
Kibernetška odpornost v malih in srednje velikih podjetjih: desetletje raziskav, spoznanj in raziskovalnih vrzeli

VARSTVOSLOVJE
leto 2026
letn. 28
str. 1–30

Sara Horvat, Simon Vrhovec, Blaž Markelj

Namen prispevka:

Namen prispevka je preučiti vsebinske poudarke na področju informacijske in kibernetške varnosti ter kibernetške odpornosti malih in srednje velikih podjetij (MSP) v obdobju 2015–2025 ter ugotoviti zastopanost funkcij Ogrodja kibernetške varnosti Nacionalnega inštituta za standarde in tehnologijo (angl. *National Institute of Standards and Technology* – NIST) in domen korporativne arhitekture.

Metode:

Izveden je bil sistematični pregled literature v bibliografskih bazah *Scopus* in *Web of Science*. V končno analizo je bilo vključenih 97 znanstvenih člankov. Analizirane so bile ključne besede, funkcije NIST, primarne domene korporativne arhitekture in praktična validacija modelov oziroma ogrođij v primarnih raziskovalnih člankih.

Ugotovitve:

Analiza po časovnih obdobjih kaže različne vsebinske poudarke, med katerimi so standardi, upravljanje tveganj, informacijska varnost, kibernetška odpornost, digitalna preobrazba, človeški dejavniki in napredne tehnologije. Najpogostejše so zastopane funkcije upravljanje (86), identifikacija (60) in zaščita (59), redkeje pa zaznavanje (38), odzivanje (37) in okrevanje (34). Poslovna arhitektura prevladuje s 77 članki, sledijo tehnološka (11), aplikacijska (6) ter podatkovna arhitektura (3). Praktična validacija je bila ugotovljena pri 14 od 87 primarnih raziskovalnih člankov, vključenih v to analizo.

Omejitve/uporabnost raziskave:

Pregled je omejen na angleške znanstvene članke iz izbranih baz in obdobja. Analiza ugotavlja prisotnost funkcij, ne pa poglobljenosti njihove obravnave ali metodološke kakovosti posameznih raziskav.

Praktična uporabnost:

Ugotovitve usmerjajo razvoj uravnoteženih, modularnih in praktično izvedljivih modelov kibernetske odpornosti za MSP.

Izvirnost/pomembnost prispevka:

Prispevek povezuje analizo vsebinskih poudarkov po časovnih obdobjih, funkcij NIST, domen korporativne arhitekture in praktične validacije modelov oziroma ogrodij ter raziskovalcem in strokovnjakom ponuja strukturiran pregled ključnih vrzeli področja.

Ključne besede: mala in srednje velika podjetja (MSP), kibernetska odpornost, informacijska in kibernetska varnost, Ogradje kibernetske varnosti NIST, korporativna arhitektura, sistematični pregled literature

UDK: 005.934:004.056

Cyber Resilience in SMEs: A Decade of Research, Insights, and Gaps

Purpose:

This paper examines thematic emphases in information security, cybersecurity and cyber resilience in small and medium-sized enterprises (SMEs) from 2015 to 2025 and assesses the representation of National Institute of Standards and Technology [NIST] Cybersecurity Framework functions and Enterprise Architecture domains.

Design/Methods/Approach:

A systematic literature review was conducted using the *Scopus* and *Web of Science* databases. The final sample comprised 97 scientific articles. The analysis covered keywords, NIST functions, primary Enterprise Architecture domains, and the practical validation of models and frameworks in primary research articles.

Findings:

The analysis across time periods identifies different thematic emphases, including standards, risk management, information security, cyber resilience, digital transformation, human factors and advanced technologies. The most frequently represented functions are Govern (86), Identify (60) and Protect (59), while Detect (38), Respond (37) and Recover (34) receive less attention. Business Architecture dominates with 77 articles, followed by Technology Architecture (11), Application Architecture (6) and Data Architecture (3). Practical validation was identified in 14 of the 87 primary research articles included in this analysis.

Research Limitations/Implications:

The review is limited to English-language scientific articles indexed in the selected databases and published within the defined period. The analysis records the presence of functions but does not assess the depth of coverage or the methodological quality of individual studies.

Practical Implications:

The findings support the development of balanced, modular and practically feasible cyber-resilience models adapted to SME constraints.

Originality/Value:

The paper combines analysis of thematic emphases across time periods with mapping across NIST functions, Enterprise Architecture domains and practical validation, providing researchers and practitioners with a structured overview of major research gaps.

Keywords: small and medium-sized enterprises (SMEs), cyber resilience, information security and cybersecurity, NIST Cybersecurity Framework, Enterprise Architecture, systematic literature review

UDC: 005.934:004.056

1 UVOD

Mala in srednje velika podjetja (MSP) predstavljajo temelj gospodarstva Evropske unije. V Evropski uniji pomenijo 99 % vseh podjetij, skupaj zaposlujejo približno 100 milijonov ljudi in ustvarijo več kot polovico bruto domačega proizvoda (ENISA, 2024b). Hkrati so vse pogostejše tarče kibernetских napadov, zlasti kadar zaradi nižje stopnje kibernetске zrelosti predstavljajo vstopno točko do večjih poslovnih partnerjev. Posebej izpostavljena so MSP, vključena v regulirane sektorje, kritično infrastrukturo in digitalne dobavne verige (Tuteja, 2024).

Poročili družbe PwC (2024) in Svetovnega gospodarskega foruma (World Economic Forum, 2024) opozarjata na rast kibernetских napadov, katerih posledice vključujejo finančne izgube, škodo ugledu in pravno odgovornost. Med pomembnejšimi grožnjami za MSP so napadi z izsiljevalsko programsko opremo, ki lahko povzročijo resne poslovne in finančne posledice. Za zmanjševanje teh tveganj se predlagajo pristopi, ki povezujejo smernice ogrođja NIST in zavarovanje kibernetских tveganj (Mukhopadhyay in Jain, 2024).

Zagotavljanje kibernetске varnosti v MSP otežuje omejena finančna sredstva (Kiiveri idr., 2024), pomanjkanje specializiranega znanja (Arroyabe idr., 2024) ter razkorak med splošnimi informacijskotehnološkimi kompetencami in znanjem, potrebnim za učinkovito upravljanje kibernetских tveganj (Almeida, 2025). Kibernetске varnosti zato ni mogoče obravnavati zgolj kot vprašanje informacijske tehnologije, temveč kot poslovno in organizacijsko vprašanje, ki zahteva sodelovanje vodstva in zaposlenih (Hovav idr., 2023). Pomembno vlogo imata vedenje uporabnikov in varnostna kultura, saj vplivata na sposobnost organizacije, da preprečuje grožnje, kot je lažno predstavljanje, in se nanje ustrezno odziva (Nastjuk idr., 2025; European Digital Innovation Hubs Network, 2024).

Kljub vse večji odvisnosti od digitalnih tehnologij številna MSP še vedno ne vlagajo dovolj v kibernetско varnost (Kern idr., 2024). V primerjavi z velikimi organizacijami imajo manj notranjih virov za obrambo pred kibernetскими grožnjami (Clemente-Almendros idr., 2024; Radzi idr., 2024), vodstva pa se pogosto premalo zavedajo njihovega poslovnega pomena (Arroyabe idr., 2024).

Zaradi tega se podjetja močno zanašajo na zunanje izvajalce, kar lahko ob nizki notranji ravni znanja omeji njihovo sposobnost prilagajanja rešitev lastnim operativnim potrebam (Hoong idr., 2024).

Dodatno težavo predstavlja neprilagojenost številnih standardov in ogrodijski značilnostim MSP. Obstoječi pristopi so pogosto splošni, obsežni in zasnovani za večje organizacije, zato jih MSP težko izvajajo v celoti (Metin idr., 2024; Proudfoot idr., 2025). Njihova kompleksnost lahko vodi v površinsko ali razdrobljeno implementacijo (Almeida, 2025). Za MSP so zato primernejši modularni in prilagodljivi pristopi, ki omogočajo postopno uvajanje ukrepov ter uporabo digitalnih platform, interaktivnih orodij in samoocenjevalnih mehanizmov za prepoznavanje varnostnih vrzeli.

Pritisk na MSP povečujejo tudi nove evropske regulativne zahteve. Akt o kibernetski odpornosti določa zahteve glede varne zasnovе, posodabljanja in upravljanja ranljivosti proizvodov z digitalnimi elementi (Trujillo, 2024; Regulation (EU) 2024/2847, 2024), pri čemer spodbuja sorazmerne ukrepe, ki upoštevajo omejitve MSP (Szedlak idr., 2024; Goikoetxea, 2024). Direktiva NIS 2 pa obveznosti kibernetske varnosti razširja tudi na številna MSP, vključena v zagotavljanje kritičnih ali pomembnih storitev in digitalnih dobavnih verig (Directive (EU) 2022/2555, 2022). Ta podjetja morajo razviti zmogljivosti, sorazmerne svojemu poslovanju, vendar to pogosto počnejo brez jasnih sektorsko prilagojenih ogrodijskih in uveljavljenih dobrih praks (Barbour, 2024; Joswig in Kurz, 2025; ENISA, 2024a).

Namen prispevka je pridobiti vpogled v vsebinske poudarke raziskav na področju informacijske in kibernetske varnosti ter kibernetske odpornosti MSP ter preučiti, kako so v obstoječih pristopih zastopane različne razsežnosti kibernetske odpornosti. Pregled je bil zato usmerjen v modele in ogrodja, saj ti praviloma predstavljajo strukturirane pristope, ki omogočajo primerjavo njihove vsebinske pokritosti in prepoznavanje področij, ki so obravnavana bolj ali manj izrazito. Vsebinska pokritost je bila analizirana z vidika funkcij Ogrodja kibernetske varnosti NIST in domen korporativne arhitekture. Za uresničitev tega cilja so bila oblikovana naslednja raziskovalna vprašanja:

RV1: Kakšni so bili vsebinski poudarki v pregledanih pristopih k informacijski in kibernetski varnosti ter kibernetski odpornosti v malih in srednje velikih podjetjih v obdobju 2015–2025?

RV2: Katere vzorce je mogoče prepoznati v porazdelitvi pregledanih člankov med domenami korporativne arhitekture in funkcijami ogrodja NIST za kibernetsko varnost?

RV3: Katere teme so v pregledani literaturi dobro zastopane ter katere raziskovalne vrzeli in pomanjkljivo obravnavana področja je mogoče prepoznati?

Z odgovori na raziskovalna vprašanja prispevek zagotavlja strukturiran pregled vsebinskih poudarkov po časovnih obdobjih ter analizira porazdelitev literature med funkcijami ogrodja NIST in domenami korporativne arhitekture. Ugotovitve lahko usmerjajo prihodnje raziskave ter podprejo razvoj bolj uravnoteženih in praktično uporabnih modelov kibernetske odpornosti, prilagojenih potrebam in omejitvam MSP.

2 TEORETIČNO IZHODIŠČE

Prispevek obravnava informacijsko in kibernetsko varnost ter kibernetsko odpornost MSP. Ker se ti pojmi v literaturi pogosto uporabljajo nedosledno ali kot sopomenke, je treba pojasniti njihove razlike. Informacijska varnost zajema varovanje vseh oblik informacij pred nepooblaščenim dostopom, uporabo, razkritjem, spreminjanjem ali uničenjem. Njen temeljni cilj je zagotavljanje zaupnosti, celovitosti in razpoložljivosti informacij, pri čemer vključuje tudi fizično varnost, nadzor dostopa in kibernetsko varnost (Urad Vlade Republike Slovenije za informacijsko varnost, 2024). Kibernetska varnost je ožje usmerjena v zaščito omrežij, informacijskih sistemov in digitalnih podatkov pred kibernetskimi grožnjami. Obsega procese, tehnološke rešitve in prakse za preprečevanje incidentov ter omejevanje njihovih posledic (Olcott, 2024). Kibernetska odpornost pomeni sposobnost organizacije, da med kibernetskim incidentom ohrani ključne poslovne funkcije ter se nanj odzove in po njem okreva (King, 2023; Houghton, 2024; Olcott, 2024).

2.1 Ogradje NIST za kibernetsko varnost

NIST je prvo različico Ogradja kibernetske varnosti (angl. *cybersecurity framework* – CSF) objavil leta 2014, leta 2024 pa njegovo prenovljeno in razširjeno različico NIST CSF 2.0. Ogradje organizacijam zagotavlja strukturirane smernice za razumevanje, upravljanje in zmanjševanje kibernetskih tveganj ter izboljševanje njihove varnostne drže (NIST, 2024). Postalo je tudi referenčni model za razvoj drugih pristopov h kibernetski odpornosti (Breaker-Rolfe, 2024).

Ogradje temelji na šestih ključnih funkcijah, ki skupaj sestavljajo strateški pristop k upravljanju kibernetskih tveganj (NIST, 2024):

- **Identifikacija** (angl. *identify*): vzpostavitev celovitega razumevanja sistemov, sredstev, podatkov in zmogljivosti organizacije, kar omogoča učinkovito upravljanje tveganj;
- **Zaščita** (angl. *protect*): izvajanje zaščitnih ukrepov za zagotavljanje neprekinjenega izvajanja ključnih storitev in dejavnosti;
- **Zaznavanje** (angl. *detect*): razvoj postopkov za pravočasno prepoznavanje anomalij in morebitnih kibernetskih incidentov;
- **Odzivanje** (angl. *respond*): opredelitev in izvajanje ustreznih odzivnih dejavnosti po zaznavi kibernetskega dogodka;
- **Okrevanje** (angl. *recover*): vzpostavitev strategij za obnovitev prizadetih sistemov in storitev po incidentu ter izboljšanje odpornosti organizacije;
- **Upravljanje** (angl. *govern*): funkcija, uvedena v posodobitvi iz leta 2024, ki poudarja pomen upravljanja pri usklajevanju in podpori preostalih petih funkcij.

Vključitev funkcije *upravljanje* v različico iz leta 2024 poudarja pomen usklajevanja posameznih aktivnosti kibernetske varnosti v okviru širšega upravljanja tveganj in varnostne strategije organizacije (NIST, 2024; Heffer in Troskie, 2024).

2.2 Korporativna arhitektura

Korporativna arhitektura (angl. *enterprise architecture* – EA) zagotavlja sistematični okvir za povezovanje poslovne strategije, procesov, informacijskih sistemov in tehnološke infrastrukture. Organizacijam omogoča usklajevanje tehnoloških rešitev s strateškimi cilji, učinkovitejše razporejanje virov, zmanjševanje podvajanj ter podporo digitalni preobrazbi in organizacijski agilnosti (The Open Group, 2022).

Čeprav je bila prvotno razvita predvsem za velika podjetja, je uporabna tudi v MSP, kjer lahko podpira postopno uvajanje tehnologij, izboljševanje procesov in usmerjanje omejenih virov v rešitve, ki neposredno podpirajo poslovne cilje (White, 2022; Estarch, 2025).

Korporativna arhitektura vključuje štiri glavne domene (The Open Group, 2022):

- **Poslovna arhitektura:** osredotoča se na poslovno strategijo, upravljanje, organizacijsko strukturo in ključne poslovne procese.
- **Aplikacijska arhitektura:** opredeljuje aplikacije, ki se uporabljajo v organizaciji, ter analizira njihove medsebojne povezave in interakcije z uporabniki ter drugimi sistemi.
- **Tehnološka arhitektura:** dokumentira strojno, programsko in omrežno infrastrukturo, ki se uporablja v organizaciji.
- **Podatkovna arhitektura:** zajema zbiranje, shranjevanje, obdelavo, distribucijo in uporabo podatkov, vključno z upravljanjem politik na področju podatkov.

V raziskavi so bile funkcije NIST CSF 2.0 in domene korporativne arhitekture uporabljene kot komplementarni analitični dimenziji pri preučevanju kibernetske odpornosti. Funkcije NIST omogočajo analizo upravljanja, identifikacije, zaščite, zaznavanja, odzivanja in okrevanja, domene korporativne arhitekture pa omogočajo presojo, ali so ti vidiki obravnavani predvsem na poslovni, aplikacijski, tehnološki ali podatkovni ravni. Takšna kombinacija omogoča primerjavo funkcionalne in arhitekturne zastopanosti kibernetske odpornosti v pregledanih modelih in ogrojdih (NIST, 2024; The Open Group, 2022).

3 METODA

Izvedli smo sistematični pregled literature z namenom preučiti vsebinske poudarke po časovnih obdobjih ter analizirati vsebinsko pokritost modelov in ogrojdij na področju informacijske in kibernetske varnosti ter kibernetske odpornosti v MSP. Vključene znanstvene članke smo analizirali in razvrstili glede na domene korporativne arhitekture ter funkcije ogroджа NIST za kibernetsko varnost. Za vsak članek smo določili primarno domeno korporativne arhitekture in vse funkcije NIST, ki jih vsebinsko obravnavajo modeli oziroma ogroджа, ki jih prispevek razvija, predstavlja ali analizira. Pri primarnih raziskovalnih člankih smo dodatno preverili praktično validacijo predstavljenih modelov oziroma ogrojdij. Takšen pristop je omogočil primerjavo njihove vsebinske pokritosti ter prepoznavanje bolj in manj zastopanih področij.

Relevantne znanstvene članke smo pridobili iz bibliografskih baz *Scopus* in *Web of Science*. Začetno iskanje je bilo izvedeno 7. januarja 2026. Iskalna strategija je bila namensko usmerjena v raziskave, ki obravnavajo modele oziroma ogrodja na področju informacijske in kibernetske varnosti ter odpornosti v MSP. Vključeni so bili tako prispevki, ki razvijajo oziroma predstavljajo lastne modele ali ogrodja, kot tudi pregledni prispevki, ki analizirajo, primerjajo oziroma sintetizirajo obstoječe modele in ogrodja. Namen takšne zamejitve je bil identificirati strukturirane pristope, pri katerih je mogoče primerjalno analizirati vsebinsko pokritost posameznih razsežnosti kibernetske odpornosti. Obravnavane modele in ogrodja smo zato analizirali z vidika funkcij Ogrodja kibernetske varnosti NIST in domen korporativne arhitekture, kar je omogočilo prepoznavanje področij, ki so v obstoječih pristopih bolj ali manj zastopana.

Vključitvena in izključitvena merila sistematičnega pregleda literature so predstavljena v Tabeli 1.

Merilo	Vključitvena merila	Izključitvena merila
Obdobje objave	članki, objavljeni v obdobju 2015–2025	članki, objavljeni zunaj opredeljenega obdobja
Jezik	angleščina	drugi jeziki
Vrsta publikacije	znanstveni članek	druge vrste publikacij
Dostopnost	dostopno celotno besedilo	celotno besedilo ni dostopno
Preučevan subjekt	raziskave, ki obravnavajo mikro, mala in srednje velika podjetja	raziskave brez relevantnega konteksta malih in srednje velikih podjetij
Vsebinsko področje	informacijska varnost, kibernetska varnost, kibernetska odpornost ter digitalna odpornost, kadar je neposredno povezana z informacijskim ali kibernetskim področjem	druge oblike varnosti ali odpornosti brez neposredne povezave z informacijskim ali kibernetskim področjem
Vsebinska relevantnost	raziskava vsebinsko prispeva k obravnavi zagotavljanja informacijske ali kibernetske varnosti oziroma odpornosti MSP	prispevek se glede na naslov, povzetek ali celotno besedilo vsebinsko ne nanaša na zagotavljanje informacijske ali kibernetske varnosti oziroma odpornosti MSP
Raziskovalni pristop	prispevek razvija oziroma predstavlja lasten model ali ogrodje ali pa analizira, primerja oziroma sintetizira obstoječe modele ali ogrodja za obravnavo informacijske ali kibernetske varnosti oziroma odpornosti MSP	prispevek ne razvija oziroma predstavlja lastnega modela ali ogrodja in ne analizira, primerja oziroma sintetizira obstoječih modelov ali ogrodij za obravnavo informacijske ali kibernetske varnosti oziroma odpornosti MSP

Tabela 1

Vključitvena in izključitvena merila sistematičnega pregleda literature

Tabela 2 prikazuje uporabljeni bibliografski bazi, omejitve iskanja, število zadetkov in uporabljeni iskalni poizvedbi. Iskalni niz je povezoval izraze s področja informacijske in kibernetske varnosti ter odpornosti, modelov oziroma ogrodij in MSP.

Tabela 2
Iskalni ukaz in zadetki

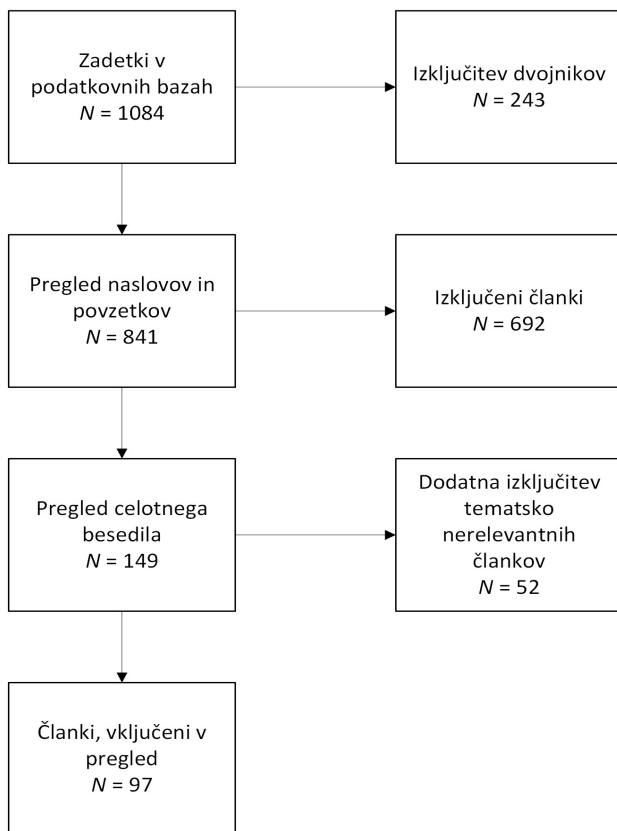
Baza znanstvene literature	Rezultati/filter/iskalni ukaz
Web of Science	384
Leta (od - do)	2015–2025
Vrsta publikacije	članek
Jezik	angleščina
Iskalna poizvedba	TS = ((„cyber security“ OR „cybersecurity“ OR „resilience“ OR „digital resilience“ OR „cyber resilience“ OR „cyberresiliency“ OR „cyber resiliency“ OR „resiliency“ OR „information security“ OR „informationsecurity“ OR „digital security“) AND („framework“ OR „model“) AND („SME“ OR „Small-sized“ OR „medium-sized“ OR „small and medium-sized“ OR „micro“) AND („business“ OR „entity“ OR „enterprise“ OR „company“))
Scopus	700
Leta (od - do)	2015–2025
Vrsta publikacije	članek
Jezik	angleščina
Iskalna poizvedba	TITLE-ABS-KEY ((„cyber security“ OR „cybersecurity“ OR „resilience“ OR „digital resilience“ OR „cyber resilience“ OR „cyberresiliency“ OR „cyber resiliency“ OR „resiliency“ OR „information security“ OR „informationsecurity“ OR „digital security“) AND („framework“ OR „model“) AND („SME“ OR „Small-sized“ OR „medium-sized“ OR „small and medium-sized“ OR „micro“) AND („business“ OR „entity“ OR „enterprise“ OR „company“))

Iskanje v bazah *Scopus* in *Web of Science* je vrnilo skupno 1.084 zapisov, od tega 700 v bazi *Scopus* in 384 v bazi *Web of Science*. Rezultate iskanja iz obeh bibliografskih baz smo izvozili in združili v enoten seznam v programu Microsoft Excel. Podvojene zapise smo identificirali na podlagi ujemanja DOI ter primerjave naslovov člankov in avtorjev. Potencialne dvojnike smo pred odstranitvijo dodatno ročno preverili, da bi upoštevali morebitne razlike v zapisu bibliografskih podatkov med bazama. Tako smo odstranili 243 podvojenih zapisov, za pregled naslovov, ključnih besed in povzetkov pa je ostalo 841 zapisov. V tej fazi smo na podlagi vključitvenih in izključitvenih meril iz Tabele 1 izločili 692 zapisov, zato je bilo v pregled celotnega besedila vključenih 149 člankov.

Velik del zapisov, izločenih v tej fazi, ni izpolnjeval merila vsebinske relevantnosti. Zaradi široko zastavljenega nabora iskalnih izrazov, povezanih z odpornostjo, so bili med zadetki tudi prispevki, ki so obravnavali finančno in ekonomsko odpornost, odpornost voditeljstva v različnih managerskih kontekstih, organizacijsko odpornost na naravne nesreče ter vpliv trajnostnih poslovnih praks na odpornost, vendar niso bili neposredno povezani z informacijsko ali kibernetiko oziroma kibernetiko odpornostjo MSP.

V naslednji fazi smo pregledali celotna besedila 149 člankov. Pri tem smo ponovno preverili njihovo skladnost z vključitvenimi in izključitvenimi merili iz Tabele 1. Pri delu prispevkov iz naslova, ključnih besed in povzetka ni bilo mogoče zanesljivo presoditi njihove vsebinske ustreznosti oziroma ugotoviti, ali dejansko razvijajo, predstavljajo, analizirajo, primerjajo oziroma sintetizirajo modele

oziroma ogrodja na obravnavanem področju, zato je bila ta presoja opravljena na podlagi celotnega besedila. Po tem pregledu smo izločili dodatnih 52 člankov. V končno analizo je bilo tako vključenih 97 znanstvenih člankov. Potek izbora člankov je prikazan na Sliki 1, seznam vseh vključenih člankov pa je dostopen v Prilogi A.



Slika 1
Potek izbora člankov v sistematičnem pregledu literature

Za analizo vsebinskih poudarkov po posameznih časovnih obdobjih smo uporabili avtorske ključne besede vključenih člankov. Pred analizo smo poenotili različne zapisne in slovnične oblike istega pojma, vključno z razlikami v velikosti začetnic, različnimi zapisi istih izrazov ter edninskimi in množinskimi oblikami. Če je bil isti normalizirani pojem v posameznem članku naveden večkrat, je bil evidentiran enkrat. Večbesedni izrazi so bili obravnavani kot posamezne pomenske enote.

Vključene članke smo nato vsebinsko kodirali glede na domene korporativne arhitekture in funkcije Ogrodja kibernetске varnosti NIST. Pri razvrščanju po domenah korporativne arhitekture je bil vsak članek uvrščen v eno primarno domeno: poslovno, aplikacijsko, tehnološko ali podatkovno arhitekturo. Primarna domena je bila določena glede na osrednji raziskovalni poudarek modelov oziroma ogrodij, ki jih je posamezni članek razvijal, predstavljal ali analiziral,

njihovo vsebino ter del organizacije oziroma poslovanja, ki so ga prvenstveno naslavljali.

Pri klasifikaciji po Ogorodju kibernetske varnosti NIST je bilo posameznemu članku mogoče pripisati več funkcij. Kodiranje je temeljilo na opredelitvah posameznih funkcij v NIST CSF 2.0. Za vsak članek smo ugotovili, katere od šestih funkcij (upravljanje, identifikacija, zaščita, zaznavanje, odzivanje in okrevanje) vsebinsko naslavljajo modeli oziroma ogrodja, ki jih prispevek razvija, predstavlja ali analizira. Posamezna funkcija je bila pri posameznem članku evidentirana največ enkrat, ne glede na obseg njene obravnave.

Za klasifikacijo vseh člankov je bila uporabljena aktualna različica NIST CSF 2.0 (NIST, 2024), tudi pri člankih, objavljenih pred njeno izdajo. S tem smo zagotovili enotno klasifikacijsko shemo za celotno analizirano obdobje. Posebno pozornost zahteva funkcija upravljanje (angl. *Govern*), ki je bila kot samostojna funkcija uvedena v različici CSF 2.0. NIST pojasnjuje, da vsebine upravljanja niso bile nove, saj so bile v različici CSF 1.1 vključene predvsem v funkcijo identifikacija, v CSF 2.0 pa so bile zaradi poudarjene vloge upravljanja kibernetskih tveganj prerazporejene v samostojno funkcijo upravljanje (NIST, 2024). Zato je bila funkcija upravljanje pripisana tudi starejšim člankom, kadar je vsebina modelov oziroma ogrodij, ki so jih obravnavali, ustrezala področjem, ki jih CSF 2.0 uvršča v to funkcijo.

Začetno kodiranje vseh vključenih člankov je izvedla prva avtorica. Primere, pri katerih razvrstitev glede na primarno domeno korporativne arhitekture ali posamezne funkcije NIST ni bila enoznačna, je označila kot mejne primere. Ti so bili nato pregledani in obravnavani skupaj s soavtorjema, končna razvrstitev pa je bila določena na podlagi skupne presoje. Ker vseh člankov ni neodvisno kodiralo več raziskovalcev, formalna zanesljivost oziroma stopnja skladnosti med raziskovalci, ki so kodirali, ni bila izračunana. Možne nejasnosti smo omejevali s predhodno določenimi klasifikacijskimi merili in skupno obravnavo mejnih primerov.

Klasifikacijska merila, uporabljena pri kodiranju člankov, so prikazana v Tabeli 3. Merila za domene korporativne arhitekture izhajajo iz štirih temeljnih domen korporativne arhitekture ter so bila za namen raziskave operacionalizirana glede na prevladujoči vsebinski poudarek modelov oziroma ogrodij, obravnavanih v posameznem članku (The Open Group, 2022). Merila za razvrščanje po funkcijah kibernetske varnosti temeljijo na opredelitvah šestih funkcij NIST CSF 2.0 (NIST, 2024). Tabela 3 tako predstavlja operativno kodirno shemo, uporabljeno za enotno razvrščanje vseh vključenih člankov.

Tabela 3
Operativna merila za klasifikacijo člankov glede na domene korporativne arhitekture in funkcije NIST CSF 2.0

Tip klasifikacije	Domena oziroma funkcija	Merilo za razvrščanje
Domena korporativne arhitekture	Poslovna arhitektura	Model oziroma ogrodje je primarno usmerjeno v poslovno strategijo, upravljanje, organizacijsko strukturo, poslovne procese, politike, odgovornosti ali druge organizacijske vidike.
	Aplikacijska arhitektura	Model oziroma ogrodje je primarno usmerjeno v aplikacije, njihove funkcije in medsebojne povezave ter podporo poslovnim funkcijam in upravljanju podatkov.

	Tehnološka arhitektura	Model oziroma ogrodje je primarno usmerjeno v tehnološko infrastrukturo, platforme, omrežja, strojno in programsko opremo oziroma druge tehnološke komponente.
	Podatkovna arhitektura	Model oziroma ogrodje je primarno usmerjeno v podatke oziroma informacije, njihovo strukturo, zbiranje, upravljanje, uporabo, izmenjavo ali druge vidike podatkovnega okolja.
Funkcija NIST CSF 2.0	Identifikacija	Model oziroma ogrodje obravnava razumevanje trenutnih kibernetских tveganj organizacije, vključno s sredstvi, dobavitelji, grožnjami, ranljivostmi in tveganji.
	Zaščita	Model oziroma ogrodje obravnava zaščitne ukrepe za obvladovanje kibernetских tveganj in zmanjševanje verjetnosti oziroma posledic kibernetских dogodkov.
	Zaznavanje	Model oziroma ogrodje obravnava spremljanje in prepoznavanje anomalij, indikatorjev kompromisa oziroma drugih znakov potencialnih kibernetских dogodkov ali incidentov.
	Odzivanje	Model oziroma ogrodje obravnava dejavnosti za obvladovanje zaznanega kibernetского incidenta, vključno z analizo, komunikacijo, omejevanjem posledic in drugimi odzivnimi dejavnostmi.
	Okrevanje	Model oziroma ogrodje obravnava obnovitev prizadetih sredstev, storitev ali dejavnosti ter ponovno vzpostavitev normalnega delovanja po kibernetском incidentu.
	Upravljanje	Model oziroma ogrodje obravnava strategijo upravljanja kibernetских tveganj, organizacijski kontekst, vloge in odgovornosti, politike, nadzor ali upravljanje tveganj dobavne verige.

Praktično validacijo smo analizirali pri 87 primarnih raziskovalnih člankih, ki so razvijali oziroma predstavljali lasten model ali ogrodje. Deset preglednih člankov, katerih namen je bil analiza oziroma sinteza obstoječih modelov in ogrodij, smo iz analize praktične validacije izključili, saj pri njih praktična validacija lastnega modela oziroma ogrodka ni bila relevantno merilo. Kot praktično validacijo smo šteli dejansko uporabo, preizkus, implementacijo ali evalvacijo predstavljenega modela oziroma ogrodka v podjetju ali drugem realnem organizacijskem okolju.

4 REZULTATI IN DISKUSIJA

Rezultati so predstavljeni glede na tri raziskovalna vprašanja. Vsebinski poudarki po časovnih obdobjih so analizirani na podlagi normaliziranih ključnih besed avtorjev, besedni oblaki pa so uporabljeni kot dopolnilna vizualna predstavitev. Izdelani so v spletni aplikaciji *WordClouds.com*. Pri tej vrsti vizualizacije so pogostejše uporabljeni izrazi prikazani z večjo pisavo. Za odgovor na drugo in tretje raziskovalno vprašanje so bili članki razvrščeni glede na funkcije Ogrodka kibernetiske varnosti NIST in primarne domene korporativne arhitekture, kar je omogočilo primerjavo njihove funkcionalne in arhitekturne zastopanosti.

Slika 2 prikazuje besedni oblak normaliziranih ključnih besed avtorjev iz analiziranih člankov. Ključne besede so bile pred analizo poenotene glede na različne zapisne in slovnične oblike istega pojma, večbesedni izrazi pa so bili obravnavani kot posamezne pomenske enote. Med 97 vključenimi članki sta bila dva brez navedenih avtorskih ključnih besed, zato analiza ključnih besed vključuje 95 člankov in 530 normaliziranih pojavitev ključnih besed. Velikost posameznega izraza je sorazmerna s pogostostjo njegove uporabe.

Slika 2
*Besedni oblak
normaliziranih
avtorskih
ključnih besed
analiziranih
člankov v
obdobju
2015–2025*



Najpogostejša ključna beseda je »SME« ($N = 54$), saj so MSP predstavljala predmet pregleda. Med vsebinskimi izrazi so najpogostejši še »cybersecurity« ($N = 44$), »information security« ($N = 15$), »risk management« ($N = 11$), »cyber resilience« ($N = 6$), »cybersecurity awareness« ($N = 6$), »resilience« ($N = 6$) in »risk assessment« ($N = 5$). To kaže na osrednjo vlogo kibernetske in informacijske varnosti ter na povezanost pregledanih pristopov z upravljanjem tveganj in odpornostjo.

Za pregled vsebinskih poudarkov po časovnih obdobjih so bile ključne besede razvrščene v pet dvoletnih obdobj. V letu 2015 ni bilo vključenih člankov, zato se analiza začne z letom 2016. Tabela 4 prikazuje število vključenih člankov, razpoložljivost ključnih besed in obseg normaliziranih pojavitev po posameznih obdobjih.

Obdobje	Vključeni članki	Članki s ključnimi besedami	Normalizirane pojavitve	Povprečno na članek ¹
2016–2017	4	4	27	6,75
2018–2019	6	6	36	6,00
2020–2021	23	22	123	5,59
2022–2023	25	25	126	5,04
2024–2025	39	38	218	5,74
Skupaj	97	95	530	5,58

Tabela 4
Obseg analize ključnih besed po dvoletnih obdobjih

Število vključenih člankov se je skozi opazovana obdobja povečevalo, medtem ko je povprečno število ključnih besed na članek ostalo razmeroma stabilno in se je gibalo med 5,04 in 6,75. Ker se število vključenih člankov med obdobji razlikuje, analiza ne ocenjuje relativnega naraščanja ali upadanja posameznih tem med obdobji, temveč deskriptivno predstavlja vsebinske poudarke znotraj posameznih obdobji. V nadaljevanju so zato predstavljeni najpogostejše zastopani izrazi in vsebinski poudarki znotraj posameznih obdobji. Besedni oblaki na Sliki 3 dopolnjujejo pregled z vizualnim prikazom najizrazitejših vsebinskih poudarkov po obdobjih.

Slika 3
Besedni oblaki normaliziranih avtorskih ključnih besed po dvoletnih obdobjih



V obdobju 2016–2017 so bili med vsebinskimi poudarki predvsem informacijska varnost, standardi, sistemi upravljanja informacijske varnosti in ocenjevanje tveganj. V obdobju 2018–2019 so med vsebinskimi poudarki modeli zrelosti, varstvo osebnih podatkov, kibernetско zavarovanje ter organizacijski in vedenjski dejavniki, kot so podpora vodstva, izobraževanje in izmenjava znanja.

¹ Povprečno število normaliziranih pojavitev ključnih besed na članek z navedenimi ključnimi besedami.

V obdobju 2020–2021 so med vsebinskimi poudarki kibernetska odpornost, neprekinjeno poslovanje, modeli zrelosti in podpora odločanju. Prisotne pa so tudi tehnološke teme, povezane s strojnim učenjem, umetno inteligenco in zaznavanjem vdorov. V obdobju 2022–2023 so med vsebinskimi poudarki kibernetska ozaveščenost in usposabljanje, dobavne verige, neprekinjeno poslovanje, notranje grožnje ter družbeno-tehnični pristopi.

V obdobju 2024–2025 so med vsebinskimi poudarki upravljanje kibernetskih tveganj, digitalna preobrazba, upravljanje kibernetske varnosti, kibernetska ozaveščenost in organizacijska odpornost. Med tehnološkimi poudarki so prisotni umetna inteligenca, arhitektura ničelnega zaupanja, večfaktorsko preverjanje pristnosti in mikrosegmentacija.

4.2 RV2: Katere vzorce je mogoče prepoznati v porazdelitvi pregledanih člankov med domenami korporativne arhitekture in funkcijami ogrodja NIST za kibernetsko varnost?

V nadaljevanju je prikazana porazdelitev pregledanih člankov glede na funkcije Ogrodja kibernetske varnosti NIST in primarne domene korporativne arhitekture. Analiza omogoča primerjavo zastopanosti posameznih funkcij in arhitekturnih domen.

Porazdelitev člankov glede na število in kombinacije šestih funkcij Ogrodja kibernetske varnosti NIST je predstavljena v Tabeli 5. Posamezen članek je lahko obravnaval več funkcij, zato analiza prikazuje širino njihove zastopanosti v pregledanih člankih.

Vseh šest funkcij je obravnavalo 16 od 97 člankov. Največ člankov je obravnavalo tri funkcije (32), sledijo članki z dvema (20) in eno funkcijo (14), medtem ko je pet funkcij obravnavalo 8, štiri pa 7 člankov. Pri vseh 14 člankih, ki so obravnavali samo eno funkcijo, je bila ta funkcija *upravljanje*. Vseh šest funkcij je bilo tako zastopanih pri manjšem delu pregledanih člankov.

Ogrodje kibernetске varnosti NIST						Skupaj	Tabela 5 Porazdelitev znanstvenih čankov po funk- cijah Ogrodja NIST
Identifikacija	Zaščita	Zaznavanje	Odzivanje	Okrevanje	Upravljanje		
✓	✓	✓	✓	✓	✓	16	
Članki z vsemi šestimi funkcijami = 16							
✓	✓	✓	✓	✓		3	
✓	✓		✓	✓	✓	2	
✓		✓	✓	✓	✓	2	
✓	✓	✓	✓		✓	1	
Članki s petimi funkcijami = 8							
✓	✓	✓			✓	2	
		✓	✓	✓	✓	1	
✓	✓		✓		✓	1	
✓	✓			✓	✓	1	
✓			✓	✓	✓	1	
✓		✓	✓	✓		1	
Članki s štirimi funkcijami = 7							
✓	✓				✓	17	
			✓	✓	✓	4	
	✓	✓			✓	3	
	✓	✓	✓			2	
✓		✓			✓	2	
✓	✓	✓				1	
✓				✓	✓	1	
	✓		✓		✓	1	
✓		✓	✓			1	
Članki s tremi funkcijami = 32							
✓					✓	8	
	✓				✓	7	
				✓	✓	2	
	✓	✓				2	
		✓	✓			1	
Članki z dvema funkcijama = 20							
					✓	14	
Članki z eno funkcijo = 14							
Skupaj ²	60	59	38	37	34	86	97

² Skupno število čankov po posameznih funkcijah presega število čankov ($N = 97$), ker nekateri članki obravnavajo več funkcij Ogrodja NIST.

Podatki kažejo na neenakomerno zastopanost posameznih funkcij. Najpogostejše je zastopano upravljanje, ki ga obravnava 86 člankov, sledita identifikacija s 60 in zaščita z 59 članki. Redkeje so zastopane funkcije zaznavanje (38), odzivanje (37) in okrevanje (34). V pregledanem naboru je tako izrazitejši poudarek na upravljavskih, identifikacijskih in zaščitnih vidikih, medtem ko so operativne funkcije zaznavanja, odzivanja in okrevanja manj pogosto vključene. Le 16 člankov je obravnavalo vseh šest funkcij, zato takšna široka funkcionalna zastopanost v pregledanem naboru ni prevladujoča.

Tabela 6 prikazuje porazdelitev pregledanih člankov glede na primarno domeno korporativne arhitekture, ki jo obravnavajo. Poslovna arhitektura izrazito prevladuje, saj je bilo vanjo razvrščenih 77 od 97 člankov, kar kaže na poudarek na organizacijskih, strateških, upravljavskih in procesnih vidikih kibernetike varnosti in odpornosti MSP. Tehnološko arhitekturo obravnava 11 člankov, aplikacijsko 6 in podatkovno 3, zato so te domene v pregledanem naboru bistveno manj zastopane.

Tabela 6
*Porazdelitev
člankov glede
na primarno
domeno
korporativne
arhitekture*

Domena korporativne arhitekture	Število člankov
Poslovna arhitektura	77
Tehnološka arhitektura	11
Aplikacijska arhitektura	6
Podatkovna arhitektura	3
Skupaj	97

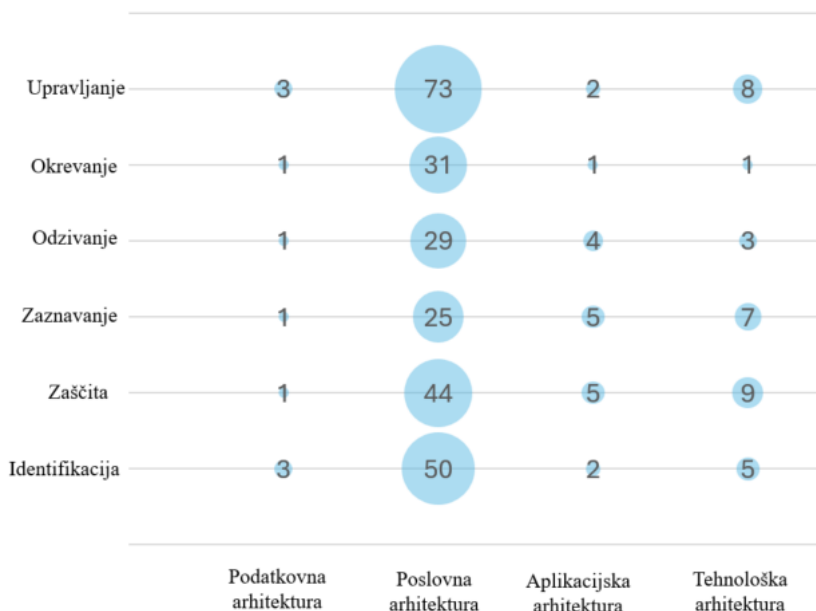
Od 97 vključenih člankov je bilo 10 preglednih prispevkov, ki so analizirali oziroma sintetizirali obstoječe modele in ogrodja, zato so bili iz analize praktične validacije izključeni. Praktična validacija je bila tako preverjena pri 87 primarnih raziskovalnih člankih, ki so razvijali oziroma predstavljali lasten model ali ogrodje. Praktično validiran model oziroma ogrodje je bil ugotovljen pri 14 od 87 člankov (16,1 %), medtem ko pri 73 člankih praktična validacija ni bila ugotovljena. Med 14 praktično validiranimi modeli oziroma ogrodji jih je bilo 11 razvrščenih v domeno poslovne arhitekture in 3 v domeno tehnološke arhitekture. V domenah aplikacijske in podatkovne arhitekture praktično validiranih modelov oziroma ogrodij nismo identificirali.

Praktična validacija je bila tako prisotna pri približno šestini primarnih raziskovalnih člankov, vključenih v to analizo. Rezultat nakazuje omejeno empirično preverjanje razvitih modelov oziroma ogrodij v realnih organizacijskih okoljih.

4.3 RV3: Katere teme so v pregledani literaturi dobro zastopane ter katere raziskovalne vrzeli in pomanjkljivo obravnavana področja je mogoče prepoznati?

V tem podglavju analiziramo zastopanost posameznih področij kibernetike odpornosti v pregledani literaturi ter prepoznavamo raziskovalne vrzeli in manj obravnavana področja. Za podporo analizi je uporabljena primerjava funkcij

Ogrodja kibernetске varnosti NIST med primarnimi domenami korporativne arhitekture, prikazana na Sliki 4.



Slika 4

Porazdelitev pregledanih člankov glede na funkcije Ogrodja kibernetске varnosti NIST in primarne domene korporativne arhitekture

Slika 4 prikazuje porazdelitev člankov na presečišču funkcij Ogrodja kibernetске varnosti NIST in primarnih domen korporativne arhitekture. Velikost posameznega mehurčka je sorazmerna s številom člankov, razvrščenih v posamezno kombinacijo funkcije in arhitekturne domene.

4.3.1 Poslovna arhitektura

Poslovna arhitektura je najbolj zastopana domena, saj je bilo vanjo razvrščenih 77 člankov. Najpogostejše so zastopane funkcije *upravljanje* v 73 člankih, *identifikacija* v 50 in *zaščita* v 44 člankih.

Pri funkciji *upravljanje* so v ospredju predvsem strategije, organizacijske politike, standardi, skladnost, odločanje vodstva in varnostna kultura. Funkcija *identifikacija* vključuje predvsem modele zrelosti, ocenjevanje tveganj, samoocenjevanje ter prepoznavanje groženj in ranljivosti. Funkcija *zaščita* vključuje sisteme upravljanja informacijske varnosti, tehnične kontrole, zaščitne modele ter vedenjske dejavnike varnega ravnanja zaposlenih.

Funkcije *zaznavanje*, *odzivanje* in *okrevanje* so zastopane redkeje, in sicer v 25, 29 oziroma 31 člankih. Obravnavane teme vključujejo prepoznavanje groženj, ocenjevanje pripravljenosti pri zaznavanju, krizno upravljanje, neprekinjeno poslovanje in forenzično pripravljenost pri odzivanju ter obnovitev poslovanja, kibernetско zavarovanje, načrtovanje naložb, metrike okrevanja in neprekinjenost dobavnih verig pri okrevanju.

Porazdelitev kaže, da so v poslovni arhitekturi izraziteje zastopani upravljavski, identifikacijski in zaščitni vidiki, medtem ko so zaznavanje, odzivanje

in okrevanje obravnavani manj pogosto. V tej domeni je bilo identificiranih tudi 11 praktično validiranih modelov oziroma ogrodij, kar skupaj z njihovo sicer izrazito zastopanostjo nakazuje omejeno empirično preverjanje razvitih pristopov.

4.3.2 Tehnološka arhitektura

Tehnološko arhitekturo obravnava 11 od 97 člankov, pri čemer so zastopane vse funkcije Ogrodja kibernetske varnosti NIST. Najpogostejše so obravnavane funkcije *zaščita* v 9 člankih, *upravljanje* v 8, *zaznavanje* v 7 in *identifikacija* v 5 člankih. Funkcija *odzivanje* je zastopana v 3 člankih, *okrevanje* pa le v enem.

Raziskave na področju funkcije *zaščita* vključujejo arhitekturo ničelnega zaupanja, decentralizirano upravljanje dostopov, avtentikacijo v okoljih interneta stvari, tehnologijo veriženja blokov in podatkovno analitiko. Funkciji *upravljanje* in *zaznavanje* obravnavata večplastna varnostna ogrodja, upravljanje ranljivosti, strojno učenje, umetno inteligenco ter sisteme za zaznavanje omrežnih vdorov. Pri funkciji *identifikacija* se pojavljajo modeli razvrščanja ranljivosti in kartiranja infrastrukture, *odzivanje* pa je povezano predvsem z avtomatiziranimi in orkestracijskimi mehanizmi.

Porazdelitev kaže izrazitejšo zastopanost zaščite, upravljanja in zaznavanja, medtem ko sta *odzivanje* in *zlasti okrevanje* obravnavana precej redkeje. Med praktično validiranimi modeli oziroma ogrodji so bili trije razvrščeni v tehnološko arhitekturo. Rezultati tako nakazujejo vrzel pri obravnavi tehnoloških vidikov *odzivanja* in *okrevanja* ter omejeno empirično preverjanje tehnološko usmerjenih modelov oziroma ogrodij.

4.3.3 Aplikacijska arhitektura

Aplikacijsko arhitekturo obravnava 6 od 97 člankov. Funkciji *zaznavanje* in *zaščita* sta zastopani vsaka v 5 člankih, *odzivanje* v 4, *identifikacija* in *upravljanje* vsaka v 2, *okrevanje* pa le v enem članku.

Raziskave se osredotočajo predvsem na zaznavanje groženj in zaščitne mehanizme na aplikacijski ravni, kot so avtentikacija, upravljanje dostopov, analiza dnevninskih zapisov in vedenjska analitika. Prisotni so tudi pristopi, ki uporabljajo strojno učenje, analitiko vedenja uporabnikov in obdelavo naravnega jezika za sprotno prepoznavanje anomalij.

Majhno število člankov ter nizka zastopanost funkcij *identifikacija*, *upravljanje* in *zlasti okrevanje* kažejo, da je aplikacijska arhitektura v pregledanem naboru obravnavana manj celovito kot poslovna arhitektura. Med primarnimi raziskovalnimi članki, vključenimi v analizo praktične validacije, v tej domeni ni bil identificiran noben praktično validiran model oziroma ogrodje. Rezultati zato nakazujejo vrzel tudi pri empiričnem preverjanju aplikacijsko usmerjenih pristopov.

4.3.4 Podatkovna arhitektura

Podatkovno arhitekturo obravnavajo samo 3 od 97 člankov, zato je najmanj zastopana domena. Funkciji *identifikacija* in *upravljanje* sta zastopani v vseh treh člankih, funkcije *zaščita*, *zaznavanje*, *odzivanje* in *okrevanje* pa vsaka v enem.

Raziskave obravnavajo podatke kot tehnični in družbeno-tehnični vir kibernetске odpornosti. Vključujejo napovedovanje tveganj na podlagi podatkov, medorganizacijsko izmenjavo informacij ter upravljanje zaupanja, identitete, zasebnosti in varnosti. Podatkovna arhitektura je tako umeščena na presečišče analitičnih modelov, izmenjave informacij in upravljanja identitet.

Majhno število člankov in omejena zastopanost večine funkcij NIST kažeta na izrazito vrzel pri vključevanju podatkovnih vidikov v modele in ogrodja kibernetске odpornosti MSP. Med primarnimi raziskovalnimi članki, vključenimi v analizo praktične validacije, v tej domeni ni bil identificiran noben praktično validiran model oziroma ogrodje.

5 ZAKLJUČEK

V prispevku smo s sistematičnim pregledom literature preučili vsebinske poudarke raziskav na področju informacijske in kibernetске varnosti ter kibernetске odpornosti MSP v obdobju 2015–2025, pri čemer je bil pregled namensko omejen na raziskave, ki razvijajo, predstavljajo ali analizirajo modele oziroma ogrodja. Začetno iskanje v bazah *Scopus* in *Web of Science* je vrnilo 1.084 zadetkov, po izvedenem izbirnem postopku pa je bilo v končno analizo vključenih 97 znanstvenih člankov. Ti so bili analizirani glede na ključne besede, funkcije Ogorodja kibernetске varnosti NIST, primarne domene korporativne arhitekture in praktično validacijo predstavljenih modelov oziroma ogrodij.

Analiza normaliziranih ključnih besed po časovnih obdobjih je pokazala različne vsebinske poudarke v pregledanih pristopih. Med obravnavanimi temami so bili informacijska varnost, standardizacija, upravljanje tveganj, kibernetška odpornost, neprekinjeno poslovanje, človeški in organizacijski dejavniki ter tehnološko podprti pristopi. V obdobju 2024–2025 so bili med vsebinskimi poudarki tudi digitalna preobrazba, upravljanje kibernetске varnosti, umetna inteligenca in arhitektura ničelnega zaupanja.

Razvrstitev po funkcijah Ogorodja kibernetске varnosti NIST je pokazala neenakomerno zastopanost posameznih funkcij. Funkcija *upravljanje* je bila zastopana v 86 člankih, *identifikacija* v 60 in *zaščita* v 59, medtem ko so bile operativne funkcije obravnavane redkeje: *zaznavanje* v 38, *odzivanje* v 37 in *okrevanje* v 34 člankih. Vseh šest funkcij je obravnavalo 16 člankov. V pregledanih modelih in ogrodjih so tako izraziteje zastopani upravljavski, identifikacijski in zaščitni vidiki, medtem ko so zaznavanje, odzivanje in okrevanje vključeni manj pogosto.

Izrazita razlika je bila ugotovljena tudi pri zastopanosti domen korporativne arhitekture. Poslovno arhitekturo je obravnavalo 77 člankov, tehnološko 11, aplikacijsko 6 in podatkovno 3. Pregledani modeli in ogrodja so tako izrazito usmerjeni v organizacijske, upravljavske in procesne vidike, medtem ko so tehnološka, aplikacijska in podatkovna arhitektura bistveno manj zastopane.

Od 97 vključenih člankov je bilo 10 preglednih prispevkov, zato je bila praktična validacija analizirana pri 87 primarnih raziskovalnih člankih, ki so razvijali oziroma predstavljali lasten model ali ogrodje. Praktična validacija je bila ugotovljena pri 14 člankih (16,1 %), medtem ko pri 73 ni bila ugotovljena. Med praktično validiranimi modeli oziroma ogrodji jih je bilo 11 razvrščenih v

poslovno in 3 v tehnološko arhitekturo, v aplikacijski in podatkovni arhitekturi pa praktično validiranih modelov oziroma ogrodi nismo identificirali. Rezultati tako kažejo na omejeno empirično preverjanje razvitih modelov in ogrodi v realnih organizacijskih okoljih.

Pri razlagi rezultatov je treba upoštevati več omejitev. Pregled je bil omejen na angleške znanstvene članke, objavljene med letoma 2015 in 2025 ter indeksirane v bazah *Scopus* in *Web of Science*. Iskalna strategija je bila z obveznim pogojem »framework OR model« namensko omejena na raziskave, ki razvijajo, predstavljajo ali analizirajo modele oziroma ogroja, zato vsebinskih poudarkov in vrzeli ni mogoče neposredno posplošiti na celotno literaturo s področja informacijske in kibernetske varnosti ter odpornosti MSP. Pri funkcijah NIST je bila evidentirana njihova prisotnost, ne pa poglobljenost obravnave, razvrščanje po domenah korporativne arhitekture pa je temeljilo na primarnem raziskovalnem poudarku posameznega članka glede na modele oziroma ogroja, ki jih je obravnaval. Začetno kodiranje je izvedla prva avtorica, mejni primeri so bili obravnavani skupaj s soavtorjema, formalna zanesljivost oziroma stopnja skladnosti med raziskovalci, ki so kodirali, pa ni bila izračunana. Prav tako ni bila izvedena sistematična presoja metodološke kakovosti vključenih raziskav. Za celotno analizirano obdobje je bila retrospektivno uporabljena klasifikacija NIST CSF 2.0, kar je treba upoštevati predvsem pri interpretaciji visoke zastopanosti funkcije upravljanje.

Ugotovitve nakazujejo potrebo po nadaljnjem razvoju modelov in ogrodi, ki bi bolj uravnoteženo vključevali posamezne funkcije NIST CSF 2.0 in domene korporativne arhitekture. Posebno pozornost je smiselno nameniti manj zastopanim funkcijam zaznavanja, odzivanja in okrevanja ter aplikacijski in podatkovni arhitekturi. Pomembno področje nadaljnega raziskovanja predstavlja tudi praktično preverjanje razvitih modelov in ogrodi v realnih okoljih MSP.

VIRI IN LITERATURA

- Almeida, F. (2025). Comparative analysis of EU-based cybersecurity skills frameworks. *Computers & Security*, 151, 104329. <https://doi.org/10.1016/j.cose.2025.104329>
- Arroyabe, M. F., Arranz, C. F. A., Fernandez de Arroyabe, I. in Fernandez de Arroyabe, J. C. (2024). Exploring the economic role of cybersecurity in SMEs: A case study of the UK. *Technology in Society*, 78, 102670. <https://doi.org/10.1016/j.techsoc.2024.102670>
- Barbour, D. (21. 10. 2024). *Small business guide to NIS 2 compliance*. Kiteworks. <https://www.kiteworks.com/regulatory-compliance/nis-2-compliance-small-business/>
- Breaker-Rolfe, J. (10. 10. 2024). *The role of the NIST CSF in cyber resilience*. Tripwire. <https://www.tripwire.com/state-of-security/role-nist-csf-cyber-resilience>
- Clemente-Almendros, J. A., Nicoara-Popescu, D. in Pastor-Sanz, I. (2024). Digital transformation in SMEs: Understanding its determinants and size heterogeneity. *Technology in Society*, 77, 102483. <https://doi.org/10.1016/j.techsoc.2024.102483>

- Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1792, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). (2022). *Official Journal of the European Union*, L 333, 80–152. <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>
- European Digital Innovation Hubs Network. (28. 8. 2024). *Train your SME on the basics of cybersecurity*. <https://european-digital-innovation-hubs.ec.europa.eu/knowledge-hub/success-stories/train-your-sme-basics-cybersecurity>
- ENISA. (22. 11. 2024a). *Navigating cybersecurity investments in the time of NIS 2*. <https://www.enisa.europa.eu/news/navigating-cybersecurity-investments-in-the-time-of-nis-2>
- ENISA. (28. 11. 2024b). *SMEs cybersecurity*. <https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/smes-cybersecurity>
- Estarch, P. (3. 1. 2025). *What is enterprise architecture (EA), and why is it important?* MEGA. <https://www.mega.com/blog/what-is-enterprise-architecture-definition>
- Goikoetxea, M. (17. 12. 2024). *New digital rules are here—and so are more compliance burdens for SMEs*. ACT | The App Association. <https://actonline.org/2024/12/17/new-digital-rules-are-here-and-so-are-more-compliance-burdens-for-smes/>
- Heffer, R. in Troskie, A. (11. 4. 2024). *A security leader's guide to the NIST Cybersecurity Framework (CSF) 2.0*. Veeam. <https://www.veeam.com/blog/nist-cybersecurity-framework-2-0.html>
- Hoong, Y., Rezania, D. in Baker, R. (2024). When traditional SME managers encounter cybersecurity: Discourse analysis of opportunities and dilemmas in meeting the demands. *Technology in Society*, 78, 102650. <https://doi.org/10.1016/j.techsoc.2024.102650>
- Houghton, S. (20. 11. 2024). *Cyber resilience vs. cyber security: Which one does your business need?* Aztech IT. <https://www.aztechit.co.uk/blog/cyber-resilience-vs-cyber-security>
- Hovav, A., Gnizy, I. in Han, J. (2023). The effects of cyber regulations and security policies on organizational outcomes: A knowledge management perspective. *European Journal of Information Systems*, 32(2), 154–172. <https://doi.org/10.1080/0960085X.2021.1908184>
- Joswig, T. in Kurz, W. (2025). Empirical analysis of NIS2 adoption in EU SMEs: Challenges for critical infrastructure in Germany. *Journal of Next-Generation Research* 5.0, 1(3). <https://doi.org/10.70792/jngr5.0.v1i3.99>
- Kern, M., Landauer, M., Skopik, F. in Weippl, E. (2024). A logging maturity and decision model for the selection of intrusion detection cybersecurity solutions. *Computers & Security*, 141, 103844. <https://doi.org/10.1016/j.cose.2024.103844>
- Kiiveri, K., Naumanen, P., Liesivuori, J., Virtanen, S. in Isoaho, J. (2024). A four-phase model and a mobile app for crisis preparedness and management in small and medium-sized enterprises. *Journal of Contingencies and Crisis Management*, 32(3), e12618. <https://doi.org/10.1111/1468-5973.12618>

- King, C. (23. 2. 2023). *Cyber resilience is critical for digital transformation*. Cyber Magazine. <https://cybermagazine.com/articles/cyber-resilience-is-critical-for-digital-transformation>
- Metin, B., Özhan, F. G. in Wynn, M. (2024). Digitalisation and cybersecurity: Towards an operational framework. *Electronics*, 13(21), 4226. <https://doi.org/10.3390/electronics13214226>
- Mukhopadhyay, A. in Jain, S. (2024). A framework for cyber-risk insurance against ransomware: A mixed-method approach. *International Journal of Information Management*, 74, 102724. <https://doi.org/10.1016/j.ijinfomgt.2023.102724>
- Nastjuk, I., Rampold, F., Trang, S. in Benitez, J. (2025). A field experiment on ISP training designs for enhancing employee information security compliance. *European Journal of Information Systems*, 34(4), 565–588. <https://doi.org/10.1080/0960085X.2024.2359460>
- NIST. (2024). *The NIST cybersecurity framework (CSF) 2.0* (NIST CSWP 29). <https://doi.org/10.6028/NIST.CSWP.29>
- Olcott, J. (22. 8. 2024). *Cyber resilience vs. cybersecurity: What's the difference and how to build a plan for both*. Bitsight. <https://www.bitsight.com/blog/cyber-resilience-vs-cybersecurity>
- Proudfoot, J. G., Cram, W. A. in Madnick, S. (2025). Weathering the storm: Examining how organisations navigate the sea of cybersecurity regulations. *European Journal of Information Systems*, 34(3), 436–459. <https://doi.org/10.1080/0960085X.2024.2345867>
- PwC. (2024). *Cloud attacks are top cyber risk concern: PwC 2024 Global Digital Trust Insights*. <https://www.pwc.com/bm/en/press-releases/pwc-2024-global-digital-trust-insights.html>
- Radzi, N. R., Ahmad Tajuddin, S. N. A. in Azam Bahari, K. (2024). Small steps, big security: TAM-powered insights of cybersecurity adoption among small-and-medium entrepreneurs in digital business. *Journal of Ecohumanism*, 3(3), 1626–1638. <https://doi.org/10.62754/joe.v3i3.3327>
- Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act). (2024). *Official Journal of the European Union*, L 2024/2847. <https://eur-lex.europa.eu/eli/reg/2024/2847/oj>
- Szedlak, C., Reinemann, H. in Hatzelmann, S. (2024). *Ensuring cybersecurity compliance: Assessing SME awareness and preparedness for the Cyber Resilience Act*. V *Proceedings of the International Conference on Industrial Engineering and Operations Management*. IEOM Society International. <https://doi.org/10.46254/AP05.20240160>
- The Open Group. (2022). *The TOGAF® Standard, 10th Edition*. <https://publications.opengroup.org/standards/togaf>
- Trujillo, S. (13. 3. 2024). *Impact of the CRA on SME equipment manufacturers in Europe: Experience and lessons learned (I20b)*. EU Cyber Resilience Act. <https://eucyberact.org/session/impact-of-the-cra-on-the-sme-equipment-manufacturers-in-europe-experience-and-lessons-learned-i20b/>

- Tuteja, A. (30. 7. 2024). *SMEs can turn cybersecurity risk into opportunity. Here's how*. World Economic Forum. <https://www.weforum.org/stories/2024/07/smes-can-turn-cybersecurity-risk-into-opportunity-heres-how/>
- Urad Vlade Republike Slovenije za informacijsko varnost. (2024). *Informacijska varnost*. <https://www.gov.si teme/informacijska-varnost/>
- White, S. K. (23. 11. 2022). *What is enterprise architecture? A framework for transformation*. CIO. <https://www.cio.com/article/222421/what-is-enterprise-architecture-a-framework-for-transformation.html>
- World Economic Forum. (2024). *3 trends set to drive cyberattacks and ransomware in 2024*. <https://www.weforum.org/agenda/2024/02/3-trends-ransomware-2024/>

PRILOGA A: SEZNAM ČLANKOV, VKLJUČENIH V ANALIZO

- Abdelmagid, A. M. in Diaz, R. (2025). Zero trust architecture as a risk countermeasure in small-medium enterprises and advanced technology systems. *Risk Analysis*, 45, 2390–2414. <https://doi.org/10.1111/risa.70026>
- Ahmed, N. N. in Nanath, K. (2021). Exploring cybersecurity ecosystem in the Middle East: Towards an SME recommender system. *Journal of Cyber Security and Mobility*, 10(3), 511–536. <https://doi.org/10.13052/jcsm2245-1439.1032>
- Aigbefo, Q. A., Blount, Y. in Marrone, M. (2022). The influence of hardiness and habit on security behaviour intention. *Behaviour & Information Technology*, 41(6), 1151–1170. <https://doi.org/10.1080/0144929X.2020.1856928>
- Al-Dosari, K. in Fetais, N. (2023). Risk-management framework and information-security systems for small and medium enterprises (SMEs): A meta-analysis approach. *Electronics*, 12(17), 3629. <https://doi.org/10.3390/electronics12173629>
- Almeida, F. (2025). Comparative analysis of EU-based cybersecurity skills frameworks. *Computers & Security*, 151, 104329. <https://doi.org/10.1016/j.cose.2025.104329>
- Almoaigel, M. F. in Abuabid, A. (2023). Implementation of cybersecurity situation awareness model in Saudi SMEs. *International Journal of Advanced Computer Science and Applications*, 14(11), 1082–1092. <https://doi.org/10.14569/IJACSA.2023.01411110>
- Alshawish, I. in Al-Haj, A. (2022). An efficient mutual authentication scheme for IoT systems. *The Journal of Supercomputing*, 78(14), 16056–16087. <https://doi.org/10.1007/s11227-022-04520-5>
- Alzahrani, L. in Seth, K. P. (2021). The impact of organizational practices on the information security management performance. *Information*, 12(10), 398. <https://doi.org/10.3390/info12100398>
- Ambreen, L., Jain, M., Yadav, R. K. in Loonkar, S. (2024). Effective cybersecurity risk management practices for small and medium-sized enterprises: A comprehensive review. *Multidisciplinary Reviews*, 6, 2023ss080. <https://doi.org/10.31893/multirev.2023ss080>
- Andi, R. in Utama, D. N. (2023). Business continuity management framework in electronic system provider (ESP) startup company. *Journal of System and Management Sciences*, 13(1), 322–343. <https://doi.org/10.33168/JSMS.2023.0118>

- Antunes, M., Maximiano, M. in Gomes, R. (2022). A client-centered information security and cybersecurity auditing framework. *Applied Sciences*, 12(9), 4102. <https://doi.org/10.3390/app12094102>
- Armenia, S., Angelini, M., Nonino, F., Palombi, G. in Schlitzer, M. F. (2021). A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. *Decision Support Systems*, 147, 113580. <https://doi.org/10.1016/j.dss.2021.113580>
- Arroyabe, M. F., Arranz, C. F. A., Fernandez de Arroyabe, I. in Fernandez de Arroyabe, J. C. (2024). Exploring the economic role of cybersecurity in SMEs: A case study of the UK. *Technology in Society*, 78, 102670. <https://doi.org/10.1016/j.techsoc.2024.102670>
- Ascue, O., Valle, O. in Santisteban, J. (2025). BLOCKSAGE: Blockchain-based cloud architecture for sensitive data management in SMEs. *Sustainability*, 17(4), 1352. <https://doi.org/10.3390/su17041352>
- Awan, M., Alam, A. in Kamran, M. (2025). Cybersecurity challenges in small and medium enterprises: A scoping review. *Journal of Cyber Security and Risk Auditing*, 2025(3), 89–102. <https://doi.org/10.63180/jcsra.thestap.2025.3.7>
- Barlette, Y. in Jaouen, A. (2019). Information security in SMEs: Determinants of CEOs' protective and supportive behaviors. *Systèmes d'Information et Management*, 24(3), 7–40. <https://doi.org/10.3917/sim.193.0007>
- Benz, M. in Chatterjee, D. (2020). Calculated risk? A cybersecurity evaluation tool for SMEs. *Business Horizons*, 63(4), 531–540. <https://doi.org/10.1016/j.bushor.2020.03.010>
- Budde, C., Karinsalo, A., Vidor, S., Salonen, J. in Massacci, F. (2023). CSEC+ framework assessment dataset: Expert evaluations of cybersecurity skills for job profiles in Europe. *Data in Brief*, 48, 109285. <https://doi.org/10.1016/j.dib.2023.109285>
- Calvo-Manzano, J., San Feliu, T., Herranz Nieva, Á., Mariño, J., Fredlund, L.-Å. in Moreno, A. (2025). CyberESP: An integrated cybersecurity framework for SMEs. *Journal of Software: Evolution and Process*, 37(9), e70050. <https://doi.org/10.1002/smr.70050>
- Carayannis, E., Dumitrescu, R., Falkowski, T., Papamichail, G. in Zota, N. (2025). Enhancing SME resilience through artificial intelligence and strategic foresight: A framework for sustainable competitiveness. *Technology in Society*, 81, 102835. <https://doi.org/10.1016/j.techsoc.2025.102835>
- Carias, J. F., Arrizabalaga, S., Labaka, L. in Hernantes, J. (2021). Cyber resilience self-assessment tool (CR-SAT) for SMEs. *IEEE Access*, 9, 80741–80762. <https://doi.org/10.1109/ACCESS.2021.3085530>
- Carias, J. F., Borges, M. R. S., Labaka, L., Arrizabalaga, S. in Hernantes, J. (2020). Systematic approach to cyber resilience operationalization in SMEs. *IEEE Access*, 8, 174200–174221. <https://doi.org/10.1109/ACCESS.2020.3026063>
- Castro, L. J. R., Aquino, P. A. C. in Rojas, F. E. G. (2024). Machine learning as a tool to combat ransomware in resource-constrained business environment. *International Journal of Advanced Computer Science and Applications*, 15(12), 509–517. <https://doi.org/10.14569/IJACSA.2024.0151253>

- Chandra, N. A. in Sadikin, M. (2020). ISM application tool, a contribution to address the barrier of information security management system implementation. *Journal of Information and Communication Convergence Engineering*, 18(1), 39–48. <https://doi.org/10.6109/jicce.2020.18.1.39>
- Chen, Y.-S., Chou, J. C.-L., Lin, Y.-S., Hung, Y.-H. in Chen, X.-H. (2023). Identification of SMEs in the critical factors of an IS backup system using a three-stage advanced hybrid MDM–AHP model. *Sustainability*, 15(4), 3516. <https://doi.org/10.3390/su15043516>
- Chidukwani, A., Zander, S. in Koutsakis, P. (2022). A survey on the cyber security of small-to-medium businesses: Challenges, research focus and recommendations. *IEEE Access*, 10, 85701–85719. <https://doi.org/10.1109/ACCESS.2022.3197899>
- Choudhary, D. in Pahuja, R. (2023). A blockchain-based cyber-security for connected networks. *Peer-to-Peer Networking and Applications*, 16(4), 1852–1867. <https://doi.org/10.1007/s12083-023-01506-9>
- Chowdhury, N., Katsikas, S. in Gkioulos, V. (2022). Modeling effective cybersecurity training frameworks: A Delphi method-based study. *Computers & Security*, 113, 102551. <https://doi.org/10.1016/j.cose.2021.102551>
- Compastié, M., López Martínez, A., Fernández, C., Gil Pérez, M., Tsarsitalidis, S., Xylouris, G., Mlakar, I., Kourtis, M. A. in Šafran, V. (2023). PALANTIR: An NFV-based security-as-a-service approach for automating threat mitigation. *Sensors*, 23(3), 1658. <https://doi.org/10.3390/s23031658>
- Dakic, V., Moric, Z., Kapulica, A. in Regvart, D. (2024). Analysis of Azure zero trust architecture implementation for mid-size organizations. *Journal of Cybersecurity and Privacy*, 5(1), 2. <https://doi.org/10.3390/jcp5010002>
- De Matteis, J., Elia, G. in Del Vecchio, P. (2023). Business continuity management and organizational resilience: A small and medium enterprises (SMEs) perspective. *Journal of Contingencies and Crisis Management*, 31(4), 670–682. <https://doi.org/10.1111/1468-5973.12470>
- Deruma, S. (2025). Cyber resilience key metrics in small and medium-sized enterprises. *Economics Ecology Socium*, 9(1), 15–23. <https://doi.org/10.61954/2616-7107/2025.9.1-2>
- Emer, A., Unterhofer, M. in Rauch, E. (2021). A cybersecurity assessment model for small and medium-sized enterprises. *IEEE Engineering Management Review*, 49(2), 98–109. <https://doi.org/10.1109/EMR.2021.3078077>
- Falch, M., Olesen, H., Skouby, K. E., Tadayoni, R. in Williams, I. (2023). Cybersecurity strategies for SMEs in the Nordic Baltic region. *Journal of Cyber Security and Mobility*, 11(6), 727–754. <https://doi.org/10.13052/jcsm2245-1439.1161>
- Fernandez de Arroyabe, J. C., Arroyabe, M. F., Fernandez, I. in Arranz, C. F. A. (2024). Cybersecurity resilience in SMEs: A machine learning approach. *Journal of Computer Information Systems*, 64(6), 711–727. <https://doi.org/10.1080/08874417.2023.2248925>
- Firoiu, M. in Bacivarov, I. C. (2016). Physical and logical security risk assessment procedure for SMEs, according to ISO/IEC 27005:2011 and SR ISO 31000:2010 standards. *Quality – Access to Success*, 17(152), 86–98.

- Franco, M., Lacerda, F. in Stiller, B. (2022). A framework for the planning and management of cybersecurity projects in small and medium-sized enterprises. *Revista de Gestão e Projetos*, 13(3), 10–37, e23083. <https://doi.org/10.5585/gep.v13i3.23083>
- García, A., Dominguez, F., Calle, L., Martinez, J. in Raymundo, C. (2018). Personal data protection maturity model for the micro financial sector in Peru. *International Journal of Engineering Research and Technology*, 11(4), 649–660.
- Grubor, G., Barac, I., Simeunovic, N. in Ristic, N. (2017). Achieving business excellence by optimizing corporate forensic readiness. *Amfiteatru Economic*, 19(44), 197–214.
- Handfield, R., Earp, J. in Sadeghi, A. H. (2025). Reducing cybersecurity vulnerabilities in the supply base: Insights from cyber experts. *Technology in Society*, 82, 102947. <https://doi.org/10.1016/j.techsoc.2025.102947>
- Hoong, Y. in Rezanian, D. (2024). Navigating cybersecurity governance: The influence of opportunity structures in socio-technical transitions for small and medium enterprises. *Computers & Security*, 142, 103852. <https://doi.org/10.1016/j.cose.2024.103852>
- Hoong, Y., Rezanian, D. in Baker, R. (2024). When traditional SME managers encounter cybersecurity: Discourse analysis of opportunities and dilemmas in meeting the demands. *Technology in Society*, 78, 102650. <https://doi.org/10.1016/j.techsoc.2024.102650>
- Jamil, H., Zia, T., Nayeem, T., Whitty, M. in D'Alessandro, S. (2025). Human-centric cyber security: Applying protection motivation theory to analyse micro business owners' security behaviours. *Information and Computer Security*, 33(1), 49–76. <https://doi.org/10.1108/ICS-10-2023-0176>
- Jayarao, G. B., Ray, S. in Panigrahi, P. K. (2024). Information security threats and organizational readiness in nWFH scenarios. *Computers & Security*, 140, 103745. <https://doi.org/10.1016/j.cose.2024.103745>
- Kaušpadienė, L., Ramanauskaitė, S. in Čenys, A. (2019). Information security management framework suitability estimation for small and medium enterprise. *Technological and Economic Development of Economy*, 25(5), 979–997. <https://doi.org/10.3846/tede.2019.10298>
- Kern, M., Landauer, M., Skopik, F. in Weippl, E. (2024). A logging maturity and decision model for the selection of intrusion detection cyber security solutions. *Computers & Security*, 141, 103844. <https://doi.org/10.1016/j.cose.2024.103844>
- Kiiveri, K., Naumanen, P., Liesivuori, J., Virtanen, S. in Isoaho, J. (2024). A four-phase model and a mobile app for crisis preparedness and management in small and medium-sized enterprises. *Journal of Contingencies and Crisis Management*, 32(3), e12618. <https://doi.org/10.1111/1468-5973.12618>
- Kim, H., So, W. in Je, S. (2019). A big data framework for network security of small and medium enterprises for future computing. *The Journal of Supercomputing*, 75(6), 3334–3367. <https://doi.org/10.1007/s11227-019-02815-8>
- Le, T. D., Le-Dinh, T. in Uwizeyemungu, S. (2024). Search engine optimization poisoning: A cybersecurity threat analysis and mitigation strategies for small and medium-sized enterprises. *Technology in Society*, 76, 102470. <https://doi.org/10.1016/j.techsoc.2024.102470>

- Le, T. D., Le-Dinh, T. in Uwizeyemungu, S. (2025). A cybersecurity framework for enhancing small and medium-sized enterprises' (SMEs) security posture using user behaviour analytics. *Enterprise Information Systems*, 19(10), 2529282. <https://doi.org/10.1080/17517575.2025.2529282>
- Li, D. in Mei, X. (2024). Evolutionary game analysis of data sharing among large and medium-sized enterprises in the perspective of platform empowerment. *Scientific Reports*, 14(1), 11447. <https://doi.org/10.1038/s41598-024-62156-2>
- Lill, B., Sauerwein, C., Mexis, N. in Langner, K. (2025). A comprehensive review of information security research regarding SMEs and future directions. *Journal of Cyber Security and Mobility*, 14(5), 1245–1288. <https://doi.org/10.13052/jcsm2245-1439.1459>
- Löffler, E., Schneider, B., Asprion, P. M. in Zanwar, T. (2021). CySecEscape 2.0—A virtual escape room to raise cybersecurity awareness. *International Journal of Serious Games*, 8(1), 59–70. <https://doi.org/10.17083/ijsg.v8i1.413>
- Ludin, W. N. E. W. M., Mohd, M. in Fauzi, W. F. P. (2024). Comparative analysis of small and medium-sized enterprises cybersecurity program assessment model. *International Journal of Advanced Computer Science and Applications*, 15(8), 796–804. <https://doi.org/10.14569/IJACSA.2024.0150878>
- Melnyk, S. A., Schoenherr, T., Speier-Pero, C., Peters, C., Chang, J. F. in Friday, D. (2022). New challenges in supply chain management: Cybersecurity across the supply chain. *International Journal of Production Research*, 60(1), 162–183. <https://doi.org/10.1080/00207543.2021.1984606>
- Metin, B., Özhan, F. G. in Wynn, M. (2024). Digitalisation and cybersecurity: Towards an operational framework. *Electronics*, 13(21), 4226. <https://doi.org/10.3390/electronics13214226>
- Mijnhardt, F., Baars, T. in Spruit, M. (2016). Organizational characteristics influencing SME information security maturity. *Journal of Computer Information Systems*, 56(2), 106–115. <https://doi.org/10.1080/08874417.2016.1117369>
- Moneva, A. in Leukfeldt, R. (2023). Insider threats among Dutch SMEs: Nature and extent of incidents, and cyber security measures. *Journal of Criminology*, 56(4), 416–440. <https://doi.org/10.1177/26338076231161842>
- Moyo, M. in Looock, M. (2021). Conceptualising a cloud business intelligence security evaluation framework for small and medium enterprises in small towns of the Limpopo Province, South Africa. *Information*, 12(3), 128. <https://doi.org/10.3390/info12030128>
- Neri, M. in Niccolini, F. (2025). On the path to cyber organizational resilience: Shedding light on the context of SMEs. *International Journal of Organizational Analysis*, 33(12), 105–131. <https://doi.org/10.1108/IJOA-06-2024-4572>
- Ngo, T. in Tick, A. (2021). Cyber-security risks assessments by external auditors. *Interdisciplinary Description of Complex Systems*, 19(3), 375–390. <https://doi.org/10.7906/indec.19.3.3>
- Ode, E., Awolowo, I. F., Nana, R. in Olawoyin, F. S. (2025). Social capital and artificial intelligence readiness: The mediating role of cyber resilience and value construction of SMEs in resource-constrained environments. *Information Systems Frontiers*. <https://doi.org/10.1007/s10796-025-10608-z>

- Oroni, C. Z. in Xianping, F. (2023). Structural evaluation of management capability and the mediation role of cybersecurity awareness towards enterprise performance. *Journal of Data, Information and Management*, 5(4), 345–361. <https://doi.org/10.1007/s42488-023-00108-7>
- Panko, M., Safar, L. in Mešfan, M. (2025). Small firms, big threats: Cybersecurity research and the role of public policy in the SME sector. *Central European Journal of Public Policy*, 19(2), 87–110. <https://doi.org/10.2478/cejpp-2025-0010>
- Park, H., Yoo, Y. in Lee, H. (2021). 7S model for technology protection of organizations. *Sustainability*, 13(13), 7020. <https://doi.org/10.3390/su13137020>
- Păunescu, C. in Argatu, R. (2020). Critical functions in ensuring effective business continuity management: Evidence from Romanian companies. *Journal of Business Economics and Management*, 21(2), 497–520. <https://doi.org/10.3846/jbem.2020.12205>
- Pawar, S. in Palivela, D. H. (2022). LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs). *International Journal of Information Management Data Insights*, 2(1), 100080. <https://doi.org/10.1016/j.ijime.2022.100080>
- Pérez-González, D., Preciado, S. T. in Solana-Gonzalez, P. (2019). Organizational practices as antecedents of the information security management performance: An empirical investigation. *Information Technology & People*, 32(5), 1262–1275. <https://doi.org/10.1108/ITP-06-2018-0261>
- Perozzo, H., Zaghoul, F. in Ravarini, A. (2022). Cybersecurity readiness: A model for SMEs based on the socio-technical perspective. *Complex Systems Informatics and Modeling Quarterly*, 33, 53–66. <https://doi.org/10.7250/csimq.2022-33.04>
- Pham, Q. H. in Vu, K. P. (2024). Insight into how cyber forensic accounting enhances the integrated reporting quality in small and medium enterprises. *Cogent Business & Management*, 11(1), 2364053. <https://doi.org/10.1080/23311975.2024.2364053>
- Prislan, K., Mihelič, A. in Bernik, I. (2020). A real-world information security performance assessment using a multidimensional socio-technical approach. *PLOS ONE*, 15(9), e0238739. <https://doi.org/10.1371/journal.pone.0238739>
- Radzi, N. R., Ahmad Tajuddin, S. N. A. in Azam Bahari, K. (2024). Small steps, big security: TAM-powered insights of cybersecurity adoption among small-and-medium entrepreneurs in digital business. *Journal of Ecohumanism*, 3(3), 1626–1638. <https://doi.org/10.62754/joe.v3i3.3327>
- Rashid, A. in Rasheed, R. (2025). Supply chain cognitive resilience through AI-powered risk mitigation and autonomous resilience. *Supply Chain Management*. <https://doi.org/10.1108/SCM-07-2025-0656>
- Rawindaran, N., Jayal, A. in Prakash, E. (2025). Cybersecurity framework: Addressing resiliency in Welsh SMEs for digital transformation and Industry 5.0. *Journal of Cybersecurity and Privacy*, 5(2), 17. <https://doi.org/10.3390/jcp5020017>
- Rawindaran, N., Jayal, A., Prakash, E. in Hewage, C. (2021). Cost benefits of using machine learning features in NIDS for cyber security in UK small medium enterprises (SME). *Future Internet*, 13(8), 186. <https://doi.org/10.3390/fi13080186>

- Rodriguez-Baca, L. S., Allagi, S., Larrea-Serquen, R., Cruzado, C. F., Diaz, M. A., Garcia-Hernández, S. in Monteiro, J. D. (2023). Experimental study based on the implementation of a regulatory framework for the improvement of cyber resilience in SMEs. *International Journal on Recent and Innovation Trends in Computing and Communication*, 11(3), 199–205. <https://doi.org/10.17762/ijritcc.v11i3.6337>
- Rusu, D. in Măntulescu, M. (2025). Development of an application-based framework for information security management in SMEs. *Sustainability*, 17(18), 8314. <https://doi.org/10.3390/su17188314>
- Saban, K. A., Rau, S. in Wood, C. A. (2021). SME executives' perceptions and the information security preparedness model. *Information and Computer Security*, 29(2), 263–282. <https://doi.org/10.1108/ICS-01-2020-0014>
- Salas-Riega, J. L., Riega-Virú, Y., Ninaquispe Soto, M. in Salas-Riega, J. M. (2025). Cybersecurity and the NIST Framework: A systematic review of its implementation and effectiveness against cyber threats. *International Journal of Advanced Computer Science and Applications*, 16(6), 723–735. <https://doi.org/10.14569/IJACSA.2025.0160672>
- Santos-Olmo, A., Sánchez, L. E., Caballero, I., Camacho, S. in Fernandez-Medina, E. (2016). The importance of the security culture in SMEs as regards the correct management of the security of their assets. *Future Internet*, 8(3), 30. <https://doi.org/10.3390/fi8030030>
- Schmitz, C. in Pape, S. (2020). LiSRA: Lightweight security risk assessment for decision support in information security. *Computers & Security*, 90, 101656. <https://doi.org/10.1016/j.cose.2019.101656>
- Song, J. in Park, M. J. (2024). A system dynamics approach for cost-benefit simulation in designing policies to enhance the cybersecurity resilience of small and medium-sized enterprises. *Information Development*. <https://doi.org/10.1177/02666669241252996>
- Taskin, N., Özkeleş Yıldırım, A., Ercan, H. D., Wynn, M. in Metin, B. (2025). Cyber insurance adoption and digitalisation in small and medium-sized enterprises. *Information*, 16(1), 66. <https://doi.org/10.3390/info16010066>
- Tsinganos, N., Fouliras, P. in Mavridis, I. (2022). Applying BERT for early-stage recognition of persistence in chat-based social engineering attacks. *Applied Sciences*, 12(23), 12353. <https://doi.org/10.3390/app122312353>
- Tubío Figueira, P., López Bravo, C. in Rivas López, J. L. (2020). Improving information security risk analysis by including threat-occurrence predictive models. *Computers & Security*, 88, 101609. <https://doi.org/10.1016/j.cose.2019.101609>
- Uraipan, N., Praneetpolgrang, P. in Manisri, T. (2021). Application of a fuzzy analytic hierarchy process to select the level of a cyber resilient capability maturity model in digital supply chain systems. *ECTI Transactions on Computer and Information Technology*, 15(2), 198–207. <https://doi.org/10.37936/ecti-cit.2021152.240631>

- Vaezi, A., Jones, S. in Asgary, A. (2023). Integrating resilience into risk matrices: A practical approach to risk assessment with empirical analysis. *Journal of Risk Analysis and Crisis Response*, 13(4), 252–272. <https://doi.org/10.54560/jracr.v13i4.411>
- Van Haastrecht, M., Ozkan, B. Y., Brinkhuis, M. in Spruit, M. (2021). Respite for SMEs: A systematic review of socio-technical cybersecurity metrics. *Applied Sciences*, 11(15), 6909. <https://doi.org/10.3390/app11156909>
- Vaseghipanih, M., Jabbehdari, S. in Navidi, H. (2025). A game-theoretic approach for quantification of strategic behaviors in digital forensic readiness. *Journal of Cybersecurity and Privacy*, 5(4), 105. <https://doi.org/10.3390/jcp5040105>
- Vasudevan, S., Piazza, A., Rajendran, L. in Duraivel, S. (2025). Mapping the metaverse minefield: A TIPS framework for security-conscious business adoption. *Computers & Security*, 160, 104710. <https://doi.org/10.1016/j.cose.2025.104710>
- Wang, S. S. (2019). Integrated framework for information security investment and cyber insurance. *Pacific-Basin Finance Journal*, 57, 101173. <https://doi.org/10.1016/j.pacfin.2019.101173>
- Wilson, M. in McDonald, S. (2025). One size does not fit all: Exploring the cybersecurity perspectives and engagement preferences of UK-based small businesses. *Information Security Journal: A Global Perspective*, 34(1), 15–49. <https://doi.org/10.1080/19393555.2024.2357310>
- Wong, L., Lee, V., Tan, G., Ooi, K. in Sohal, A. (2022). The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. *International Journal of Information Management*, 66, 102520. <https://doi.org/10.1016/j.ijinfomgt.2022.102520>
- Yigit Ozkan, B. in Spruit, M. (2023). Adaptable security maturity assessment and standardization for digital SMEs. *Journal of Computer Information Systems*, 63(4), 965–987. <https://doi.org/10.1080/08874417.2022.2119442>
- Yigit Ozkan, B., Spruit, M., Wondolleck, R. in Burriel Coll, V. (2020). Modelling adaptive information security for SMEs in a cluster. *Journal of Intellectual Capital*, 21(2), 235–256. <https://doi.org/10.1108/JIC-05-2019-0128>
- Yudhiyati, R., Putritama, A. in Rahmawati, D. (2021). What small businesses in developing country think of cybersecurity risks in the digital age: Indonesian case. *Journal of Information, Communication and Ethics in Society*, 19(4), 446–462. <https://doi.org/10.1108/JICES-03-2021-0035>
- Zhang, X., Xie, H., Yang, H., Shao, H. in Zhu, M. (2020). A general framework to understand vulnerabilities in information systems. *IEEE Access*, 8, 121858–121873. <https://doi.org/10.1109/ACCESS.2020.3006361>

O avtorjih

Sara Horvat, mag. varstvoslovja, doktorska kandidatka, Fakulteta za varnostne vede, Univerza v Mariboru, sara.tomse@student.um.si

Prof. dr. Simon Vrhovec, Fakulteta za varnostne vede, Univerza v Mariboru, simon.vrhovec@um.si

Izr. prof. dr. Blaž Markelj, Fakulteta za varnostne vede, Univerza v Mariboru, blaz.markelj@um.si