov lahko na RV6 odgovorimo le delno pritrdilno.

Za opažene vzorce obstajata vsaj dve razlagi. Prva je časovna komponenta: številne organizacije se zakonodaji šele prilagajajo in so še v začetni fazi uvajanja morebitnih dodatnih kadrovskih ukrepov. Druga razlaga je raznolikost v stopnji notranje zrelosti in upravljavske sposobnosti med organizacijami, kar vpliva na to, katere ukrepe so posamezne sposobne implementirati in katere ne.

Na tej osnovi lahko sklepamo, da zakonodaja v prvi fazi predvsem spodbuja kadrovske ukrepe, ki ne zahtevajo večjih sprememb organizacijske strukture, kot so dodatna interna usposabljanja. Vprašanje pa ostaja, ali bo zakonodajni pritisk dolgoročno spodbudil tudi širše organizacijske spremembe, kot so ustvarjanje novih varnostnih funkcij, sistematično načrtovanje kadrovskega razvoja in okrepljeno sodelovanje z zunanjimi strokovnjaki.

Z vidika oblikovanja politik to pomeni, da bi morala implementacija ZInfV-1 in NIS2 poleg nadzora nad skladnostjo vključevati tudi mehke ukrepe, kot so podpora vodstvom, svetovanje o kadrovski krepitvi ter usmerjanje organizacij v dolgoročno gradnjo internih zmogljivosti. Ob pričakovanem povečanju števila zavezancev bo ključno zagotoviti, da zakonodaja ne ostane zgolj formalna obveznost, temveč tudi vzvod za strateško upravljanje z znanji in kadri.

4 DISKUSIJA

Rezultati raziskave kažejo, da slovenske organizacije zaznavajo pomanjkanje kompetentnega kadra na področju informacijske/kibernetske varnosti kot resno in sistemsko oviro za dolgoročno digitalno odpornost. Povprečna ocena razpoložljivosti kadrov (2,74 na lestvici od 1 do 5) potrjuje ujemanje s svetovnimi trendi, kot jih navaja poročilo organizacije ISC² za leto 2024, kjer globalni primanjkljaj presega 4 milijone strokovnjakov [16]. Tudi Svetovni gospodarski forum (WEF) opozarja, da je pomanjkanje ustreznih

Tabela 8: **Rezultati χ^2 testa v sklopu analize RV6**

Potencialni dodatni kadrovski ukrep zaradi implementacije ZInfV-1 / NIS2	**Pearsonov χ^2 (df = 1)**	***p***	**Statistična značilnost**
Povečala se je potreba po dodatnem strokovnem kadru.	0,837	0,360	ne
Povečala se je potreba po dodatnih znanjih in usposabljanjih obstoječih zaposlenih.	**5,250**	**0,022**	**da**
Uvedli smo nove funkcije ali vloge (npr. CISO ipd.).	0,402	0,526	ne
Pogosteje sodelujemo z zunanjimi izvajalci.	0,402	0,526	ne
Okrepljena je bila vloga vodstva pri upravljanju informacijske/kibernetske varnosti.	0,007	0,935	ne

kadrov ena ključnih groženj kibernetski odpornosti na svetovni ravni [33]. Rezultati raziskave so pokazali, da pomanjkanje kadra bolj pesti javne organizacije kot pa zasebne ali mešane.

Poseben pomen ima ugotovitev, da organizacije, ki informacijsko/kibernetsko varnost obravnavajo kot strateško prioriteto, statistično značilno pogosteje zaznavajo pomanjkanje ustrezno usposobljenega in kompetentnega kadra, nakazuje na višjo stopnjo ozaveščenosti teh organizacij glede zahtev, ki jih postavlja učinkovito zagotavljanje varnosti. Takšne organizacije imajo praviloma bolje razvite procese, standarde in varnostne politike, zato tudi hitreje prepoznajo vrzeli v kadrovskih kompetencah. To pomeni, da je zaznavanje pomanjkanja kadra lahko tudi posledica višjih standardov in ambicij, ne zgolj objektivnega primanjkljaja, kar je pomembno upoštevati pri oblikovanju kadrovskih strategij in izobraževalnih programov. Slednje ugotovitve so povsem v skladu z izsledki v literaturi [21, 22].

Večdimenzionalna analiza ovir pri razvoju kompetenc na področju informacijske/kibernetske varnosti, ki vključuje tako strukturne kot organizacijske in sistemske dejavnike, potrjuje ugotovitve ENISA, ISACA in OECD, da se kompetenčne vrzeli ne pojavljajo le zaradi tržnega neravnotežja, temveč tudi zaradi pomanjkljive podpore vodstva, šibkih kadrovskih strategij ter slabe dostopnosti usposabljanj [23, 24, 34]. Rezultati faktorske analize so potrdili, da ovire nastopajo sočasno in v medsebojni odvisnosti, kar pomeni, da morajo biti rešitve prilagojene konkretnim tipom organizacij in sektorjem.

Analiza vpliva zakonodaje (ZInfV-1 in NIS2) na dodatne kadrovske ukrepe kaže, da je zakonodaja pomemben spodbujevalec, vendar trenutno vpliva predvsem na dodatna usposabljanja ne pa še na širše kadrovske premike. To je lahko posledica zgodnje faze implementacije, pomanjkanja institucionalne podpore ali dejstva, da številne organizacije še ne razpolagajo z notranjimi kapacitetami za prilagoditve. Primerjalne študije iz držav EU (npr. Finska, Nizozemska) kažejo, da so sistemski premiki mogoči predvsem tam, kjer zakonodajne zahteve spremljajo tudi spodbudne politike, javno sofinancirani programi in jasni kazalniki spremljanja učinkov [34, 35].

Menimo, da rezultati te raziskave predstavljajo dobro empirično podlago za oblikovanje nacionalnega kompetenčnega okvira, skladnega z ECSF, ki bi moral vključevati:

- razvoj standardov znanj in certifikatov na nacionalni ravni,
- oblikovanje spodbud za delodajalce v najbolj prizadetih sektorjih (npr. davčne olajšave za certificirana usposabljanja),
- vzpostavitev javno sofinanciranih programov kibernetskega izpopolnjevanja,
- vključitev kazalnikov kompetenčne razvitosti v nacionalne strategije (npr. Digitalna Slovenija, Nacionalni program kibernetske varnosti),
- boljše usklajevanje med akademsko sfero, gospodarstvom in državnimi organi (npr. preko javno-zasebnih partnerstev ali strateških svetov za kibernetsko odpornost).

Prav tako se odpira prostor za oblikovanje nacionalne podatkovne zbirke o stanju kadrovskih kapacitet na področju informacijske/kibernetske varnosti, ki bi omogočala redno spremljanje razkoraka med potrebami trga, izobraževalno ponudbo in dejansko zaposlenimi. Podoben pristop že razvijajo v nekaterih državah, kjer se kadrovski trendi spremljajo na podlagi centralnih kazalnikov in letnih poročil, kot na primer v okviru ameriške pobude Cybersecurity Workforce Data Initiative [36]. Takšna zbirka bi lahko služila kot podlaga za nadgradnjo obstoječih nacionalnih prizadevanj, saj so bile tudi v Sloveniji v zadnjih letih izvedene nekatere pomembne aktivnosti na področju kibernetske varnosti. Urad Republike Slovenije za informacijsko varnost (URSIV) je izdal *Priročnik kibernetske varnosti* [32], ki služi kot praktično vodilo za organizacije. Nacionalni odzivni center SI-CERT redno pripravlja letna poročila o incidentih [6], ki nudijo vpogled v aktualne grožnje in odzive. Državni svet RS je v svojih priporočilih [17] izpostavil potrebo po prilagoditvi izobraževalnega sistema realnim potrebam trga dela, medtem ko strateški dokument *Digitalna Slovenija 2030* opredeljuje krepitev kibernetske odpornosti kot eno od nacionalnih prioritet. Čeprav so ti ukrepi pomembni, ostajajo razpršeni in delno nepovezani, zato je oblikovanje enotnega nacionalnega kompetenčnega okvira še vedno nujno.

Za nadaljnje raziskave bi bilo smiselno izvesti longitudinalne študije, ki bi spremljale učinke zakonodaje in ukrepov skozi čas, ter razviti napovedne modele za potrebe po kompetencah, denimo s pomočjo simulacijskih tehnik, kot je sistemska dinamika. Tovrstni modeli bi omogočili tudi boljše strateško planiranje vlaganj in ciljno oblikovanje programov usposabljanja.

Raziskava ima nekaj omejitev, ki jih je treba upoštevati pri interpretaciji rezultatov. Vzorec, pridobljen prek strokovnih omrežij in partnerskih institucij, morda ni povsem reprezentativen za celotno populacijo slovenskih organizacij. Podatki temeljijo na samooceni, kar lahko vključuje subjektivne pristranskosti. Poleg tega so ugotovitve vezane na slovenski kontekst in časovno obdobje pred polno implementacijo zakonodajnih zahtev, kot je ZInfV-1 in NIS2, zato njihove pavšalne posplošitve na druge države ali kasnejša časovna obdobja niso povsem upravičene.

5 ZAKLJUČEK

Prispevek obravnava premalo raziskan a ključen vidik informacijske in kibernetske varnosti, kompetenčne vrzeli v slovenskih organizacijah. Rezultati empirične raziskave potrjujejo, da pomanjkanje usposobljenega kadra ni zgolj operativni problem posameznih organizacij, temveč odsev širših strateških, organizacijskih in sistemskih neravnovesij. Razkorak med potrebami trga, ponudbo izobraževalnega sistema in dejansko razpoložljivostjo kadra se kaže kot dolgoročna ovira za digitalno odpornost slovenskih organizacij.

Znanstveni doprinos članka je v konceptualni integraciji kompetenčnih potreb z regulativnim, organizacijskim in tržnim kontekstom. Na podlagi empiričnih podatkov članek ponuja večdimenzionalni vpogled v stanje kadrovskih kapacitet na področju informacijske/kibernetske varnosti v slovenskih organizacijah ter identificira ključne ovire in strateške razlike, ki vplivajo na zaznavo in obvladovanje kompetenčnih vrzeli. Ugotovitve potrjujejo, da so kompetenčne vrzeli v slovenskem prostoru večplastne, sistemsko pogojene in pogosto neodvisne od posameznih organizacij, zato zahtevajo usklajene odzive tako na ravni politike kot znotraj organizacij samih, vključno s sistematičnim načrtovanjem izobraževanja in usposabljanja na vseh ravneh.

Za oblikovalce politik rezultati predstavljajo pomembno podlago za razvoj nacionalnega kompetenčnega okvira, usklajenega z ECSF, ter pripravo sektorsko prilagojenih ukrepov tako od javno sofinanciranih programov usposabljanja do partnerstev med državo, gospodarstvom in akademskim okoljem. Nadaljnje raziskave naj se usmerijo v spremljanje dolgoročnih učinkov ukrepov, razvoj napovednih modelov ter sistemsko povezovanje empiričnih podatkov s strateškim načrtovanjem na državni ravni.

Trajnostna kibernetska odpornost bo v prihodnje mogoča le, če bo Slovenija svoje kompetenčne politike oblikovala na preverjenih podatkih o kadrovskih vrzelih, potrebah trga dela in učinkovitosti izobraževanj, ob jasnem sistemskem pristopu in dolgoročnem razvoju človeškega kapitala.

LITERATURA

[1] Uredba DORA – Digital Operational Resilience Act: regulativa za digitalno odpornost financ. (2025, 6. marec). iVarnost. https://ivarnost.si/dora-regulativa-za-digitalno-odpornost-financ/ (Dostopano dne: 6. avgust 2025)

[2] ENISA. (2023). Cybersecurity Threat Landscape 2023. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 (Dostopano dne: 1. april 2025)

[3] CEN. (2024). European eCompetence Framework (eCF): An Introduction to the Standard and its Ecosystem (v2). https://www.researchgate.net/publication/375765291 (Dostopano dne: 1. april 2025)

[4] ENISA. (n.d.). European Cybersecurity Skills Framework (ECSF). https://www.enisa.europa.eu/topics/skills-and-competences/skills-development/european-cybersecurity-skills-framework-ecsf (Dostopano dne: 1. april 2025)

[5] Ruoslahti, H., Coburn, J., Trent, A., and Tikanmäki, I. (2021). "Cyber Skills Gaps – A Systematic Review of the Academic Literature", Connections: The Quarterly Journal, vol. 20, no. 2, pp. 33–45, 2021 https://doi.org/10.11610/Connections.20.2.02 (Dostopano dne: 1. april 2025)

[6] SI-CERT. (2025). Kibernetska varnost 2024 v številkah. https://www.cert.si/kibernetska-varnost-2024-v-stevilkah/ (Dostopano dne: 28. junij 2025)

[7] Dalal, R. S., Howard, D. J., Bennett, R. J., Posey, C., Zaccaro, S. J., & Brummel, B. J. (2021). Organizational science and cybersecurity: Abundant opportunities for research at the interface. Current Opinion in Psychology, 41, 80–85. https://doi.org/10.1016/j.copsyc.2021.04.005 (Dostopano dne: 13. junija 2025)

[8] Vlada RS. (2025). Zakon o informacijski varnosti (ZInfV-1). Uradni list RS, št. 40/2025. https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2025-01-1571 (Dostopano dne: 20. junij 2025)

[9] Evropski parlament. (2023). Direktiva (EU) 2022/2555 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji (NIS2). https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX:32022L2555 (Dostopano dne: 20. junij 2025)

[10] Scholz, T., & Mayer, N. (2024). Towards a Research Agenda for the NIS2 Directive: Exploring Organisational and Compliance Challenges. arXiv preprint arXiv:2412.08084. https://arxiv.org/abs/2412.08084 (Dostopano dne: 11. junij 2025)

[11] Savin, A. (2024). NIS2 & Cybersecurity in Practice: Compliance Challenges. International In-house Counsel Journal, 17(69), 1–10. https://research.cbs.dk/en/publications/nis2-amp-cybersecurity-in-practice-compliance-challenges (Dostopano dne: 12. maj 2025)

[12] Ullah, F., Ye, X., Fatima, U., Akhtar, Z., Wu, Y., & Ahmad, H. (2025). What Skills Do Cyber Security Professionals Need? arXiv preprint arXiv:2502.13658. https://arxiv.org/abs/2502.13658 (Dostopano dne: 15. maj 2025)

[13] Kure, E., & Islam, N. (2022). Context-based and adaptive cybersecurity risk management framework. Risks, 11(6), 101.

https://www.mdpi.com/2227-9091/11/6/101 (Dostopano dne: 22. junij 2025)
[14] De Zan, T., & Di Franco, F. (2019). Cybersecurity skills development in the EU. ENISA – European Union Agency for Cybersecurity. https://millenniumedu.org/wp-content/uploads/2021/02/ENISA-Report-Cybersecurity-Skills-Development-in-the-EU.pdf (Dostopano dne: 22. junij 2025)
[15] OECD (2023), Building a Skilled Cyber Security Workforce in Five Countries: Insights from Australia, Canada, New Zealand, United Kingdom, and United States, OECD Skills Studies, OECD Publishing, Paris, https://doi.org/10.1787/5fd44e6c-en. (Dostopano dne: 22. junij 2025)
[16] ISC2. (2024). Cybersecurity Workforce Study 2024. https://edu.arrow.com/media/wtjfmszx/2024-isc2-wfs.pdf (Dostopano dne: 1. junij 2025)
[17] Državni svet RS. (2024). Kibernetska varnost zahteva odziven, realnim potrebam trga prilagojen izobraževalni sistem. Dostopno na: https://www.ds-rs.si/sl/novice/kibernetska-varnost-zahteva-odziven-realnim-potrebam-trga-prilagojen-izobrazevalni-sistem (Dostopano dne: 5. avgust 2025)
[18] BDO Global. (2024). Bridging the Cybersecurity Talent Gap: Augmenting human efforts with AI.https://www.bdo.si/getattachment/dc00d5b2-53ee-41a4-8013-6cdcc72e530e/Bridging-the-cybersecurity-talent-gap-TEDEN-4.pdf (Dostopano dne: 5. avgust 2025)
[19] Lesjak, D., Zwilling, M., & Klein, G. (2019). Cyber crime and cyber security awareness among students: A comparative study in Israel and Slovenia. Issues in Information Systems, 20(1), 80–87. https://doi.org/10.48009/1_iis_2019_80-87 https://iacis.org/iis/2019/1_iis_2019_80-87.pdf (Dostopano dne: 10. junij 2025)
[20] Markun, A., Kompetenčne potrebe slovenskih organizacij na področju kibernetske varnosti [magistrsko delo], Univerza v Mariboru, Fakulteta za organizacijske vede, 2025.
[21] Veale, M., & Brown, I. (2020). Cybersecurity. Internet Policy Review, 9(4). https://doi.org/10.14763/2020.4.1533 (Dostopano dne: 30. junij 2025)
[22] Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. arXiv preprint arXiv:2106.14701. https://arxiv.org/abs/2106.14701 (Dostopano dne: 1. julij 2025)
[23] Goupil, F., Laskov, P., Pekaric, I., Felderer, M., Dürr, A., & Thiesse, F. (2022). Towards understanding the skill gap in cybersecurity. Proceedings of ITiCSE '22. https://arxiv.org/abs/2204.13793 (Dostopano dne: 22. junij 2025)
[24] Ullah, F., Ye, X., Fatima, U., Akhtar, Z., Wu, Y., & Ahmad, H. (2025). What skills do cybersecurity professionals need? https://arxiv.org/abs/2502.13658 (Dostopano dne: 22. junij 2025)
[25] ENISA. (2022). European Cybersecurity Skills Framework – User Manual. https://www.enisa.europa.eu/sites/default/files/publications/European%20Cybersecurity%20Skills%20Framework%20User%20Manual.pdf (Dostopano dne: 22. junij 2025)
[26] National Institute of Standards and Technology – NIST. (2020). NICE Cybersecurity Workforce Framework (NIST SP 800-181 Rev. 1). https://doi.org/10.6028/NIST.SP.800-181r1 (Dostopano dne: 12. junij 2025)
[27] ENISA. (2020). Cybersecurity Skills Development in the EU. https://www.enisa.europa.eu/publications/cybersecurity-skills-development-in-the-eu (Dostopano dne: 12 junij 2025)
[28] Taherdoost, H. (2021). A Review on Risk Management in Information Systems: Risk Policy, Control and Fraud Detection. Electronics, 10(24), 3065. https://doi.org/10.3390/electronics10243065 (Dostopano dne: 26. junij 2025)
[29] Person, D., & Pareek, A. (2022). A qualitative study of human factors in cybersecurity: Beliefs, attitudes and behaviors. Cyberpsychology, Behavior, and Social Networking, 25(7), 450–456. https://www.liebertpub.com/doi/10.1089/cyber.2022.0191 (Dostopano dne: 3. julij 2025)
[30] Ruohonen, J. (2024). A Systematic Literature Review on the NIS2 Directive. arXiv preprint arXiv:2412.08084. https://arxiv.org/abs/2412.08084 (Dostopano dne: 3. julij 2025)
[31] National University Library. (2025). Partial Eta Squared – Statistics Resources. https://resources.nu.edu/statsresources/eta (Dostopano dne: 13. julij 2025)
[32] Urad Republike Slovenije za informacijsko varnost (URSIV). (2025). Priročnik kibernetske varnosti. https://www.gov.si/assets/vladne-sluzbe/URSIV/Datoteke/Prirocnik-kibernetske-varnosti.pdf (Dostopano dne: 12. junij 2025)
[33] World Economic Forum. (2024). Global Cybersecurity Outlook 2024. https://www.weforum.org/publications/global-cybersecurity-outlook-2024 (Dostopano dne: 22 junij 2025)
[34] OECD. (2024). Building a Skilled Cyber Security Workforce in Europe. OECD Skills Studies. https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/02/building-a-skilled-cyber-security-workforce-in-europe_6abaf769/3673cd60-en.pdf (Dostopano dne: 12. julij 2025)
[35] Ministry of Transport and Communications of Finland. (2024). Digital skills and competence strategy for Finland 2023–2030. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/165138/LVM_2024_5.pdf (Dostopano dne: 12. julij 2025)
[36] National Center for Science and Engineering Statistics. (2024). Cybersecurity Workforce Data Initiative. https://ncses.nsf.gov/initiatives/cybersecurity-workforce-data-initiative (Dostopano dne: 8. avgust 2025)

▪

Andreja Markun je magistrica organizatorka informatičarka, zaposlena na področju informacijske varnosti. V svoji raziskavi se ukvarja s sistemskimi pristopi k razvoju kibernetskih kompetenc, vplivom regulative na kadrovske ukrepe ter dolgoročno odpornostjo organizacij v digitalnem okolju.

▪

Alenka Brezavšček je izredna profesorica na Fakulteti za organizacijske vede Univerze v Mariboru, predstojnica Katedre za metodologijo. Doktorirala je na področju integralnega upravljanja kakovosti. Njeno raziskovalno delo vključuje operacijske raziskave, stohastične procese, zanesljivost in razpoložljivost sistemov, optimizacijo vzdrževanja ter informacijsko in kibernetsko varnost.