Zaprimljen: 17.6.2025.
Odobren za objavu: 13.10.2025.
Pregledni rad

ZNANSTVENO MAPIRANJE I TRENDOVI ISTRAŽIVANJA KIBERNETIČKE SIGURNOSTI U PODRUČJU EKONOMIJE I MENADŽMENTA I POSLOVANJA

Višnja Bartolović[1], Donata Pospišil[2], Milan Puvača[3]
[1] Sveučilište u Slavonskom Brodu, Odjel društveno-humanističkih znanosti, Trg I. B. Mažuranić 2, 35000 Slavonski Brod, Hrvatska, ePošta: vbartolovic@unisb.hr
[2] Sveučilište u Slavonskom Brodu, Odjel društveno-humanističkih znanosti, Trg I. B. Mažuranić 2, 35000 Slavonski Brod, Hrvatska, ePošta: dposlpisil@unisb.hr
[3] Ofir d.o.o. Osijek, Ramska 20, 31 000 Osijek, Hrvatska, ePošta: milan@ofir.hr

Sažetak: Kibernetička sigurnost u posljednje vrijeme postaje sve važnija tema na sjecištu tehnologije, ekonomije i menadžmenta, no struktura istraživanja u ovom interdisciplinarnom polju nije uvijek jasno definirana. Trendovi u istraživanju kibernetičke sigurnosti usmjeravaju se prema istraživanju rizika, otpornosti, kriptografiji, blokchain tehnologiji, strojnom učenju i industriji 5.0.

Cilj rada je identificirati istraživačke klastere u području kibernetičke sigurnosti. Obzirom da kibernetička sigurnost značajno korelira s temama ekonomije i menadžmenta provedeno je klasteriranje kibernetičke sigurnosti u području ekonomije i menadžmenta.

Pregledom znanstvenih baza podataka (Web of Science) koristeći ključnu temu „cyber security" i njezine inačice identificirano je 28.669 dokumenata te je odabirom područja ekonomije, menadžmenta i poslovanja uzorkovanjem obuhvaćeno 777 istraživanja objavljenih u periodu od 2002. do travnja 2025. godine. U obzir su uzete ključne riječi koje su autori studija eksplicitno navodili te ključne riječi koje Web of Science algoritamski dodaje. Podaci su prethodno pročišćeni i normalizirani, obzirom na različitost znanstvenih područja.

Programom za vizualizaciju VOSviewer, koristeći frakcijsko brojanje za analizu ko-pojavnosti ključnih riječi, identificirani su klasteri znanstvenih istraživanja koji otkrivaju frekvencije, povezanost i intenzitet veza među ključnim temama. Identificirano je devet istraživačkih klastera, najznačajniji autori, institucije, zemlje te povezanost tema kibernetičke sigurnosti u području ekonomije i menadžmenta s pojedinim ciljevima održivosti Ujedinjenih naroda.

Ključne riječi: analiza ključnih riječi, ekonomija, kibernetička sigurnost, menadžment, vizualizacija, znanstveno mapiranje

1. Uvod

Bibliometrijska analiza područja kibernetičke sigurnosti predstavlja mogućnost znanstvenog mapiranja te identifikaciju trendova istraživanja u ovom dinamičnom području. Iako je kibernetička sigurnost u posljednje vrijeme sve važnija tema sjecišta tehnologije, ekonomije, menadžmenta i poslovanja, struktura istraživanja u ovom interdisciplinarnom polju nije dovoljno istražena. Ovaj rad popunjava navedenu istraživačku prazninu pružajući prvu sveobuhvatnu bibliometrijsku analizu i znanstveno mapiranje polja kibernetičke sigurnosti na sjecištu s ekonomijom, menadžmentom i poslovanjem.

U pregledu literature na platformi Web of Science Core Collection tek je jedan rad

koji se bavi mapiranjem područja kibernetičke sigurnosti i to u kibernetičko-fizičkim sustavima. Pourmadadkar et. al. identificiraju sedam klastera u području istraživanja kibernetičke sigurnosti u kibernetičko-fizičkim sustavima (Pourmadadkar et al., 2024). Ostali radovi koriste sustavne preglede, meta analize. Primjerice, Pandey et. al. identificiraju 16 kibernetičkih rizika u lancu opskrbe, rad nije klasteriranje već identifikacija rizika (Pandey et al., 2020). Abd et al. identificiraju istraživačka područja kibernetičke sigurnosti u lancima opskrbe kroz sustavni pregled literature (Abd Latif et al., 2021). Zadorozhnyi et al. identificiraju razine interakcija ekonomske i kibernetičke sigurnosti s naglaskom na računovodstvo (Zadorozhnyi et al., 2021). Nobrega et al. identificiraju, na temelju vojne znanosti, načine na koji organizacije mogu pristupiti kibernetičkoj obrani (Nobrega et al., 2024). Efimova et al. identificiraju evolucijski put pet generacija pristupa kibernetičkoj sigurnosti, od jednostavnijih reaktivnih do složenih proaktivnih strategija i tehnologija (Efimova et al., 2019). Iz objavljenih studija uočava se nedostatak mapiranja kibernetičke sigurnosti u području ekonomije, menadžmenta i poslovanja putem klasteriranja istraživačkog područja, budući da je samo je jedan rad u tom smislu prisutan, no ne u području ekonomije, menadžmenta i poslovanja (Pourmadadkar et al., 2016). Uočava se potreba da se pristupi klasteriranju istraživačkog polja kibernetičke sigurnosti upravo u području menadžmenta, ekonomije i poslovanja. Ovim istraživanjem pokriva se uočen znanstveni jaz. Stoga se kao cilj rada postavlja: IC 1. identificirati istraživačke klastere u području kibernetičke sigurnosti.

2. Metodologija

Koristiti će se kombinirani pristup: a) kvantitativna bibliometrijska analiza (deskriptivna analiza ključnih riječi: učestalost, ukupna snaga veza, citiranost, prosječna godina objave, prosječan normalizirani broj citata) te dodatno: b) kvalitativna analiza ključnih studija. Nakon klasteriranja identificirati će se značajniji radovi mjereno brojem citata i sadržajno pregledati radi dubljeg razumijevanja nalaza.

Kao izvor podataka koriste se publikacije objavljene u bazi Web of Science Core Collection (WoS CC). Ključna tema pretraživanja: „cyber security" i srodni pojmovi. Ovim procesom odabira uzorka u inicijalnim rezultatima identificirano je 28.669 dokumenata. Daljnjim filtriranjem skupa podataka odabrani su radovi područja ekonomije, menadžmenta i poslovanja, te dodatno radovi na engleskom jeziku. Odabiru se radovi vremenskog obuhvata od pojave prvog rada koji udovoljava kriterijima pretrage te sve do posljednjeg objavljenog rada u pretrazi dokumenata: od 2002. – 25. travnja 2025. Konačni uzorak čini: 777 znanstvenih radova.

Podaci su prethodno pročišćeni i normalizirani. Radi pročišćavanja podataka uklanjaju se sinonimi, odabire se frakcijsko brojanje (obzirom na različitost znanstvenih područja), od metoda koristi se: snaga asocijacije te ko-pojavljivanje ključnih riječi, ukupna snaga veza, normalizirani prosječan broj citata, prosječna godina objave. Od alata za analizu koristi se VOSviewer, verzija 1.6.20.

U uzorak se odabiru članci u časopisima, radovi s konferencija, poglavlja u knjigama te pregledni radovi. U obzir su uzete ključne riječi koje su autori studija navodili te ključne riječi koje Web of Science algoritamski dodaje. Odabranim skupom podataka (777 dokumenata dostupnih u punom zapisu) identificirati će se najznačajniji autori, institucije, zemlje te povezanost tema kibernetičke sigurnosti u području ekonomije, menadžmenta i poslovanja s pojedinim ciljevima održivosti Ujedinjenih naroda.

Nakon deskriptivne analize, izvršiti će se kvalitativan pregled najcitiranijih radova na tragu nalaza ove studije, radi produbljivanja razumijevanja samih nalaza te prijedloga za buduća istraživanja.

3. Rezultati i rasprava

Obradom podataka pomoću softvera Vosviewer postavljen je prag za ko-citiranje na 5 riječi. Identificirano je 205 ključnih riječi, daljnjim čišćenjem podataka od sinonima uklonjeno je 36 sinonima. U analizu ulazi 169 ključnih riječi. Identificirano je devet istraživačkih klastera:

a) Klaster 1 bavi najnovijim tehnologijama koje pokreću digitalnu transformaciju i njihovim sigurnosnim implikacijama. Klaster se usmjerava na primjenu ovih tehnologija u poslovnom kontekstu. Dominantni pojmovi su: blockchain, internet of things (IoT), cloud computing, big data, industry 4.0, industry 5.0, cyber-physical system, supply chain management. Primjerice, cloud computing ima izuzetno visok normalizirani broj citata (5.41), što ga čini jednom od najutjecajnijih tema u cijelom uzorku. Nadalje, industry 5.0: također vrlo utjecajan pojam (4.31) i relativno nov (2021.8).

b) Klaster 2 bavi se ljudskim faktorom, ponašanjem i percepcijom. Ovaj klaster je usmjeren na "ljudski zid" u cyber-sigurnosti. Istražuje kako individualno ponašanje, percepcija rizika, svijest i teorijski modeli (poput teorije zaštite motivacije) utječu na sigurnost. Ključni pojmovi u ovom klasteru su: awareness (svijest), behavior (ponašanje), trust (povjerenje), adoption (prihvaćanje), protection motivation theory, planned behavior, fear appeals, policy compliance (pridržavanje politika). Pojam fear appeals bilježi vrlo visok prosječan broj citata (90.14) i normaliziran (2.44), što ukazuje na utjecajnu nišu unutar ovog klastera. Idući pojam je planned behavior, također je izuzetno citiran pojam (103.16), iako nešto starijeg datuma (2017.1).

c) Klaster 3 bavi se upravljanjem rizicima, korporativnom upravljanju i poslovnom utjecaju. Fokusira se na to kako organizacije upravljaju cyber-rizicima, kakav je utjecaj sigurnosnih incidenata na poslovanje i tržište, te koje uloge imaju korporativno upravljanje i cyber-osiguranje. Ključni su pojmovi unutar ovog klastera: cyber risk, impact (utjecaj), governance (upravljanje), firms (poduzeća), insurance (osiguranje), market (tržište), data breach (povreda podataka), operational risk (operativni rizik). Pojam cyber risk jest najvažniji pojam u ovom klasteru, s najvećom učestalošću (44) i snagom veza (41).

Pojam impact je također vrlo centralan pojam, što je i očekivano za klaster kao što je ovaj.

d) Klaster 4 bavi se istraživanjima financijskog sektora, računovodstva i revizije. Prisutni su ključni pojmovi: banking, fintech, accounting, internal audit (interna revizija), digitalization, sustainability (održivost). Ovaj se klaster bavi primjenom i rizicima cyber-sigurnosti u financijskom sektoru. Pojmovi poput bankarstva, fintecha i računovodstva jasno definiraju ovu domenu. Interna revizija igra ključnu ulogu u osiguravanju kontrole.

e) Klaster 5 bavi se cyber-kriminalom, otpornosti i informacijskim sustavima. Ključni pojmovi su: cybercrime, cyberattack, resilience (otpornost), information systems, digital economy.

Ovaj klaster povezuje prijetnje (cyber-kriminal) s konceptom otpornosti sustava i širim kontekstom digitalne ekonomije.

Fokus je na razumijevanju kriminalnih aktivnosti i izgradnji sustava koji imaju sposobnost oporaviti se od napada. Temeljna je tema ovdje information systems, ima vrlo visok normalizirani broj citata (4.57), što ju čini temeljnom i utjecajnom temom. Također utjecajan pojam jest resilience (3.98).

f) Klaster 6 odnosi se na tehnički aspekti napada, ranjivosti i analizu rizika. Pojmovi koji se ovdje izučavaju su: attack, cyber-attack, security, vulnerability (ranjivost), risk analysis,

risk assessment. Ovo je u tehničkom smislu tzv. "obrambeni" klaster. Bavi se identificiranjem i analizom napada, procjenom ranjivosti i analizom rizika iz tehničke perspektive. Za razliku od klastera 3 koji je menadžerski, ovaj je više usmjeren na tehničku provedbu kibernetičke sigurnosti. Centralni pojam je security, jedan od najvažnijih pojmova u cijelom skupu podataka, s ogromnom snagom veza (120).

g) Klaster 7 usmjeren je na istraživanje primjene umjetne inteligencije i strojnog učenja u cyber-obrani. Ključni pojmovi koji obilježavaju ovo područje su: artificial intelligence (AI), machine learning, deep learning, network, mitigation (ublažavanje), intrusion detection (detekcija upada). Ovaj klaster je u potpunosti posvećen korištenju umjetne inteligencije i strojnog učenja za poboljšanje cyber-sigurnosti. Kao utjecajni pojmovi ovdje su identificirani: network (3.16 normaliziranih citata) te mitigation. Iako se ovaj pojam ne pojavljuje često, ima vrlo visok utjecaj (3.68).

h) Klaster 8 usmjeren je na sigurnost informacija, privatnost i ekonomske aspekte. Ključni pojmovi koje se unutar ovog klastera dominantno pojavljuju su information security, privacy (privatnost), data protection (zaštita podataka), computer security, economics. Ovaj klaster se bavi fundamentalnim konceptima sigurnosti informacija i zaštite podataka. Povezivanje s poljem ekonomije sugerira istraživanja o ekonomskim poticajima i troškovima ulaganja u sigurnost i privatnost. Teme uključuju automatsku detekciju upada, analizu mrežnog prometa i ublažavanje napada.

i) Klaster 9 se bavi temama kao što su: cyber-otpornost (cyber resilience). U ovom je klasteru prisutan samo jedan istaknuti pojam, cyber resilience, a osim njega i pojmovi phishing i ransomware koji se pojavljuju kao zasebni. Ovo je manji klaster. To sugerira zaključak da je ovo specifičan i važan koncept u nastajanju koji se povezuje s mnogim drugim temama, ali zadržava svoj jedinstveni fokus, a to je kibernetička otpornost.

Kada se sumiraju svi ovi nalazi mogu se prepoznati stupovi istraživačkog polja i najutjecajniji pojmovi:
cyber security: 271 pojavljivanja, TLS (Total Link Strength) 237
security: 124 pojavljivanja, TLS 120
information security: 64 pojavljivanja, TLS 63
management: 62 pojavljivanja, TLS 61
impact: 50 pojavljivanja, TLS 48
risk: 48 pojavljivanja, TLS 47.
Kao najutjecajniji pojmovi (metoda mjerenja: score<Avg. norm. citations) najveći prosječan broj citata, (obrazloženje: normaliziran i pouzdan) koji se pojavljuju u radovima koji su dobili najviše pažnje akademske zajednice su:
cloud computing (5.41)
knowledge management (5.19)
supply chain management (5.01)
information systems (4.57)
industry 5.0 (4.31)
big data analytics (4.30)
fear appeals (2.44) i planned behavior (2.61). Istraživanja koja povezuju cyber-sigurnost s primjenama u oblaku, upravljanjem lancem opskrbe i industrijskom automatizacijom su iznimno utjecajna.
Nadalje, pojmovi koji dominiraju u najnovijim radovima znanstvenika te pokazuju smjer u kojem se odabrano istraživačko polje kreće (pokazatelj: score<Avg. pub. year>) su:
hackers (2024.4) –
autonomous vehicles (2023.6)
firm performance (2023.2)
maturity model (2023.1)
data security (2023)
risks (2023)
barriers (2023).

Ovo su najnoviji istraživački trendovi (mjereno najvišom prosječnom godinom objave). Razdoblje objavljivanja radova koje je uključeno u ovu analizu (od 2002. do 2025. godine) može se na ovaj način prikazati:

a) Starije, temeljne teme (od 2015.-2018.): e-commerce (2015), terrorism (2015.7), cyber crime (2016.6), planned behavior (2017.16), globalization (2017.6). Ovo su temelji na kojima je polje izgrađeno.
b) Središnje, razvijene teme (od 2019.-2022.): Većina ključnih pojmova poput cyber security (2020.5), risk management (2020.7), blockchain (2021.8), impact (2021.9) i challenges (2022.2) spada u ovaj period. Ovo predstavlja glavninu trenutnih istraživanja.
c) Nove, nadolazeće teme (2022+): autonomous vehicles, barriers, data security, risk analysis, corporate governance, firm performance, fintech, cryptography, models, predstavljaju neke od novijih istraživačkih fronta.
Najznačajniji autori, institucije, zemlje prikazani su slijedećim tabelarnim prikazima tablice 1., 2. i 3.

Tablica 1. Autori s najvećim brojem radova

Autori	Broj radova
GREEN, J. S.	8
RENAUD, KAREN	7
CHEN, HSINCHUN	5
MAZZOCCOLI, ALESSANDRO	4
NUNAMAKER, JAY F. F.	4
FRANKE, ULRIK	4
KIM, DAN J.	4
CAPEK, JAN	4
DOUCEK, PETR	4
SCHOITSCH, ERWIN	4
ELING, MARTIN	4
JANKOVA, MARTINA	4

Izvor. Web of Science Core Collection

Tablica 1. prikazuje najznačajnije autore. Među prva tri identificirani su Green (8 radova), Renaud (7 radova) i Chen (5 radova).

Tablica 2. Najznačajnije zemlje

Zemlje	Broj radova
USA	173
ENGLAND	93
INDIA	54
PEOPLES R CHINA	42
AUSTRALIA	39
CZECH REPUBLIC	38
ROMANIA	35

Izvor. Web of Science Core Collection

Sjedinjene Američke države, prema tablici 2 su dominantna zemlja s najvećim doprinosom znanstvenika (173), mjereno brojem radova.

Povezanost tema kibernetičke sigurnosti u području ekonomije, menadžmenta i poslovanja s pojedinim ciljevima održivosti Ujedinjenih naroda prikazano je u tablici 3. Najviše radova pribraja se području industrijskih inovacija i infrastrukture (177), potom održivi gradovi i zajednice (121) te dobrom zdravlju i blagostanju (105). Zastupljenost ostalih najznačajnijih ciljeva prikazana je u tablici 3.

Tablica 3. Povezanost publikacija sa ciljevima održivosti Ujedinjenih naroda

Ciljevi održivosti Ujedinjenih naroda (SDG)	Broj radova
09 INDUSTRY INNOVATION AND INFRASTRUCTURE	177
11 SUSTAINABLE CITIES AND COMMUNITIES	121
03 GOOD HEALTH AND WELL BEING	105
12 RESPONSIBLE CONSUMPTION AND PRODUCTION	91
08 DECENT WORK AND ECONOMIC GROWTH	61

Izvor. Web of Science Core Collection

3.1. Rasprava

Rezultati analize ukazuju na višeslojnu strukturu istraživačkog polja. Obzirom da je identificirano devet klastera, dodatnim uvidom u najcitiranije radove pokušati će se produbiti razumijevanje nalaza u

kontekstu ekonomije, menadžmenta i poslovanja. U tri najcitiranija rada istraživači se bave lancima opskrbe i kibernetičkim rizicima, izravno povezujući cyber-phisical sustave s temom (Ghadge et al., 2020), (Pandey et al., 2020), s rizicima u globaliziranim lancima opskrbe u kontekstu Industrije 4.0 (Ghadge et al., 2020) te IoT kao jedan od četiri ključna elementa istraživanja u području kibernetičke sigurnosti i lanaca opskrbe (Abd Latif et al., 2021). Ovi nalazi su u području klastera 1 gdje se povezuje tehnološka osnova i njene napredne primjene (industrija 4.0/5.0, IoT, cloud computing, automation, smart manufacturing). U klasteru 2 koji se identificira kao „ljudski zid" u kibernetičkoj sigurnosti, prisutni su visoko citirani radovi, što ukazuje na zrelost istraživačkog područja. Ghadge, et al. (2020) navode "ljudske/bihevioralne elemente" kritične, no privukli su manje pažnje od tehničkih. Autori eksplicitno pozivaju na podizanje svijesti (awareness), što je središnji pojam klastera 2. Kumar et al. navode kako "uloga višeg menadžmenta" utječe na sigurnost, što je direktno povezano s organizacijskim ponašanjem i kulturom (S Kumar et al., 2021). Loonam, J. et al. fokusiraju se na strateško vodstvo i poticanje "nove kulturne svijesti" o kibernetičkoj otpornosti, što je srž ljudskih i organizacijskih faktora (Loonam et al., 2022). Klasteri 3 i 4 bave se upravljanjem rizicima, poslovnim utjecajima i financijama (cyber risk, governance, insurance, banking, terorrism, impact). U klasteru 3 identificirana je menadžerska perspektiva koja povezuje pojam sigurnost s financijskim posljedicama i upravljanjem. Ovo je snažno podržano radom Wanga koji istražuje optimizaciju ulaganja u sigurnost i kibernetičko osiguranje (Wang, 2019), radom Hua i Bapne koji tematiziraju ekonomski utjecaj kibernetičkog terorizma, što zanima menadžere (Hua & Bapna, 2013). Hoppe et al. analiziraju upravljanje kibernetičkim rizikom (cyber risk management) u malim i srednjim poduzećima, potvrđujući relevantnost ove teme za sve vrste poduzeća (Hoppe et al., 2021). Radovi u ovom klasteru su primjeri istraživanja koja "prevode" tehničke probleme kibernetičke sigurnosti na jezik poslovanja: kroz pojmove rizik, trošak, osiguranje i utjecaj na performanse poduzeća. Klasteri 5, 6, 8 i 9 bave se temeljnim konceptima kibernetičke sigurnosti kao što su prijetnje, otpornost, sigurnost informacija). Choras et al. identificiraju taksonomiju kibernetičkih prijetnji koje utječu na kritične infrastrukture, što je temeljni doprinos razumijevanju pojmova iz klastera 5 i 6 (Choras et al., 2016). Klaster 7 bavi se umjetnom inteligencijom i strojnim učenjem, a umjetna inteligencija može pridonijeti detekciji i smanjenju kibernetičkih prijetnji (Havryliuk, 2023). Pourmadadkar et al. u bibliometrijskoj analizi identificiraju fokuse prema kibernetičko-fizičkim sustavima u kritičnim infrastrukturama i teme poput ranjivosti, napada i otpornosti (Pourmadadkar et al., 2024). Autori Ghadge et al. predstavljaju kibernetičku otpornost (cyber resilience) kao ključni cilj, potvrđujući važnost ovdje identificiranog klastera 9 (Ghadge et al., 2020).

Slijedeće aktivnosti pridonose kibernetičkoj sigurnosti u području ekonomije, menadžmenta i poslovanja:
a) Integracija sigurnosti u menadžerske funkcije kako bi se povećala svijest i osigurala zaštita (Korcek et al., 2017).
b) Nacionalne strategije i politike: potreba razvoja nacionalnih strategija kibernetičke sigurnosti ključna je za stvaranje održivog i sigurnog digitalnog ekosustava (Stitilis et al., 2016).
c) Potreba zaštite kritičnih infrastruktura u osiguranju kibernetičke i fizičke sigurnosti (Choras et al., 2016).
d) Uključivanje psihologije u edukaciju pomaže stručnjacima da bolje razumiju motivaciju napadača i ponašanje korisnika (Lois et al., 2021).

e) Pridržavanje sigurnosnih politika (Compliance). Učinkovitost ovisi o tome koliko zaposlenici (posebno oni koji rade na daljinu) razumiju i pridržavaju se sigurnosnih politika (Nyarko & Fong, 2023).
f) Korištenje umjetne inteligencije nudi značajan potencijal za osiguranje poslovanja kroz automatiziranu detekciju i minimizaciju prijetnji (Havryliuk et al., 2023).
g) Podatkovno vođeni sustavi i algoritmi. Razvoj sigurnosnih sustava temeljenih na podacima i analitičkim algoritmima omogućuje precizniju i učinkovitiju obranu (Efimova et al., 2019).
h) Optimalno ulaganje i kibernetičko osiguranje: kombinacija optimalnog ulaganja i prilagođenog kibernetičkog osiguranja je najučinkovitiji način upravljanja rizikom (Wang, 2019).
i) Kvantifikacija rizika (Cyber Value at Risk): Korištenje metrika poput Cy-VaR omogućuje organizacijama da kvantificiraju gubitke i donose informirane odluke o ulaganjima (Orlando, 2021).
j) Postojanje pravnih posljedica, "pravne posljedice" su, uz tehničke mjere, najvažniji pokretač koji potiče organizacije na poboljšanje sigurnosti (S. Kumar et al., 2021).
k) Zakoni i propisi, jasno definirani zakoni i propisi na nacionalnoj razini predstavljaju temelj za osiguranje kibernetičke sigurnosti (Guo & Destech Publicat, 2016).

3.2. Prijedlog za buduća istraživanja kibernetičke sigurnosti u području ekonomije, menadžmenta i poslovanja

Nekoliko se ključnih budućih istraživačkih fronti može identificirati u utjecajnim radovima ovog istraživačkog polja: razvoj empirijskih modela za upravljanje lancima opskrbe i s tim povezanim sustavima, radi razvoja standardiziranih politika i suradničkih strategija među parterima u lancu (Ghadge et al., 2020). Identifikacija rizika (opskrbni, operativni i potražni) i njihov utjecaj na kontinuitet poslovanja lanca opskrbe i razvoj specifičnih strategija za ublažavanje svakog od navedenih tipova rizika (Pandey et al., 2020). Istraživanje veza percepcija, znanja, stavova i procesa upravljanja kibernetičkim rizikom kroz empirijske studije (Hoppe et al., 2021).
Buduće intervencije za sprječavanje napada "iznutra" (od strane zaposlenika) trebale bi se preusmjeriti s općenitih prijetnji kaznama na specifične intervencije koje smanjuju ili ublažavaju stres ("strain") zaposlenika, ovisno o fazi u kojoj se nalaze na putu prema zlonamjernom ponašanju (Johnston et al., 2024). Poboljšanje integracije kibernetičke sigurnosti u cjelokupnu strategiju upravljanja rizicima (Hoppe et al., 2021). Razvoj stohastičkih igara kibernetičke sigurnosti koje treba i nadalje razvijati. Igre temeljene na prometu trebaju se proširivati na zračni, kopneni i pomorski promet (Hausken et al., 2024).
Pokretanje daljnjih istraživanja u smjeru razvoja računovodstvene metodologije za identifikaciju i procjenu ekonomskih gubitaka koje poduzeće snosi kao posljedicu kibernetičkih rizika (Zadorozhnyi et al., 2021).
Ograničenja istraživanja: analiza je temeljena samo na jednoj bazi podataka (Web of Science CC), kvalitativni dio je interpretativan i usmjeren na najcitiranije radove, ne na sve radove.

4. Zaključak

Temeljem analize prethodnih studija objavljenih na Web of Science Core Colletion bazi nije identificirano mapiranje kibernetičke sigurnosti u području ekonomije, menadžmenta i poslovanja. Ovaj rad predstavlja prvi doprinos utvrđenoj problematici. Bibliometrijskom analizom dokumenata objavljenih u Web of Science Core Collection bazi o kibernetičkoj sigurnosti u području ekonomije, menadžmenta i poslovanja otkriveno je dinamično i multidisciplinarno istraživačko polje, strukturirano u devet klastera. Rezultati pokazuju da se suvremena istraživanja

kreću od tehnoloških pokretača poput blockchaina, IoT-a i Industrije 5.0, preko "ljudskog zida" koji istražuje bihevioralne aspekte i psihologiju, do menadžerskih disciplina kao što su upravljanje rizicima, korporativno upravljanje i financije. Iako su pojmovi poput cyber security i security centralni, najutjecajnija su istraživanja usmjerena na primijenjivost tehnologija kao što su cloud computing i supply chain management, što ukazuje na važnost praktične implementacije u poslovnom kontekstu. Analizom trendova potvrđena je evolucija polja od temeljnih koncepata prema novim istraživačkim frontama. Dok su starije teme poput e-commerce identificirane kao temeljne, nova istraživanja fokus usmjeravaju prema konceptima kao što su autonomous vehicles, firm performance i maturity models. Povezanost objavljenih radova s ciljevima održivog razvoja, Ujedinjenih naroda, posebice s industrijom, inovacijama i infrastrukturom, dodatno naglašava stratešku važnost kibernetičke sigurnosti za globalni napredak.

Na temelju provedene analize, buduća istraživanja trebala bi se usmjeriti na četiri ključna područja: 1) razvoj empirijskih modela za upravljanje rizicima u složenim sustavima poput lanaca opskrbe; 2) dublje istraživanje ljudskog faktora, s fokusom na prevenciju internih prijetnji kroz razumijevanje psiholoških pokretača; 3) stvaranje standardiziranih računovodstvenih i financijskih metodologija za kvantifikaciju ekonomskog utjecaja kibernetičkih incidenata te 4) ulogu strateškog menadžmenta u stvaranju kulture u podizanju svijesti o rizicima, budući da se je „ljudski zid" u kibernetičkoj sigurnosti pokazao značajnim u nalazima istraživača. Ovaj pristup omogućiti će potpunu integraciju kibernetičke sigurnosti u strateško odlučivanje, operativno poslovanje, oblikovanje specifične kulture ponašanja u organizacijama kada su u pitanju kibernetički izazovi, prevodeći tehničke rizike u mjerljiv poslovni jezik.

5. Literatura

Abd Latif, M., Abd Aziz, N., Hussin, N., & Aziz, Z. (2021). CYBER SECURITY IN SUPPLY CHAIN MANAGEMENT: A SYSTEMATIC REVIEW [Review]. LOGFORUM, 17(1), 49-57. https://doi.org/10.17270/J.LOG.2021.555

Choras, M., Kozik, R., Flizikowski, A., Holubowicz, W., & Renk, R. (2016). Cyber Threats Impacting Critical Infrastructures. In R. Setola, V. Rosato, E. Kyriakides, & E. Rome (Eds.), Managing the Complexity of Critical Infrastructures: A Modelling and Simulation Approach (Vol. 90, pp. 139-161). Springer International Publishing Ag. https://doi.org/10.1007/978-3-319-51043-9_7

Efimova, Y., Gavrilov, A., & Svirina, A. (2019, Nov 13-14). Data Driven Cyber-Security Corporate Systems: Development and Implementation. [Vision 2025: Education excellence and management of innovations through sustainable economic competitive advantage]. 34th International-Business-Information-Management-Association (IBIMA) Conference, Madrid, SPAIN.

Ghadge, A., Weiss, M., Caldwell, N., & Wilding, R. (2020). Managing cyber risk in supply chains: a review and research agenda [Review]. Supply Chain Management-an International Journal, 25(2), 223-240. https://doi.org/10.1108/SCM-10-2018-0357

Guo, Y. M., & Destech Publicat, I. (2016, Jan 15-17). Cyber Information Security: An Increasingly Important Concern in China. [2016 international conference on business and management (icbm 2016)]. International Conference on Business and Management (ICBM), Shenzhen, PEOPLES R CHINA.

Hausken, K., Welburn, J., & Zhuang, J. (2024). A Review of Attacker-Defender Games and Cyber Security [Review]. Games, 15(4), Article 28. https://doi.org/10.3390/g15040028

Havryliuk, O., Yakushev, O., Petchenko, M., Zachosova, N., Bielialov, T., & Kozlovska, S. (2023). CYBER SECURITY AND ARTIFICIAL INTELLIGENCE IN THE CONTEXT OF ENSURING BUSINESS SECURITY IN WARTIME. FINANCIAL AND CREDIT ACTIVITY-PROBLEMS OF THEORY AND PRACTICE, 6(53), 451-459. https://doi.org/10.55643/fcaptp.6.53.2023.4130

Hoppe, F., Gatzert, N., & Gruner, P. (2021). Cyber risk management in SMEs: insights from industry surveys. Journal of Risk Finance, 22(3-4), 240-260. https://doi.org/10.1108/jrf-02-2020-0024

Hua, J., & Bapna, S. (2013). The economic impact of cyber terrorism. Journal of Strategic Information Systems, 22(2), 175-186. https://doi.org/10.1016/j.jsis.2012.10.004

Johnston, A., Goel, S., & Williams, K. (2024). From cyber benign to cyber malicious: unveiling the evolution of insider cyber maliciousness from a stage theory perspective [Article; Early Access]. European Journal of Information Systems. https://doi.org/10.1080/0960085X.2024.2413072

Korcek, F., Mlynarovic, V., Romanová, T., & Benová, M. (2017, Apr 04-06). Integration of Cyber Security Concepts into the Functions of Management. [International scientific conference for doctoral students and post-doctoral scholars (edamba 2017)]. International Scientific Conference for Doctoral Students and Post-Doctoral Scholars (EDAMBA): Knowledge and Skills for Sustainable Development - The Role of Economics, Business, Management and Related Disciplines, Univ Econ Bratislava, Bratislava, SLOVAKIA.

Kumar, S., Biswas, B., Bhatia, M., & Dora, M. (2021). Antecedents for enhanced level of cyber-security in organisations [Article]. Journal of Enterprise Information Management, 34(6), 1597-1629. https://doi.org/10.1108/JEIM-06-2020-0240

Kumar, S., Biswas, B., Bhatia, M. S., & Dora, M. (2021). Antecedents for enhanced level of cyber-security in organisations. Journal of Enterprise Information Management, 34(6), 1597-1629. https://doi.org/10.1108/jeim-06-2020-0240

Lois, P., Drogalas, G., Karagiorgos, A., Thrassou, A., & Vrontis, D. (2021). Internal auditing and cyber security: audit role and procedural contribution. INTERNATIONAL JOURNAL OF MANAGERIAL AND FINANCIAL ACCOUNTING, 13(1), 25-47. <Go to ISI>://WOS:000674963400002

Loonam, J., Zwiegelaar, J., Kumar, V., & Booth, C. (2022). Cyber-Resiliency for Digital Enterprises: A Strategic Leadership Perspective. Ieee Transactions on Engineering Management, 69(6), 3757-3770. https://doi.org/10.1109/tem.2020.2996175

Nobrega, K., Rutkowski, A., & Saunders, C. (2024). The whole of cyber defense: Syncing practice and theory [Article]. Journal of Strategic Information Systems, 33(4), Article 101861. https://doi.org/10.1016/j.jsis.2024.101861

Nyarko, D., & Fong, R. (2023, 2023-01-01). Cyber Security Compliance Among Remote Workers. CYBERSECURITY IN THE AGE OF SMART SOCIETIES, 2022, GEWERBESTRASSE 11, CHAM, CH-6330, SWITZERLAND.

Orlando, A. (2021). Cyber Risk Quantification: Investigating the Role of Cyber Value at Risk. Risks, 9(10), 12, Article 184. https://doi.org/10.3390/risks9100184

Pandey, S., Singh, R., Gunasekaran, A., & Kaushik, A. (2020). Cyber security risks in globalized supply chains: conceptual framework [Article]. JOURNAL OF GLOBAL OPERATIONS AND STRATEGIC SOURCING, 13(1), 103-128. https://doi.org/10.1108/JGOSS-05-2019-0042

Pourmadadkar, M., Lezzi, M., & Corallo, A. (2024). Cyber Security for Cyber-Physical Systems in Critical Infrastructures: Bibliometrics Analysis and Future Directions. Ieee Transactions on Engineering Management, 71, 15405-15421. https://doi.org/10.1109/tem.2024.3489273

Stitilis, D., Pakutinskas, P., & Malinauskaite, I. (2016). PRECONDITIONS OF SUSTAINABLE ECOSYSTEM: CYBER SECURITY POLICY AND STRATEGIES. Entrepreneurship and Sustainability Issues, 4(2), 174-182. https://doi.org/10.9770/jesi.2016.4.2(5)

Wang, S. S. (2019). Integrated framework for information security investment and cyber insurance. Pacific-Basin Finance Journal, 57, 12, Article 101173. https://doi.org/10.1016/j.pacfin.2019.101173

Zadorozhnyi, Z., Muravskyi, V., Shevchuk, O., & Bryk, M. (2021). INNOVATIVE ACCOUNTING METHODOLOGY OF ENSURING THE INTERACTION OF ECONOMIC AND CYBERSECURITY OF ENTERPRISES [Article]. Marketing and Management of Innovations(4), 36-46. https://doi.org/10.21272/mmi.2021.4-03

SCIENCE MAPPING AND RESEARCH TRENDS IN CYBERSECURITY WITHIN ECONOMICS, MANAGEMENT AND BUSINESS

Abstract: In recent years, cybersecurity has emerged as a critical topic at the intersection of technology, economics, and management; however, the intellectual structure of this interdisciplinary field is not always clearly defined. Research trends in cybersecurity are increasingly directed towards topics such as risk, resilience, cryptography, blockchain technology, machine learning, and Industry 5.0. The aim of this paper is to identify key research clusters in the field of cybersecurity, with a specific focus on its intersection with economics, management and business. A search of the Web of Science database using the keyword "cyber security" and its variants yielded 28,669 documents. By filtering for the research areas of economics, management, and business, a final sample of 777 studies published between 2002 and April 2025 was obtained. The analysis considered both author-provided keywords and the algorithmically assigned Keywords Plus®. The dataset was subsequently cleansed and normalized to ensure consistency. Using VOSviewer software, a co-occurrence analysis of keywords was performed with the fractional counting method to identify research clusters, revealing the frequency, co-occurrence, and total link strength among key topics. The analysis identified nine research clusters, the most prominent authors, institutions, and countries, as well as the alignment of cybersecurity topics with the United Nations Sustainable Development Goals.

Keywords: keyword analysis, economics, cybersecurity, management, visualization, science mapping