Festung

Časopis za interdisciplinarna istraživanja u poslovanju

Godište 1, Broj 2/2025

Slavonski Brod, Listopad, 2025.
ISSN 3102-1107

FESTUNG - časopis za interdisciplinarna istraživanja u poslovanju

Nakladnik / Publisher

Sveučilište u Slavonskom Brodu

University of Slavonski Brod

Glavni i odgovorni urednik / Editor-in-Chief:

Mirko COBOVIĆ

Zamjenice glavnog urednika / Deputy Editor-in-Chief:

Maja VRETENAR COBOVIĆ

Lena SIGURNJAK

Sanja KNEŽEVIĆ KUŠLJIĆ

Počasni urednik / Honorary Editor

Antun STOIĆ

Tehnička urednica / Technical Editor

Ivana LOVRIĆ SENJAK

ISSN: 3102-1107

Urednički odbor / Editorial Board:

Marinko STOJKOV, Matilda KOLIĆ STANIĆ, Sara HAVRLIŠAN, Željka ROSANDIĆ (svi sa Sveučilišta u Slavonskom Brodu), Tomislav MATIĆ (Fakultet elektrotehnike računarstva i informacijskih tehnologija Osijek), Tomislav MATIĆ (Fakultet elektrotehnike računarstva i informacijskih tehnologija Osijek), Jerko GLAVAŠ (Ekonomski fakultet u Osijeku), Hrvoje SERDARUŠIĆ (Ekonomski fakultet u Osijeku), Ljiljana ZEKANOVIĆ KORONA (Sveučilište u Zadru), Jurica BOSNA (Sveučilište u Zadru), Kristian ĐOKIĆ (Fakultet turizma i ruralnog razvoja u Požegi), Dejan TUBIĆ (Veleučilište u Virovitici), Nikola PAPAC (Ekonomski fakultet Sveučilišta u Mostaru, Bosna i Hercegovina),Željko VOJINOVIĆ (Ekonomski fakultet Subotica, Srbija), Abdelhamid NECHAD (Abdelmalek Essaadi University, Morocco), Tai FEI (Fachhochschule Dortmund, University of Applied Sciences and Arts, Germany)

Savjetodavni odbor / Advisory Board

Ivan SAMARDŽIĆ, Goran ŠIMUNOVIĆ (svi sa Sveučilišta u Slavonskom Brodu), Željko HOCENSKI, Franjo JOVIĆ (Fakultet elektrotehnike računarstva i informacijskih tehnologija Osijek), Branko MATIĆ (Ekonomski fakultet u Osijeku)

Adresa uredništva / Address

Sveučilište u Slavonskom Brodu

University of Slavonski Brod

Ulica 108. brigade ZNG 36, 35000 Slavonski Brod, Croatia

Telefon: +385 35 492 633

ePošta: festung@unisb.hr

https://journal-festung.com/

Časopis Festung

Časopis pruža platformu za diseminaciju najnovijih istraživanja i spoznaja stručnjaka iz područja društvenih i tehničkih znanosti, s posebnim naglaskom na teme iz gospodarstva, ekonomije, poslovanja te kibernetičke sigurnosti. Publikacijom odabranih radova, časopis Festung doprinosi širenju znanja i potiče daljnju raspravu o aktualnim izazovima i prilikama u navedenim područjima. Radovi zaprimljeni na objavu strogo su kontrolirani te samo oni iznimno dobre kvalitete, a koji su u skladu s temama iz područja časopisa, se upućuju na postupak dvostruke slijepe recenzije.

Recenzija:

Vanjske recenzije, podjednako tuzemna i inozemna, samo znanstveni i stručni radovi, dvostruko slijepa.

Područja pokrivanja:

Interdisciplinarno područje društvenih, tehničkih i prirodnih znanosti, odnosno polja ekonomije, informacijskih znanosti, računarstva, elektrotehnike, strojarstva i matematike te srodnih područja vezana uz istraživanje u poslovanju

Jezik:

Radovi se objavljuju na hrvatskom ili engleskom jeziku.

Zaprimanje radova:

Radovi se uredništvu dostavljaju isključivo u elektroničkom obliku putem e-mail adrese: festung@unisb.hr

Prilozi objavljeni u Časopisu referiraju se u:

Hrčak – Portal znanstvenih časopisa Republike Hrvatske (MZO, Srce & HIDD)

Prava korištenja:

Časopis je u otvorenom pristupu. Radovi objavljeni u znanstvenom časopisu Festung - časopis za interdisciplinarna istraživanja u poslovanju besplatno se smiju koristiti za svaku svrhu uz poštivanje autorskih prava autora i izdavača te navođenje izvora. Ova odredba u skladu je s CC BY-NC-ND 4.0. licencom (Creative Commons Attribution Non-Commercial 4.0 International licence) dostupno na https://creativecommons.org/licenses/by-nc-nd/4.0/

Copyright© 2025.

Sveučilište u Slavonskom Brodu – Sva prava pridržana

Prva godina izlaženja: 2025

Časopis izlazi četiri puta godišnje.

CYBER FESTUNG

SVEUČILIŠTE U SLAVONSKOM BRODU

Ulica 108. brigade ZNG 36 | tel: +385 35 446 188 | OIB: 3302783437

35000 Slavonski Brod | https://festung.unisb.hr/ | IBAN:HR0923400091111084627

Časopis Festung proizašao je iz aktivnosti projekta Cyber Festung

Projekt FSTP-OI-22: Cyber Festung Sveučilišta u Slavonskom Brodu ima za cilj povećati svijest o kibernetičkoj sigurnosti među građanima i organizacijama. Kroz istraživanje, analize, edukaciju, simulacije i druge aktivnosti, projekt će jačati otpornost na cyber napade. Ciljne skupine su zaposlenici, studenti, učenici i poslodavci. Očekivani rezultati su bolja zaštita podataka, povećana svijest o rizicima i jača suradnja između različitih dionika u području kibernetičke sigurnosti.

Stopa sufinanciranja ovog projekta iznosi 100% ukupnih prihvatljivih troškova projekta navedenih u sklopu projektne prijave. 50% ukupnih prihvatljivih troškova podmiruje Europska unija, 50% Erste banka.

https://festung.unisb.hr/

SADRŽAJ

Izvorni znanstveni radovi

KOMPARATIVNA ANALIZA FINANCIRANJA ZDRAVSTVA U HRVATSKOJ U ODNOSU NA ZEMLJE ČLANICE EU-a

Sanja Pešić, Mirko Pešić _____ 85

UMJETNA INTELIGENCIJA I KIBERNETIČKA SIGURNOST: STAVOVI ZAPOSLENIKA I IZAZOVI ZA SUVREMENA PODUZEĆA

Ivana Miklošević, Gabrijela Bosak _____ 95

OZBILJNE IGRE O KIBERNETIČKOJ SIGURNOSTI U KURIKULUMU NASTAVE INFORMATIKE

Ivana Lovrić Senjak, Slavko Dukarić, Mihovil Gašić _____ 107

Prethodna priopćenja

MARKETINŠKE STRATEGIJE I SIGURNOSNI IZAZOVI U FAZI LANSIRANJA DIGITALNOG BANKARSKOG PROIZVODA _____ *115*

Mirjana Kraljević, Andreja Katolik Kovačević _____ 115

Pregledni radovi

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

Višnja Bartolović, Donata Pospišil, Milan Puvača _____ 123

RAZVOJ PAMETNIH GRADOVA

Anita Kulaš Mirosavljević, Valentina Vuleta _____ 135

ULOGA KIBERNETIČKE SIGURNOSTI U JAČANJU REGIONALNE GOSPODARSKE OTPORNOSTI: INSTITUCIONALNE I GEOPOLITIČKE PERSPEKTIVE

Sanela Ravlić, Ivana Unukić _____ 143

Stručni radovi

KIBERNETIČKA SIGURNOST INDUSTRIJSKIH SUSTAVA

Mato Galović, Ivan Matasović, Mato Kokanović, Zoran Crnac _____ 151

Uvodna riječ glavnog urednika

Poštovane čitateljice, poštovani čitatelji,

S ponosom vam predstavljamo prvi broj časopisa FESTUNG – časopis za interdisciplinarna istraživanja u poslovanju, izdanje Sveučilišta u Slavonskom Brodu. Rođenje svakog novog znanstvenog časopisa predstavlja značajan događaj za akademsku zajednicu, a za nas, na Sveučilištu u Slavonskom Brodu, to je posebno uzbudljiv trenutak koji svjedoči o našoj predanosti razvoju znanosti, poticanju inovacija i širenju znanja.

Naziv "Festung" nije slučajno odabran. On simbolizira snagu, stabilnost i uporište – sve ono što želimo da naš časopis predstavlja u svijetu znanstvene publikacije. Naša vizija je stvoriti platformu koja će okupljati istraživače iz različitih disciplina, poticati interdisciplinarnost i promicati originalna znanstvena dostignuća. U današnjem složenom svijetu, problemi rijetko pripadaju samo jednoj znanstvenoj grani. Stoga je časopis zamišljen kao most koji spaja različite perspektive i metodologije, omogućujući dublje razumijevanje suvremenih izazova u poslovanju i šire.

U ovom prvom broju donosimo vam selekciju radova koji odražavaju širinu naših interesa i predanost kvaliteti. Svaki objavljeni članak prošao je strogi postupak recenzije, što jamči njegovu znanstvenu utemeljenost i doprinos struci. Ovim putem želim zahvaliti svim autorima na povjerenju koje su nam ukazali svojim vrijednim rukopisima, kao i cijenjenim recenzentima na njihovom predanom radu i neprocjenjivom doprinosu kvaliteti ovog izdanja.

Posebnu zahvalnost upućujem našem Uredničkom i Savjetodavnom odboru, čija su znanja, iskustva i angažman bili ključni u oblikovanju uredničke politike i osiguravanju visokih standarda. Njihova podrška temelj je na kojem gradimo budućnost časopisa. Također, neizostavna je podrška našeg izdavača, Sveučilišta u Slavonskom Brodu, bez koje ovaj projekt ne bi bio ostvariv.

Pred nama je uzbudljiv put. Časopis Festung će težiti tome da postane prepoznatljiv časopis na nacionalnoj i međunarodnoj razini, indeksiran u relevantnim bazama podataka, čime će se osigurati široka dostupnost i vidljivost objavljenih radova. Pozivamo sve istraživače da nam se pridruže u ovoj misiji i svojim radovima doprinesu bogatstvu budućih brojeva.

Nadam se da ćete uživati u čitanju ovog prvog broja i pronaći inspiraciju za nova istraživanja. Vjerujem da će Festung postati nezaobilazna platforma za sve koji se bave interdisciplinarnim istraživanjima u poslovanju i šire.

S poštovanjem,

Glavni urednik

Mirko Čobović

Ovaj rad je licenciran pod Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International.

Zaprimljen: 7.9.2025.
Odobren za objavu: 13.10.2025.
Izvorni znanstveni rad

KOMPARATIVNA ANALIZA FINANCIRANJA ZDRAVSTVA U HRVATSKOJ U ODNOSU NA ZEMLJE ČLANICE EU-a

Sanja Pešić[1], Mirko Pešić[2]
[1]Fakultet za dentalnu medicinu i zdravstvo, Crkvena ulica 21, 31000 Osijek, Hrvatska
ePošta: spesic@fdmz.hr
[2]Medicinski fakultet Osijek, Josipa Huttlera 4, 31000 Osijek, Hrvatska
ePošta: mpesic@mefos.hr

Sažetak: Cilj ovog rada je analizirati financiranje hrvatskog zdravstvenog sustava u usporedbi s prosjekom Europske unije. Glavni odabrani indikatori korišteni za analizu su ukupni izdaci za zdravstvo, izdaci po glavi stanovnika i izdaci izraženi kao postotak od BDP-a. Analiza je provedena na temelju podataka Eurostata za 27 država članica Europske unije u razdoblju od 2015. do 2022. godine uz primjenu deskriptivne statističke metode, komparativne analize, analize varijance (ANOVA), Tukey HSD post-hoc testa, korelacijske analize te analize složene godišnje stope rasta (CAGR). Dobiveni rezultati pokazuju da se Hrvatska nalazi ispod prosjeka EU prema svim ključnim indikatorima. Ukupni izdaci i izdaci po glavi stanovnika u Hrvatskoj znatno su niži od europskog prosjeka, kao i udio izdataka za zdravstvo u BDP-u. ANOVA analiza potvrdila je postojanje statistički značajnih razlika među skupinama država, pri čemu je Hrvatska svrstana u skupinu zemalja s nižim izdvajanjima odnosno izdacima za zdravstvo. Iako Hrvatska bilježi brži rast zdravstvene potrošnje od prosjeka EU, polazi s niže baze izdvajanja, što održava jaz u odnosu na razvijenije zemlje članice. Rezultati naglašavaju potrebu za reformama usmjerenima na povećanje učinkovitosti i održivosti zdravstvenog financiranja u Hrvatskoj.

Ključne riječi: financiranje zdravstva, izdaci za zdravstvo, učinkovitost financiranja

1. Uvod

Financiranje zdravstvenih sustava jedna je od aktualnijih tema u gotovo svim državama svijeta, posebno razvijenijim, jer izravno utječe na dostupnost i održivost zdravstvene zaštite. Jedna od važnih posljedica gospodarskog razvoja je kontinuirana potražnja za zdravstvenim uslugama koje se preslikavaju na potrošnju zdravstva (Kovač i Smolić, 2021). Ovdje se dodatno ističe i model univerzalne zdravstvene pokrivenosti, koji posebno potiču Svjetska zdravstvena organizacija i Ujedinjeni narodi, i kao takav postao je primaran za sve zdravstvene sustave. Upravo zato države članice Europske unije nastoje pratiti načelo univerzalne pokrivenosti i dostupnosti zdravstvene zaštite, međutim, modeli financiranja i ulaganja u zdravstvene sustave bitno se razlikuje među njima (Thomson i sur., 2022.). Uzimajući u obzir trenutnu razinu javnog duga i državne izdatke vezane za starenje stanovništva, gotovo sve države članice Europske unije, uključujući i Hrvatsku, morat će se suočiti sa izazovima upravljanja troškovima (European Commission, 2019). Hrvatska je među zemljama kod kojih prevladavaju javni izvori financiranja, primarno kroz sustav obveznog zdravstvenog osiguranja (Vončina i sur., 2007.; WHO, 2021.). Ovakav model financiranja poznat je pod nazivom Bismarckov model financiranja. On omogućuje visoku razinu dostupnosti zdravstvene zaštite ali dovodi u pitanje održivost, posebno uzimajući u obzir činjenicu starenja stanovništva (European Commission, 2021).

Promatrajući sve aspekte financiranja, Hrvatska izdvaja daleko manja sredstva za zdravstvenu zaštitu od prosjeka Europske unije. Hrvatska zaostaje za prosjekom Europske unije i u ukupnom iznosu financiranja zdravstva, i u financiranju po glavi stanovnika i u financiranju iskazanom kao postotak od BDP-a. S obzirom na veliko oslanjanje na sustav javnog financiranja, ovakav podatak je zabrinjavajući u kontekstu hrvatskog zdravstvenog sustava. Hrvatski zdravstveni sustav, koji je snažno oslonjen na javne izvore financiranja, dodatno se suočava sa izazovima učinkovitosti sustava i racionalnog korištenja resursa, što predstavlja dodatni problem za državu (WHO, 2021; Kaštelan Brumen i sur., 2022).

Cilj rada je analiza financiranja hrvatskog zdravstvenog sustava u odnosu na prosjek Europske unije koristeći se podacima Eurostata. Analiza je posebno usmjerena na ukupnu zdravstvenu potrošnju, potrošnju po glavi stanovnika i potrošnju za zdravstvo u odnosu na visinu BDP-a. Dodatno će se prikazati omjer javnog i privatnog izdvajanja za zdravstvo kako bi se dobio dodatni uvid u poziciju Hrvatske u odnosu na druge države članice.

2. Metodologija

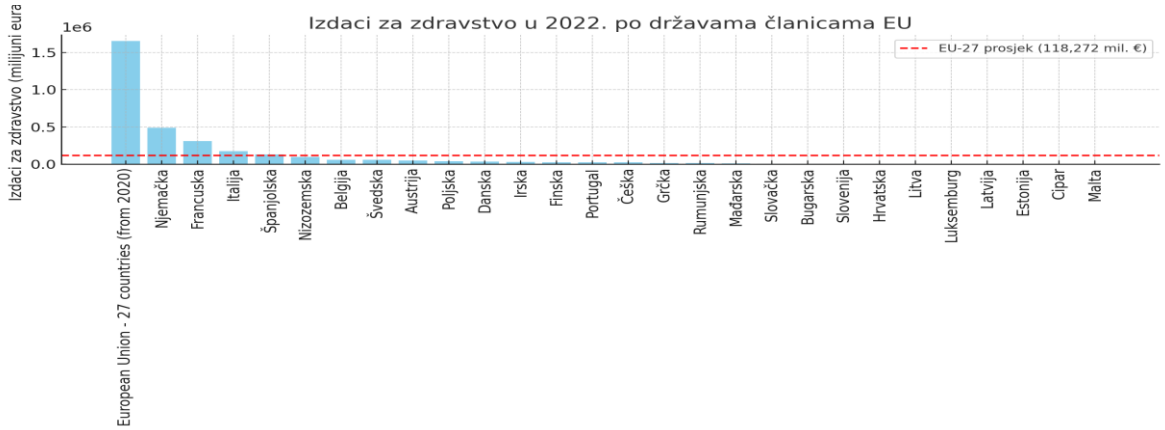
Metodologija rada bazira se na komparativnoj analizi kvantitativnih podataka o financiranju zdravstvenih sustava zemalja članica Europske unije u usporedbi sa Hrvatskom. Prikazat će se pregled razlika i sličnosti u strukturi zdravstvene potrošnje te trendovi financiranja zdravstva u Hrvatskoj u odnosu na druge zemlje članice Europske unije. Obuhvat istraživanja uključuje podatke 27 zemlja članica sa službene stranice Eurostata (poveznica: https://ec.europa.eu/eurostat/web/health/database?node_code=hlth_sha11) u razdoblju 2015. do 2022. godina (iako su dostupni podaci i za 2023. i 2024. godinu, isti nisu potpuni, stoga se radi dobivanja bolje slike koristila 2022. godina kao referentna). Ovo ujedno predstavlja i ograničenje istraživanja. Podaci koji su korišteni odnose se na ukupne izdatke za zdravstvo (u milijunima eura), izdatke po glavi stanovnika (u EUR), izdatke iskazane kao postotak BDP-a, te odnos financiranja iz državnog proračuna, obveznog zdravstvenog osiguranja i izravnih plaćanja građana. Korištene statističke metode obuhvaćaju deskriptivnu statistiku kojom su dobivene osnovne mjere središnje tendencije i varijabilnosti (aritmetička sredina, medijan, standardna devijacija, minimum i maksimum) za sve promatrane pokazatelje čime je dobiven pregled osnovnih obilježja podataka. Komparativnom analizom podaci za Hrvatsku uspoređeni su sa prosjekom ostalih zemalja članica EU te je Hrvatska rangirana u odnosu na druge članice prema ukupnoj zdravstvenoj potrošnji, potrošnji po glavi stanovnika i potrošnji prema udjelu u ukupnom BDP-u. Korelacijskom analizom pomoću Pearsonovog koeficijenta korelacije ispitana je povezanost izdataka za zdravstvo po glavi stanovnika i kao udio u ukupnom BDP-u u Hrvatskoj u odnosu na prosjek Europske unije. Analizom varijance (ANOVA) testirano je postoje li statistički značajne razlike u zdravstvenoj potrošnji u odnosu na postotak BDP-a između Hrvatske i ostalih zemalja članica EU. Primijenjen je i Tukey HSD post-hoc test radi identifikacije značajnih razlika između definiranih skupina zemalja. Izrađena je i CAGR Analiza (analiza složene godišnje stope rasta) prema formuli:

$$CAGR = \left(\frac{Vkraj}{Vpočetak}\right)^{\frac{1}{n}} - 1 \qquad (1)$$

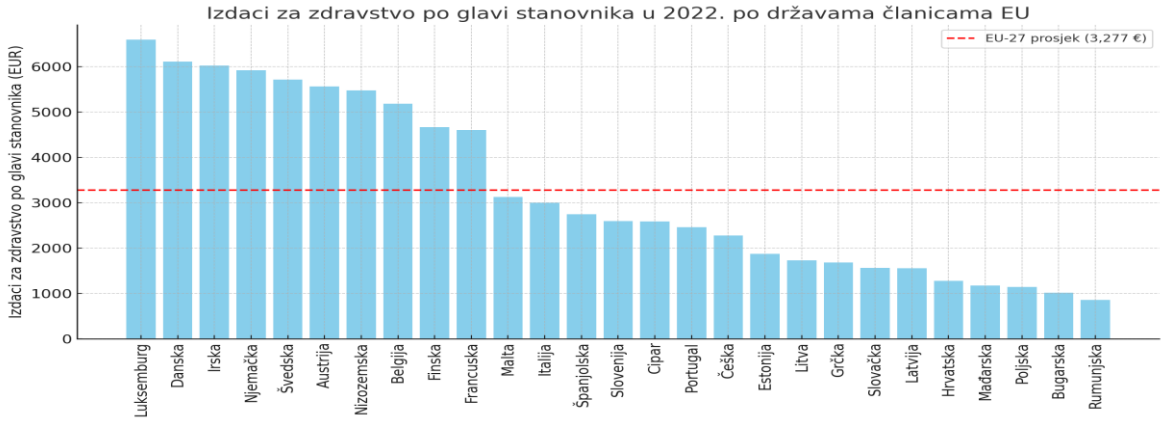
CAGR analizom izračunata je prosječna godišnja stopa rasta svih pokazatelja u Hrvatskoj u odnosu na prosjek Europske unije.

3. Rezultati

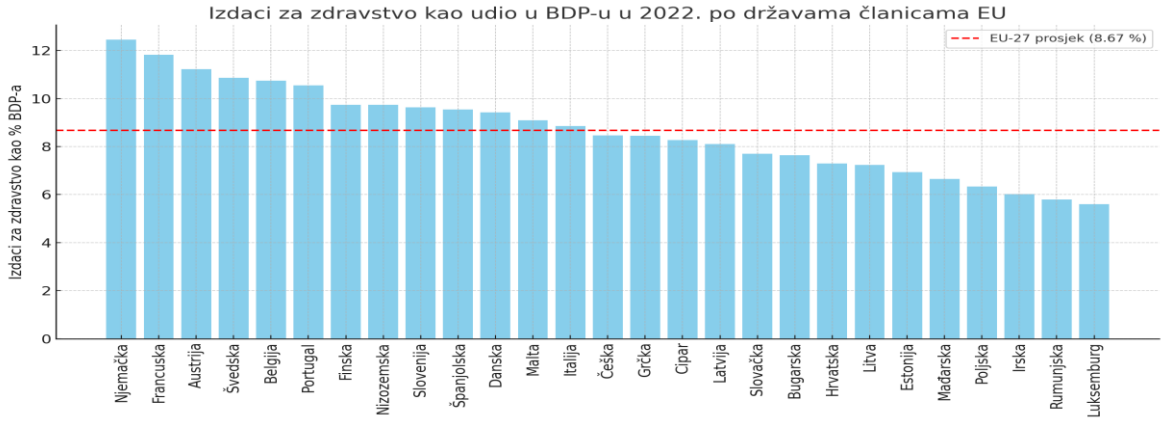
Kako je navedeno, temeljni indikatori korišteni u radu su ukupni izdaci u milijunima eura, izdaci po glavi stanovnika i izdaci kao % od BDP-a. Na slikama 1., 2. i 3. su prikazani podaci s ciljem prikaza položaja Hrvatske u odnosu na druge zemlje članice i u odnosu na prosjek Europske unije.



Slika 1. Ukupni izdaci za zdravstvo u mil. eura



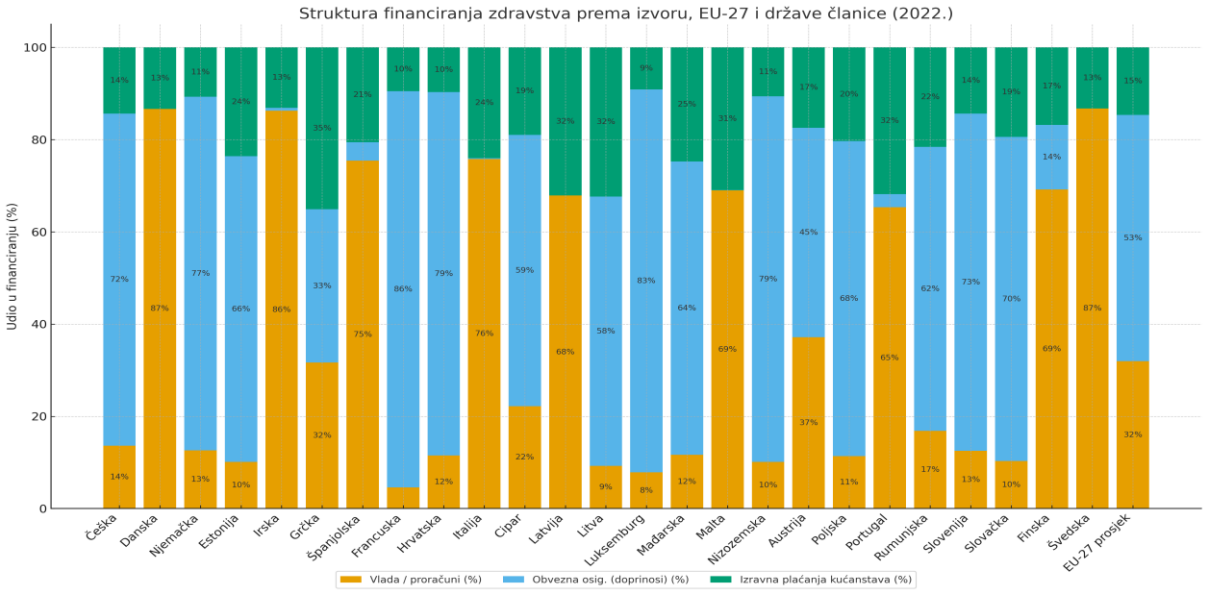
Slika 2. izdaci za zdravstvo po glavi stanovnika



Slika 3. izdaci za zdravstvo kao % od BDP-a

Hrvatska se prema sva tri indikatora nalazi ispod prosjeka Europske unije. Omjer financiranja zdravstva iskazuje se kao omjer javnog i privatnog

financiranja. Ovo je bitno napomenuti jer se rasprave u literaturi najčešće vode vezano za povećanje privatnog financiranja u odnosu na javno kako bi sustav bio učinkovitiji i održiviji. Iako se ovaj rad ne bavi striktno analizom raspodjele financiranja već samim problemom dostatnosti financiranja, kako bi se stekla cjelokupna slika o financijskom okviru za zdravstvo na Slici 4. prikazan je udio javnog i privatnog financiranja zdravstvenog sustava.



Slika 4. Udio javnog i privatnog financiranja zdravstva

Deskriptivnom analizom u tablici 1. obuhvaćeni su podaci o ukupnim zdravstvenim izdacima (u milijunima eura), izdaci po glavi stanovnika (u eurima) i izdaci kao % BDP-a u razdoblju od 2015. do 2022. godine za sve zemlje članice čime se daje uvid u strukturu svega što se u ovom radu promatra i uspoređuje. Deskriptivna analiza obuhvaća podatke o aritmetičkoj sredini, standardnoj devijaciji, minimumu, medijanu i maksimumu promatranih podataka.

Tablica 1. Deskriptivna statistika

Pokazatelji	Aritmetička sredina	St. dev.	Min	Medijan	Max
Ukupni izdaci za zdravstvo (u mil. EUR)	51.861,98	91.869,91	889,47	16.959,91	492.139
Izdaci po glavi stanovnika (EUR)	3.732,66	1.749,86	399,83	2.145,14	6.590,17
Izaci kao % BDP-a	8,51	1,91	4,94	8,52	12,72

Izvor: izračun autora

Komparativnom analizom obuhvaćena je 2022. godina, a analizom je utvrđeno da se Hrvatska prema svim pokazateljima nalazi ispod prosjeka Europske unije. Ukupni izdaci (mil. EUR): Hrvatska 4,93 mlrd., EU-27 prosjek 1,66 bilijuna → Hrvatska je ~99,7% ispod prosjeka.

Izdaci po glavi stanovnika (EUR): Hrvatska 1.279 EUR, EU-27 prosjek 3 706 EUR → Hrvatska je 65,5 % ispod prosjeka.

Izdaci (% BDP-a): Hrvatska 7,3%, EU-27 prosjek 10,26% → Hrvatska je 28,9% ispod prosjeka. U Tablici 2. prikazani su navedeni podaci komparativne analize.

Tablica 2. Komparativna analiza

Pokazatelji	Hrvatska (2022)	Prosjek EU (2022)	Apsolutna razlika	Relativna razlika
Ukupni izdaci za zdravstvo (u mil. EUR)	4.933,18	1.655.810,47	-1.650.877,29	-99,70
Izdaci po glavi stanovnika (EUR)	1.279,15	3.705,65	-2.426,5	-65,48
Izaci kao % BDP-a	7,3	10,26	-2,96	-28,85

Izvor: izračun autora

Analizom varijance (ANOVA) testirano je postoji li razlika u izdacima za zdravstvo prikazanim kao % od BDP-a. Podaci su prikazani u Tablici 3. Već samim pregledom rezultata jasno je vidljivo da razlike postoje, što je analiza i pokazala.

Tablica 3. ANOVA

Test	Vrijednost F	p-vrijednost
ANOVA	5,248316	0,012859

Izvor: izračun autora

Dobiveni rezultat F vrijednosti (F=5,25) govori da postoje razlike među skupinama koje su više od pet puta veće od razlika unutar skupine, dok p vrijednost (p=0,01) potvrđuje da su razlike u izdacima mjerenima kao % od BDP-a statistički značajne. ANOVA testom su zemlje podijeljene u tri skupine prema tercilima zdravstvene potrošnje (niska, srednja, visoka) pri čemu su dobiveni slijedeći primjeri skupina u odnosu na izdatke za zdravstvo kao % BDP-a:

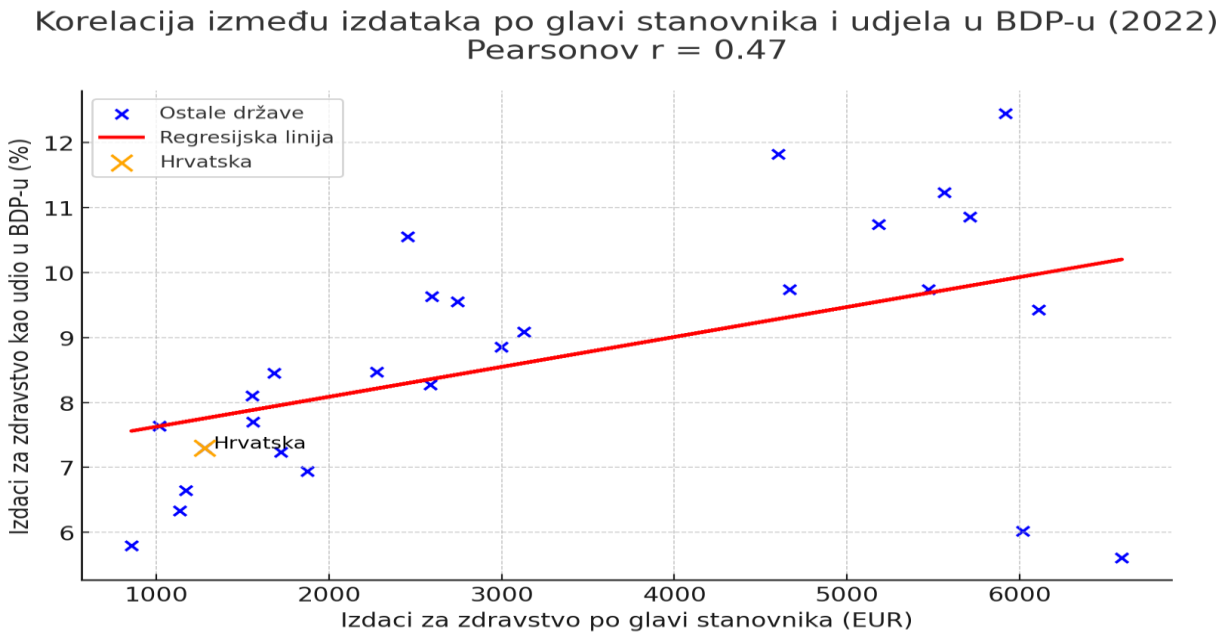
Niska: Rumunjska, Bugarska, Poljska, Hrvatska.
Srednja: Estonija, Portugal, Italija, Francuska.
Visoka: Njemačka, Austrija, Švedska, Danska, Luksemburg.
Provođenjem Tukey HSD post-hoc testa radi identifikacije značajnih razlika između definiranih skupina zemalja dobiveni su slijedeći rezultati:

Tablica 4. Tukey HSD post-hoc test

Skupina 1	Skupina 2	Razlika sredina	p-prilagođeno	Donja granica	Gornja granica	Odbacivanje H0
Visoka	Niska	-2,29	0,0173	-4,2106	-0,3694	DA
Visoka	Srednja	-0,2944	0,9226	-2,2151	1,6262	NE
Niska	Srednja	1,9956	0,0406	0,0749	3,9162	DA

Izvor: izračun autora

Visoka-Niska: razlika je značajna (p = 0.0173) → zemlje s visokom potrošnjom po glavi stanovnika izdvajaju znatno drugačiji % BDP-a od zemalja s niskom potrošnjom.
Niska-Srednja: razlika je značajna (p = 0.0406) → i ovdje postoji statistički značajna razlika u % BDP-a.
Visoka-Srednja: razlika nije značajna (p = 0.923) → ove dvije skupine su slične po izdacima % BDP-a.
Najveće razlike postoje između zemalja s niskom potrošnjom, dok su zemlje članice sa srednjom i visokom potrošnjom po glavi stanovnika slične u potrošnji kao % od BDP-a.
Korelacijskom analizom između izdataka po glavi stanovnika i izdataka za zdravstvo kao % BDP-a provedenom za sve zemlje Europske unije u 2022. godini dobiven je Pearsonov koeficijent korelacije r=0,47 što označava da postoji umjerena pozitivna povezanost, odnosno zemlje koje imaju veće izdatke po glavi stanovnika, u pravilu izdvajaju i veći udio BDP-a za zdravstvo.



Slika 5. CAGR analiza

Na grafikonu (Slika 5.) se vidi raspodjela zemalja sa regresijskom linijom. Hrvatska se nalazi u donjem lijevom dijelu, izdvajanje za zdravstvo po glavi stanovnika je nisko, kao i prema % od BDP-a.

Konačno, analiza složene godišnje stope rasta (CAGR) prikazana u Tablici 5. za razdoblje 2015-2022 za Hrvatsku i prosjek zemalja članica EU pokazuje slijedeće rezultate:

Ukupni izdaci (mil. EUR):
Hrvatska: +7,22% godišnje
EU-27: +4,51% godišnje
Izdaci po glavi stanovnika (EUR):
Hrvatska: +8,37% godišnje
EU-27: +4,40% godišnje
Izdaci kao % BDP-a:
Hrvatska: +1,32% godišnje
EU-27: +0,54% godišnje
Hrvatska pokazuje brži rast zdravstvene potrošnje od EU prosjeka, i u apsolutnim iznosima i po glavi stanovnika.

Tablica 5. CAGR

Indikator	Zemlja	2015	2022	CAGR (2015-2022)
Ukupni izdaci za zdravstvo (u mil. EUR)	Hrvatska	3.027,78	4.933,18	0,072225403
Ukupni izdaci za zdravstvo (u mil. EUR)	EU-27	1.215.654	1.655.810	0,045132939
Izdaci po glavi stanovnika (EUR)	Hrvatska	728,53	1.279,15	0,083739399
Izdaci po glavi stanovnika (EUR)	EU-27	2.741,36	3.705,65	0,043998226
Izdaci kao % BDP-a	Hrvatska	6,66	7,3	0,013194122
Izdaci kao % BDP-a	EU-27	9,88	10,26	0,005406036

Izvor: izračun autora

4. Rasprava

Rezultati istraživanja dobiveni jasnim pregledom podataka kao i statističkom obradom pokazuju da se Hrvatska nalazi ispod prosjeka Europske unije prema svim pokazateljima. Ovakav rezultat u skladu je sa drugim znanstvenim istraživanjima u kojima je istaknuto da zemlje srednje i istočne Europe (možemo reći novije zemlje članice EU) imaju veće probleme i slabije izvore financiranja zdravstva u odnosu na zapadne odnosno razvijenije zemlje članice EU (Rechel i sur., 2018). Hrvatska se u odnosu na druge zemlje članice jako oslanja na javne izvore financiranja (posebice iz obveznog zdravstvenog osiguranja) čime pridonosi građanima u kontekstu dostupne i univerzalne zdravstvene zaštite, odnosno ne oslanja se na izravna plaćanja građana (tzv. out-of-pocket plaćanja kojima građani samostalno financiraju zdravstvenu zaštitu), kao neke druge zemlje članice koje izravnim plaćanjima za zdravstvo ograničavaju pristup zdravstvene skrbi svim građanima na jednak način (Mladovsky i sur., 2012). Model javnog financiranja, s druge strane, ograničava fleksibilnost financiranja zdravstvenog sustava. Naime, otpornost i fleksibilnost zdravstvenog sustava ne mjeri se samo razinom potrošnje već i sposobnošću financijskog reagiranja na krizne situacije (Cylus i sur., 2020). Hrvatska bilježi brži rast zdravstvene potrošnje u odnosu na prosjek Europske unije što može ukazivati i na ubrzani rast, razvoj i ulaganje u zdravstvo. Ono što je bitno spomenuti jest činjenica da problem nije u visini ulaganja odnosno rasta potrošnje već i u samoj učinkovitosti raspodjele resursa odnosno smanjenja troškovno neučinkovitih zdravstvenih intervencija (Buljan i Šimović, 2022). Ograničenje istraživanja ogleda se u dostupnosti podataka na stranici Eurostat. Naime, neki podaci kasne, pa se moraju koristiti stariji podaci kako bi se dobila cjelokupna slika. Nadalje, podaci se analiziraju samo iz perspektive kvantitativnih financijskih podataka što svakako ne odražava kompletnu sliku i kvalitetu sustava zdravstvene zaštite pojedine zemlje na temelju učinkovitosti, dostupnosti i zdravstvenih ishoda. I posljednje, promatrano razdoblje obuhvaća i period pandemije COVID-19 kada su zdravstveni troškovi neplanirano skočili, što dodatno utječe na pojedine pokazatelje.

5. Zaključak

Provedena analiza jasno je pokazala da se Hrvatska, unatoč kontinuiranom rastu zdravstvene potrošnje u posljednjih nekoliko godina, i dalje nalazi ispod prosjeka Europske unije prema svim ključnim pokazateljima – ukupnim izdacima, izdacima po glavi stanovnika te izdacima kao udio u BDP-u.

Struktura financiranja hrvatskog zdravstvenog sustava, s velikim udjelom javnog financiranja, omogućuje visoku razinu dostupnosti zdravstvene zaštite, ali istodobno otvara pitanje fiskalne održivosti i otpornosti sustava na negativne utjecaje. Analize provedene u radu potvrdile su postojanje značajnih razlika među državama članicama te ukazale na specifičnu poziciju Hrvatske u skupini zemalja s nižim izdvajanjima.

Rezultati upućuju na potrebu za daljnjim reformama zdravstvenog financiranja u Hrvatskoj, koje bi trebale biti usmjerene na raspodjelu sustava financiranja između javnog i privatnog te smanjenje neučinkovitih rashoda poput ponovnih hospitalizacija, produženog boravka u bolnici, nepotrebnih dijagnostičkih postupaka, nepravilnog upravljanja kroničnim bolestima, niske stope preventivnih postupaka, loše koordinacije zdravstvene skrbi i drugih. Takav pristup potencijalno može osigurati ekonomsku racionalnost sustava i smanjenje postojećeg jaza u odnosu na prosjek Europske unije.

6. Literatura

Buljan, A. i Šimović, H. (2022). Učinkovitost hrvatskog zdravstvenog

sustava - usporedba sa zemljama Europske unije. Revija za socijalnu politiku, 29 (3), 321-354. https://doi.org/10.3935/rsp.v29i3.1933

Cylus, J., Figueras, J., & Thomson, S. (2020). Resilient and people-centred health systems: Progress, challenges and future directions in Europe. World Health Organization. https://apps.who.int/iris/handle/10665/332441European Commission (2019).

Joint report on health care and long-term care systems & fiscal sustainability: Country documents: 2019 update. https://doi.org/10.2765/861798

European Commission. (2021). State of Health in the EU: Croatia – Country Health Profile 2021. Publications Office of the European Union. https://health.ec.europa.eu/system/files/2021-12/2021_chp_hr_english.pdf

Eurostat: https://ec.europa.eu/eurostat/web/health/database?node_code=hlth_sha11)

Kaštelan Brumen, I., Rukavina, T. V., & Radin, D. (2022). Disparities in healthcare financing: A comparative analysis of Croatia and selected CEE countries. Financial Theory and Practice, 46(2), 145–168. https://doi.org/10.3326/fintp.46.2.2

Kovač, N. i Smolić, Š. (2021). PRIVATE HEALTH CARE SECTOR IN CROATIA: IS PRIVATE SPENDING ON HEALTH CARE MYTH OR REALITY?. Ekonomski pregled, 72 (4), 619-639. https://doi.org/10.32910/ep.72.4.6

Mladovsky, P., Allin, S., Masseria, C., Hernández-Quevedo, C., McDaid, D., & Mossialos, E. (2012). Health in the European Union: Trends and analysis. European Observatory on Health Systems and Policies. World Health Organization Regional Office for Europe. https://apps.who.int/iris/handle/10665/327971

Rechel, B., Jakubowski, E., McKee, M., & Nolte, E. (Eds.). (2018). Organization and financing of public health services in Europe. European Observatory on Health Systems and Policies.

Thomson, S., Cylus, J., Evetovits, T., & Figueras, J. (2022). How resilient is health financing policy in Europe? Evidence from the COVID-19 pandemic. The Lancet Regional Health – Europe, 14, 100294. https://doi.org/10.1016/j.lanepe.2021.100294

Voncina, L., Dzakula, A., & Mastilica, M. (2007). Health care funding reforms in Croatia: A case of mistaken priorities. Health Policy, 80(1), 144–157. https://doi.org/10.1016/j.healthpol.2006.02.009

World Health Organization (WHO) Regional Office for Europe. (2021). Croatia: Health system review. European Observatory on Health Systems and Policies. https://eurohealthobservatory.who.int/publications/i/croatia-health-system-review-2021

World Health Organization (WHO) Regional Office for Europe. (2021). Croatia: Health system review. European Observatory on Health Systems and Policies. https://eurohealthobservatory.who.int/publications/i/croatia-health-system-review-2021

COMPARATIVE ANALYSIS OF HEALTH CARE FINANCING IN CROATIA IN RELATION TO THE EU MEMBER STATES

Abstract: The aim of this paper is to examine the financing of the Croatian healthcare system in comparison with the European Union average. The main indicators selected for analysis are total healthcare expenditure, per capita expenditure, and expenditure expressed as a share of GDP. The analysis is based on Eurostat data for the 27 EU member states covering the period from 2015 to 2022, and applies descriptive statistical methods, comparative analysis, analysis of variance (ANOVA), the Tukey HSD post-hoc test, correlation analysis, and the compound annual growth rate (CAGR) analysis.
The findings indicate that Croatia falls below the EU average across all key indicators. Both total expenditure and per capita expenditure are considerably lower than the European average, as is the proportion of healthcare spending in GDP. The ANOVA results confirmed statistically significant differences between groups of countries, with Croatia classified among those with lower levels of healthcare expenditure. Although Croatia has recorded faster growth in healthcare spending than the EU average, it starts from a lower base, thereby maintaining the gap with more developed member states.
The results highlight the need for reforms aimed at improving the efficiency and sustainability of healthcare financing in Croatia.

Keywords: financing efficiency, health expenditure, health financing

Ovaj rad je licenciran pod Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International.

Zaprimljen: 9.6.2025.
Odobren za objavu: 23.7.2025.
Izvorni znanstveni rad

UMJETNA INTELIGENCIJA I KIBERNETIČKA SIGURNOST: STAVOVI ZAPOSLENIKA I IZAZOVI ZA SUVREMENA PODUZEĆA

Ivana Miklošević, Gabrijela Bosak, studentica
Sveučilište u Slavonskom Brodu, Trg I. B. Mažuranić 2, 35000 Slavonski Brod, Hrvatska
ePošta: imiklosevic@unisb.hr

Sažetak: Rad analizira percepcije zaposlenika u Republici Hrvatskoj o primjeni umjetne inteligencije i kibernetičke sigurnosti, s posebnim naglaskom na njihovu upoznatost s ovim tehnologijama te stavove o potencijalima i rizicima njihove primjene u suvremenom poslovanju. Cilj rada bio je identificirati razinu upoznatosti zaposlenika s tehnologijama umjetne inteligencije i kibernetičke sigurnosti te istražiti postoje li razlike u stavovima s obzirom na demografska obilježja, poput spola i stupnja obrazovanja. Empirijsko istraživanje provedeno je online anketom na uzorku od 111 zaposlenika različitih djelatnosti u Republici Hrvatskoj. Primjenom deskriptivne i inferencijalne statističke analize (t-test, ANOVA) istražena je povezanost demografskih obilježja ispitanika s percepcijom i upoznatosti ispitanika s umjetnom inteligencijom i kibernetičkom sigurnošću.

Rezultati pokazuju umjerenu razinu upoznatosti ispitanika s pojmovima umjetne inteligencije i kibernetičke sigurnosti te izraženu zabrinutost zbog potencijalnog gubitka radnih mjesta radi automatizacije poslovanja i mogućnosti kibernetičkih napada. Spol ispitanika nema značajan utjecaj na istraživane stavove, dok stupanj obrazovanja značajno utječe na upoznatost ispitanika s umjetnom inteligencijom. Rad doprinosi razumijevanju izazova implementacije umjetne inteligencije u poduzećima te pruža preporuke poput edukacije zaposlenika i razvoja organizacijskih strategija. Rezultati imaju praktične implikacije za strateško upravljanje ljudskim potencijalima u digitalnom okruženju.

Ključne riječi: edukacija zaposlenika, kibernetička sigurnost, percepcija zaposlenika, poduzeća, umjetna inteligencija

1. Uvod

Primjena umjetne inteligencije (AI) i kibernetičke sigurnosti u suvremenom poslovanju danas predstavlja ključne čimbenike tehnološke konkurentnosti i održivosti poduzeća. Naime, umjetna inteligencija se ne promatra više samo kao tehnološka inovacija, već i kao strateška prednost za konkurentnost suvremenih organizacija (Dwivedi i sur., 2021). U suvremenom poslovnom okruženju, organizacije se sve više oslanjaju na digitalne platforme i umjetnu inteligenciju kao pokretače inovacija. Kako ističu Lin i suradnici (2025), upravo strateško upravljanje podacima i razvoj analitičkih sposobnosti ključni su za jačanje organizacijske inovativnosti. Unatoč sve većoj rasprostranjenosti AI tehnologija, postoji određena razina nesigurnosti i nejasnoća u percepcijama zaposlenika o njezinim potencijalima, koristima i rizicima. U kontekstu ubrzane digitalne transformacije, rasprava se i dalje vodi o tome ima li umjetna inteligencija povoljne učinke na

gospodarski razvoj (Qin i sur., 2024). Paralelno s tehnološkim napretkom raste i važnost kibernetičke sigurnosti zbog povećanih rizika digitalizacije poslovanja. Upravo stoga, ovaj rad usmjeren je na istraživanje percepcija zaposlenika u Republici Hrvatskoj o umjetnoj inteligenciji i kibernetičkoj sigurnosti, s posebnim naglaskom na identificiranje potencijala, rizika te prepreka za njihovu učinkovitu integraciju. Kibernetička sigurnost suočava se s promjenjivim spektrom prijetnji i sve većom potražnjom za inovativnim tehnologijama (Kelley, 2022). Delso-Vicente i sur. (2025) ističu da su organizacijska kultura, osobna odgovornost zaposlenika i podrška menadžmenta ključni čimbenici usklađenosti s pravilima informacijske sigurnosti. Dodatno, u radu se istražuje utjecaj demografskih karakteristika poput spola i razine obrazovanja na stavove ispitanika o navedenim temama. Rezultati ovog istraživanja imaju potencijalno značajne implikacije za strateško planiranje obrazovnih politika te implementaciju AI tehnologija i mjera kibernetičke sigurnosti u hrvatskim poduzećima. Kako navode Aleca & Mihai (2025), strateška ulaganja u automatizaciju, digitalnu infrastrukturu i razvoj digitalnih vještina radne snage ključni su za jačanje gospodarske konkurentnosti.

2. Metodologija

U ovome radu korišten je kvantitativni istraživački pristup temeljen na anketnom ispitivanju stavova zaposlenika u Republici Hrvatskoj o primjeni umjetne inteligencije i kibernetičke sigurnosti u suvremenom poslovnom okruženju. Prikupljanje podataka provedeno je online anketnim upitnikom izrađenim pomoću platforme Google Forms. Anketni upitnik bio je strukturiran tako da omogućava prikupljanje relevantnih kvantitativnih podataka pogodnih za statističku analizu, čime se osigurava visoka razina znanstvene valjanosti i pouzdanosti rezultata istraživanja.

2.1. Ciljevi i svrha istraživanja

Glavni cilj ovog istraživanja je ispitati percepcije zaposlenika u Republici Hrvatskoj o primjeni umjetne inteligencije (AI) i kibernetičkoj sigurnosti u poslovanju. Specifični ciljevi su: definiranje ključnih stavova zaposlenika o primjeni AI tehnologija, analiza svijesti ispitanika o rizicima kibernetičke sigurnosti i ispitivanje postoje li razlike u stavovima ispitanika s obzirom na spol i obrazovanje ispitanika. Dobiveni rezultati provedenog istraživanja pružit će temelj za unaprjeđenje politika integracije umjetne inteligencije i upravljanja kibernetičkom sigurnošću. U skladu s navedenim ciljevima, postavljena su sljedeća istraživačka pitanja:

1. Postoje li statistički značajne razlike u stavovima i percepcijama zaposlenika o umjetnoj inteligenciji i kibernetičkoj sigurnosti s obzirom na spol?
2. Postoje li statistički značajne razlike u razini upoznatosti zaposlenika s kibernetičkom sigurnošću u odnosu na njihov stupanj obrazovanja?
3. Postoje li statistički značajne razlike u razini upoznatosti zaposlenika s umjetnom inteligencijom u odnosu na njihov stupanj obrazovanja?

2.2. Istraživački instrument i uzorak

Za prikupljanje podataka korišten je standardizirani strukturirani anketni upitnik koji je sadržavao ukupno 36 pitanja, a koji je bio podijeljen u tri glavna dijela: demografska pitanja,

stavovi zaposlenika o umjetnoj inteligenciji i stavovi zaposlenika o kibernetičkoj sigurnosti. Demografska pitanja uključivala su pitanja o dobi i spolu ispitanika, stupnju obrazovanja ispitanika te regiji stanovanja ispitanika. Pitanja o primjeni umjetne inteligencije odnosila su se na pitanja o razini poznavanja AI tehnologija, percepciji koristi i rizika te potencijalima za primjenu u poduzećima. Stavovi zaposlenika o kibernetičkoj sigurnosti obuhvaćali su pitanja koja istražuju percepciju zaposlenika o rizicima, prijetnjama, važnosti edukacije te preventivnim mjerama u vezi s primjenom kibernetičke sigurnosti. Anketni upitnik bio je dizajniran u obliku zatvorenih pitanja s višestrukim izborom te Likertovih ljestvica (1 – uopće se ne slažem, 5 – u potpunosti se slažem) kako bi se omogućila precizna kvantitativna analiza. Istraživanje je provedeno u ožujku i travnju 2025. godine, u skladu s opće prihvaćenim etičkim načelima znanstvenog istraživanja, što uključuje anonimnost i dobrovoljnost sudjelovanja svih ispitanika. Ciljana populacija bili su zaposlenici u poduzećima različitih djelatnosti u Republici Hrvatskoj. Konačni uzorak činio je 111 ispitanika. Ispunjavanju anketnog upitnika odazvalo se 82.9% žena i 17.1% muškaraca. Zbog opsežnosti upitnika, u ovom radu nisu prikazani svi odgovori ispitanika i rezultati, već su odabrani oni koji izravno doprinose analizi postavljenih istraživačkih pitanja.

2.3. Statistička obrada podataka

Nakon što su anketni upitnici prikupljeni i ispunjeni, podaci su izvezeni u program MS Excel te pripremljeni za daljnju statističku obradu u programskom paketu IBM SPSS Statistics 25.0. Provedena statistička obrada podataka uključivala je sljedeće metode: deskriptivna statistika (analiza frekvencija, srednjih vrijednosti i standardnih devijacija) i primjenjena je za prikazivanje osnovnih demografskih obilježja ispitanika, T-test za nezavisne uzorke primijenjen je kako bi se istražile razlike u stavovima ispitanika prema spolu. Jednosmjerna ANOVA analiza korištena je za utvrđivanje statistički značajnih razlika u percepcijama zaposlenika s obzirom na stupanj obrazovanja. Pri tome je proveden Tukey HSD post-hoc test za dodatnu analizu specifičnih razlika između pojedinih obrazovnih skupina i Bonferroni test radi detaljnijeg utvrđivanja specifičnih razlika među obrazovnim skupinama. Razina statističke značajnosti u svim analizama definirana je na razini $p < 0.05$, čime se osigurala pouzdanost donošenja zaključaka o postavljenim istraživačkim hipotezama.

2.4. Ograničenja istraživanja

Glavna ograničenja istraživanja vezana su uz veličinu i strukturu uzorka. Unatoč tome što uzorak omogućuje preliminarnu generalizaciju, preporučuje se da buduća istraživanja uključe veći broj ispitanika s ravnomjernijom strukturom po spolu.

3. Rezultati i rasprava

Analiza demografskih obilježja ispitanika prikazana u Tablici 1 obuhvaća četiri osnovne varijable: spol, dob, regiju prebivališta i stupanj obrazovanja ispitanika.

Tablica 1. Deskriptivna statistika za demografske varijable ispitanika

Varijabla	**Mod (n)**	**Srednja vrijednost**	**Standardna devijacija**	**Minimum**	**Maksimum**
Spol ispitanika	2 (ženski)	-	-	1	2
Dob ispitanika	-	37.53	13.16	18	65
Regija prebivališta	-	3.34	1.74	1	6
Stupanj obrazovanja	-	2.87	1.20	1	6

Izvor: autorica (vlastita obrada podataka)

U uzorku sudjeluje ukupno 111 ispitanika, bez nedostajućih vrijednosti, što osigurava potpunost obrade podataka. Prosječna dob ispitanika iznosi M = 37.53 godine, uz standardnu devijaciju SD = 13.16, što upućuje na značajnu heterogenost u dobi ispitanika. Raspon dobi od 18 do 65 godina pokriva široki spektar radno aktivnog stanovništva, čime se osigurava dobra reprezentativnost uzorka za teme vezane uz percepciju umjetne inteligencije i kibernetičke sigurnosti. Struktura ispitanika prema spolu pokazuje jasnu dominaciju žena (Mod = 2, ženski spol), što je u skladu s čestim trendovima većeg odaziva žena na anketna istraživanja. Varijabla regija prebivališta ima prosječnu vrijednost M = 3.34 (od šest mogućih kategorija hrvatskih regija) uz standardnu devijaciju SD = 1.74, što ukazuje na dobru teritorijalnu disperziju ispitanika diljem Hrvatske, uključujući i Grad Zagreb. S obzirom na stupanj obrazovanja, ispitanici u prosjeku imaju završen prijediplomski ili diplomski studij (M = 2.87, SD = 1.20), čime je potvrđena visoka obrazovna struktura sudionika, što može pozitivno utjecati na kvalitetu odgovora i sposobnost razumijevanja složenijih pitanja u anketi. Ovako strukturiran uzorak pruža pouzdanu osnovu za daljnje statističko testiranje hipoteza, te detaljnije analize stavova i percepcija ispitanika vezanih uz umjetnu inteligenciju i kibernetičku sigurnost u poslovnom okruženju. Zaposlenici trebaju prepoznati umjetnu inteligenciju kao priliku i usvojiti učinkovite mjere kako bi se lakše prilagodili tehnološkim promjenama (Xu i sur., 2023). Rezultati istraživanja pokazuju kako je većina ispitanika umjereno upoznata s pojmom umjetne inteligencije (45.9%), zatim slijede oni ispitanici koji su vrlo dobro upoznati (20.7%), slabo upoznati (16.2%), dobro upoznati (14.4%) te najmanji broj ispitanika koji uopće nisu upoznati (2.8%). Najveći potencijal primjene AI ispitanici vide u području marketinga i digitalne promocije (72.1%), zatim u razvoju proizvoda i inovacija (38.7%), upravljanju opskrbnim lancima i logistikom (21.6%), prodaji i odnosima s kupcima (20.7%), ljudskim resursima (18.0%) te financijama i upravljanju rizicima (17.1%). Prema mišljenju ispitanika, poduzeća bi trebala povećati ulaganja u istraživanje i razvoj umjetne inteligencije (55.0%), dok 29.7% ispitanika nije sigurno, a 15.3% ispitanika smatra da ulaganja ne bi trebalo povećavati. Neutralan stav o budućem utjecaju umjetne inteligencije na tržište rada ima većina ispitanika (41.4%), pozitivan utjecaj vidi 24.3%, negativan 13.5%, izrazito negativan 12.6%, a izrazito pozitivan svega 8.2%. Kao najveće rizike povezane s umjetnom inteligencijom ispitanici ističu gubitak radnih mjesta zbog automatizacije (80.2%), zlouporabu umjetne inteligencije (64.9%), privatnost i sigurnost podataka (45.0%) te etička pitanja i odgovornost za odluke AI (37.8%), dok samo 5.4% smatra da nema razloga za zabrinutost. Wang i Lu (2025) navode da zaposlenici sve

više doživljavaju umjetnu inteligenciju kao vrijednost u poslu, a ne prijetnju, osobito u sektorima usmjerenima na održivi razvoj i zelene tehnologije.

Najvećom prednošću umjetne inteligencije u poduzetništvu ispitanici smatraju poboljšanu analizu podataka (63.1%), poticanje inovacija (39.6%), povećanje operativne učinkovitosti (36.0%) te unaprjeđenje korisničkog iskustva (22.5%). U sljedeće dvije godine, 44.1% ispitanika smatra da će možda povećati korištenje umjetne inteligencije u poslovanju, 35.1% ispitanika neće povećati korištenje, a 20.8% planira povećati primjenu AI alata. Najveći broj ispitanika nije se susreo s izazovima implementacije AI u poslovanju (65.8%), dok kao najveće izazove ističu nedostatak kvalificiranog kadra (21.6%), nedovoljnu podršku unutar poduzeća (15.3%), regulativne prepreke (9.0%), visoke troškove (7.2%) te tehnološke barijere (6.3%). Prema Baslomu i Tongu (2019), menadžment na svim razinama trebao bi prepoznati pozitivnu ulogu klime učenja u razvoju svijesti zaposlenika o umjetnoj inteligenciji. Glede upoznatosti s pojmom kibernetičke sigurnosti, najveći dio ispitanika je djelomično upoznat (32.4%), slabo upoznat (25.2%), dobro upoznat (18.9%), uopće nije upoznat (17.1%) te vrlo dobro upoznat (6.4%). Kibernetičke prijetnje kao ozbiljan rizik uz odgovarajuće mjere zaštite vidi 41.4% ispitanika, nesigurno je 28.8%, a kao ozbiljan rizik kibernetičke prijetnje vidi 27.0% ispitanika, a 2.8% ispitanika smatra da prijetnje nisu značajne. S kibernetičkim napadom ili povredom podataka većina ispitanika nije se susrela (51.4%), dok 28.8% ispitanika poznaje nekoga tko je bio žrtva, 13.5% susrelo se jednom, a 6.3% više puta. Parsons i sur. (2017) navode kako je svijest o informacijskoj sigurnosti ključna za zaštitu organizacije od kibernetičkih prijetnji. Po pitanju ulaganja poduzeća u zaštitu podataka, najviše ispitanika smatra kako su ulaganja djelomična, ali postoji prostor za poboljšanje (45.9%), nesigurno je 27.9%, smatraju da je zaštita često zanemarena 20.7%, a dovoljno ulaganja navodi samo 5.5% ispitanika. Kao ključne mjere za unaprjeđenje kibernetičke sigurnosti ispitanici smatraju edukaciju zaposlenika (66.7%), jačanje internih protokola u poduzećima (52.3%), povećanje ulaganja u napredne sigurnosne tehnologije u poduzećima (43.2%), suradnju s vanjskim stručnjacima i razvoj sigurnosnih politika (30.6%), dok samo 0.9% ispitanika smatra da mjere nisu potrebne.

Nadalje, postavljene su dvije hipoteze, nulta i alternativna hipoteza.

H_0: Ne postoje statistički značajne razlike prema spolu ispitanika u stavovima o pitanjima vezanima uz umjetnu inteligenciju i kibernetičku sigurnost.

H_1: Postoje statistički značajne razlike prema spolu ispitanika u stavovima o pitanjima vezanima uz umjetnu inteligenciju i kibernetičku sigurnost.

Rezultati t-testa interpretirani su prema Leveneovom testu homogenosti varijanci, ovisno o njegovoj statističkoj značajnosti (Tablica 2).

Tablica 2. Rezultati t-testa za ispitivanje razlika prema spolu ispitanika u stavovima o umjetnoj inteligenciji i kibernetičkoj sigurnosti (N = 111)

Varijabla	**t**	**ss**	**p-vrijednost**	**Razlika sredina**	**Standardna pogreška**	**95% IP Donja granica**	**95% IP Gornja granica**
Upoznatost s kibernetičkom sigurnošću	1.47	109	0.14	0.47	0.32	-0.16	1.01
Percepcija rizika AI i kibernetičke sigurnosti	-0.16	109	0.87	-0.04	0.26	0.48	0.56
Iskustvo s kibernetičkim napadima	-0.48	109	0.66	-0.14	0.29	-0.70	0.43
Percepcija učinaka AI na operativne troškove	0.29	109	0.80	0.10	0.36	-0.61	0.80
Upoznatost s pojmom umjetne inteligencije	-0.44	109	0.66	-0.13	0.29	-0.70	0.44
Plan korištenja umjetne inteligencije u sljedeće 2 godine	0.18	109	0.86	0.04	0.21	-0.38	0.46
Poštivanje etičkih standarda u poduzećima u primjeni umjetne inteligencije	1.70	109	0.09	0.60	0.36	-0.10	1.31

Izvor: autorica (vlastita obrada podataka)

Rezultati t-testa (Tablica 2) pokazuju da ne postoje statistički značajne razlike prema spolu ispitanika u stavovima i percepcijama vezanim uz umjetnu inteligenciju i kibernetičku sigurnost (sve p-vrijednosti > 0.05). Svi intervali pouzdanosti uključuju nulu, dodatno potvrđujući odsutnost jasnih razlika među skupinama. Stoga se prihvaća nulta hipoteza (H_0), a odbacuje alternativna hipoteza (H_1). Ovi nalazi upućuju na zaključak da spol ispitanika nema značajan utjecaj na istraživane varijable.

U radu su također postavljene nulta hipoteza (H_0) i alternativna hipoteza (H_2):

H_0: Ne postoje statistički značajne razlike u upoznatosti s kibernetičkom sigurnošću među ispitanicima različitog stupnja obrazovanja.

H2: Postoji barem jedna statistički značajna razlika u upoznatosti s kibernetičkom sigurnošću među ispitanicima različitog stupnja obrazovanja.

Kako bi se utvrdilo postoje li statistički značajne razlike u razini upoznatosti ispitanika s kibernetičkom sigurnošću s obzirom na njihov stupanj obrazovanja, provedena je jednofaktorska ANOVA analiza (Tablica 3). Ispitanici su bili podijeljeni u šest skupina prema stupnju obrazovanja: osnovno

obrazovanje, srednja stručna sprema, prijediplomski studij, diplomski studij, poslijediplomski studij i doktorat.

Tablica 3. Rezultati jednofaktorske ANOVA analize razlika upoznatosti ispitanika s kibernetičkom sigurnošću prema stupnju obrazovanja (N = 111)

Izvor varijance	**Zbroj kvadrata**	**ss**	**Srednji kvadrat**	**F**	**p-vrijednost**
Između grupa	12.83	5	2.57	1.64	0.16
Unutar grupa	164.60	105	1.57		
Ukupno	177.42	110			

Izvor: autorica (vlastita obrada podataka)

Rezultati jednofaktorske ANOVA analize (Tablica 3) pokazuju da ne postoje statistički značajne razlike među ispitanicima različitih stupnjeva obrazovanja u upoznatosti s kibernetičkom sigurnošću ($F = 1.64$, $p = 0.16$). Budući da je dobivena p-vrijednost veća od standardne razine značajnosti od 0.05, prihvaća se nulta hipoteza (H_0), dok se alternativna hipoteza (H_2) odbacuje. Dobiveni rezultati pokazuju da ispitanici različitih stupnjeva obrazovanja imaju sličnu razinu upoznatosti s kibernetičkom sigurnošću, što znači da razina obrazovanja nema značajan utjecaj na ovu varijablu.

U radu je također postavljena nulta hipoteza (H_0) i alternativna hipoteza (H_3).

H_0: Ne postoje statistički značajne razlike u upoznatosti s umjetnom inteligencijom među ispitanicima različitog stupnja obrazovanja

H_3: Postoji barem jedna statistički značajna razlika u upoznatosti s umjetnom inteligencijom među ispitanicima različitog stupnja obrazovanja.

Za ispitivanje ovih hipoteza provedena je jednofaktorska ANOVA analiza, pri čemu su ispitanici razvrstani u šest skupina prema stupnju obrazovanja: osnovno obrazovanje, srednja stručna sprema, prijediplomski studij, diplomski studij, poslijediplomski studij i doktorat (Tablica 4).

Tablica 4: Rezultati jednofaktorske ANOVA analize razlika upoznatosti ispitanika s umjetnom inteligencijom prema stupnju obrazovanja (N = 111)

Izvor varijance	**Zbroj kvadrata**	**ss**	**Srednji kvadrat**	**F**	**p-vrijednost**
Između grupa	30.36	5	6.07	5.71	0.001***
Unutar grupa	111.60	105	1.06		
Ukupno	141.96	110			

Izvor: autorica (vlastita obrada podataka)

Rezultati jednofaktorske ANOVA analize (Tablica 4) ukazuju na postojanje statistički značajnih razlika u upoznatosti ispitanika s umjetnom inteligencijom među ispitanicima različitih stupnjeva obrazovanja ($F = 5.71$, $p < 0.001$). S obzirom na to da je dobivena p-vrijednost manja od standardne razine značajnosti od 0.05, nulta hipoteza (H_0) se odbacuje, a alternativna hipoteza (H_3) prihvaća. Dobiveni nalazi jasno pokazuju da stupanj obrazovanja značajno utječe na razinu upoznatosti ispitanika s umjetnom inteligencijom, sugerirajući da različiti obrazovni stupnjevi imaju različitu razinu informiranosti i percepcije vezane uz pojam i primjenu umjetne inteligencije. Post-hoc Tukey HSD analiza (Tablica 5)

dodatno potvrđuje rezultate ANOVA testa, pokazujući statistički značajne razlike u upoznatosti s pojmom umjetne inteligencije između ispitanika višeg obrazovnog stupnja (doktorat, poslijediplomski i diplomski studij) i ispitanika nižeg obrazovnog stupnja (srednja stručna sprema, osnovno obrazovanje).

Tablica 5: Rezultati post-hoc Tukey HSD analize razlika među skupinama ispitanika različitog stupnja obrazovanja u upoznatosti s umjetnom inteligencijom (N = 111)

Stupanj obrazovanja ispitanika	**N**	**Podskup 1**	**Podskup 2**
Doktorat	2	1.50	
Poslijediplomski studij	11	1.91	
Diplomski studij	21	2.05	
Prijediplomski studij	21	2.76	2.76
Srednja stručna sprema	49	3.00	3.00
Osnovno obrazovanje	7		3.71
p-vrijednost		0.077	0.511

Izvor: autorica (vlastita obrada podataka)

Najbolju upoznatost s umjetnom inteligencijom pokazuju ispitanici s doktoratom (1.50), dok je najslabija razina upoznatosti kod ispitanika s osnovnim obrazovanjem (3.71). Ispitanici sa srednjom stručnom spremom i završenim prijediplomskim studijem nalaze se u oba homogena podskupa, što znači da njihove prosječne vrijednosti nisu statistički značajno različite ni od viših ni od nižih obrazovnih skupina. Budući da je ANOVA analiza pokazala statistički značajne razlike ($F = 5.71$; $p < 0.001$), dodatno je provedena Bonferroni post-hoc analiza, koja je potvrdila statistički značajne razlike između sljedećih skupina: srednja stručna sprema i diplomski studij ($p = 0.009$), srednja stručna sprema i poslijediplomski studij ($p = 0.024$), te osnovno obrazovanje i poslijediplomski studij ($p = 0.007$). Rezultati jasno pokazuju da viši stupanj obrazovanja ima značajan utjecaj na veću upoznatost ispitanika s umjetnom inteligencijom, dok su ispitanici nižih obrazovnih stupnjeva manje upoznati s tim pojmom.

4. Zaključak

Provedeno istraživanje pokazalo je umjerenu razinu upoznatosti zaposlenika u Hrvatskoj s pojmovima umjetne inteligencije i kibernetičke sigurnosti, pri čemu najveći potencijal primjene umjetne inteligencije ispitanici vide u područjima marketinga, razvoja inovacija i unaprjeđenja operativne učinkovitosti. Kao najveći rizici povezani s umjetnom inteligencijom ističu se automatizacija radnih mjesta i moguća zlouporaba tehnologije, što ukazuje na važnost ciljane edukacije zaposlenika. U području kibernetičke sigurnosti ispitanici prepoznaju potrebu za preventivnim mjerama poput edukacije i jačanja sigurnosnih protokola, iako većina nije imala izravnih iskustava s kibernetičkim napadima. Rezultati t-testa pokazali su da spol ispitanika nema statistički značajan utjecaj na njihovu upoznatost s umjetnom inteligencijom i kibernetičkom sigurnošću. Jednofaktorskom ANOVA analizom utvrđeno je da obrazovni stupanj nema značajan utjecaj na upoznatost s kibernetičkom sigurnošću. Međutim, obrazovni

stupanj pokazao se značajnim čimbenikom za razinu upoznatosti s umjetnom inteligencijom, pri čemu ispitanici viših obrazovnih stupnjeva (doktorat, poslijediplomski i diplomski studij) pokazuju veću razinu upoznatosti u odnosu na ispitanike nižih obrazovnih stupnjeva (srednja stručna sprema, osnovno obrazovanje), što je dodatno potvrđeno post-hoc Tukey HSD analizom. Dobiveni rezultati sugeriraju nužnost provođenja edukacijskih aktivnosti usmjerenih na podizanje razine upoznatosti zaposlenika s umjetnom inteligencijom te povećanje svijesti o kibernetičkoj sigurnosti. Upravo zato, digitalna pismenost i informacijska sigurnost trebaju postati integralni dio svakog poduzeća koje teži održivoj konkurentnosti. Buduća istraživanja trebala bi koristiti veći i reprezentativniji uzorak kako bi dodatno istražila čimbenike koji utječu na upoznatost zaposlenika s umjetnom inteligencijom i kibernetičkom sigurnošću.

5. Literatura

Aleca, O. E., & Mihai, F. (2025). The Role of Digital Infrastructure and Skills in Enhancing Labor Productivity: Insights from Industry 4.0 in the European Union. Systems, 13(2), 113. https://doi.org/10.3390/systems13020113

Baslom, M.M.M., Tong, S. (2019). Strategic management of organizational knowledge and employee's awareness about artificial intelligence with mediating effect of learning climate. International Journal of Computational Intelligence Systems 12, 1585–1591. https://doi.org/10.2991/ijcis.d.191025.002

Delso-Vicente, AT., Diaz-Marcos, L., Aguado-Tevar, O. et al. (2025). Factors influencing employee compliance with information security policies: a systematic literature review of behavioral and technological aspects in cybersecurity. Futur Bus J 11, 28. https://doi.org/10.1186/s43093-025-00452-7

Dwivedi, Y. K., et al. (2021). Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. International Journal of Information Management, 57, 101994. https://doi.org/10.1016/j.ijinfomgt.2019.08.002

Kelley, S. (2022). Employee Perceptions of the Effective Adoption of AI Principles. J Bus Ethics 178, 871–893. https://doi.org/10.1007/s10551-022-05051-y

Lin, Y., Yousaf, Z., Grigorescu, A., & Popovici, N. (2025). Harnessing digital foundations and artificial intelligence synergies: Unraveling the role of digital platforms, artificial intelligence, and strategic adaptability in organizational innovativeness. Journal of Innovation & Knowledge, 10(2), 100670. https://doi.org/10.1016/j.jik.2025.100670

Parsons K, Calic D, Zwaans T, Pattinson M (2017). The human aspects of information security questionnaire (HAIS-Q): two further validation studies. Computers & Security, 66, 40–51. https://doi.org/10.1016/j.cose.2017.01.004

Qin, Y., Xu, Z., Wang, X. et al. (2024). Artificial Intelligence and Economic Development: An

Evolutionary Investigation and Systematic Review. J Knowl Econ 15, 1736–1770. https://doi.org/10.1007/s13132-023-01183-2

Wang, K.-H., & Lu, W.-C. (2025). AI-induced job impact: Complementary or substitution? Empirical insights and sustainable technology considerations. Sustainable Technology and Entrepreneurship, 4(1), 100085. https://doi.org/10.1016/j.stae.2024.100085

Xu, G., Xue, M., & Zhao, J. (2023). The Relationship of Artificial Intelligence Opportunity Perception and Employee Workplace Well-Being: A Moderated Mediation Model. International Journal of Environmental Research and Public Health, 20(3), 1974. https://doi.org/10.3390/ijerph20031974

ARTIFICIAL INTELLIGENCE AND CYBER SECURITY: EMPLOYEE PERCEPTIONS AND CHALLENGES FOR MODERN ENTERPRISES

Abstract: This paper examines employee perceptions regarding the application of artificial intelligence (AI) and cybersecurity in Croatia, with a particular focus on their familiarity with these technologies and their views on the opportunities and risks associated with their implementation in modern business operations. The aim of this research was to identify the level of employee awareness regarding artificial intelligence and cybersecurity, as well as to investigate whether demographic characteristics such as gender and education level affect these perceptions. Empirical research was conducted using an online survey on a sample of 111 employees from various sectors in Croatia. Through descriptive and inferential statistical analyses (t-test, ANOVA), the relationship between demographic characteristics of respondents and their perceptions and familiarity with AI and cybersecurity was explored. Results indicate a moderate level of awareness regarding artificial intelligence and cybersecurity concepts, alongside pronounced concerns about potential job losses due to automation and risks of cyber-attacks. Gender did not significantly influence employee perceptions, whereas educational level had a significant impact on respondents' familiarity with artificial intelligence. This study contributes to the understanding of challenges related to AI implementation in enterprises and offers recommendations such as employee education and the development of organizational strategies. Findings also hold practical implications for strategic human resource management in a digital environment.

Keywords: artificial intelligence, cybersecurity, employee education, employee perceptions, enterprises

Ovaj rad je licenciran pod Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International.

Zaprimljen: 27.4.2025.
Odobren za objavu: 13.10.2025.
Izvorni znanstveni rad

OZBILJNE IGRE O KIBERNETIČKOJ SIGURNOSTI U KURIKULUMU NASTAVE INFORMATIKE

Ivana Lovrić Senjak[1], Slavko Dukarić[2], Mihovil Gašić[1,2]
[1] Sveučilište u Slavonskom Brodu, Trg I. B. Mažuranić 2, 35000 Slavonski Brod, Hrvatska, ePošta: ilovricsenjak@unisb.hr, mgasic1@unisb.hr
[2] Ministarstvo obrane RH, Trg kralja Petra Krešimira IV br. 1, 10000 Zagreb, Hrvatska, ePošta: slavko.dukaric@morh.hr

Sažetak: Ovaj rad analizira mogućnosti implementacije ozbiljnih igara o kibernetičkoj sigurnosti u nastavi informatike te njihovu kurikularnu integraciju u osnovnoškolskim i gimnazijskim programima. Primijenjen je kvalitativni pristup i deskriptivna analiza osam web-baziranih igara, uz mapiranje njihovih sadržaja na ishode iz važećeg kurikuluma. Rezultati pokazuju da postoji određeni prostor za usklađenje sadržaja igara s predviđenim ishodima učenja, iako su uočena i ograničenja unutar kurikularne strukture. Ozbiljne igre prepoznate su kao potencijalno vrijedan alat za suvremeno planiranje i obogaćivanje nastave informatike.

Ključne riječi: digitalna sigurnost, gamifikacija, informatika, kurikulum, ozbiljne igre

1. Uvod

Sveprisutnost interneta i digitalnih tehnologija u svakodnevnom životu zahtijeva kompetencije koje omogućuju sigurno i odgovorno korištenje digitalnih alata. Integracija kibernetičke sigurnosti u obrazovni sustav povećava svijest o potencijalnim prijetnjama i osnažuje učenike da postanu proaktivni sudionici u zaštiti digitalnog okruženja (European Union Agency for Cybersecurity, 2023).

Jedan od inovativnih pristupa poučavanju kibernetičke sigurnosti jest korištenje ozbiljnih igara koje povećavaju angažman učenika i olakšavaju usvajanje složenih koncepata. Prema istraživanju koje je analiziralo ozbiljne igre namijenjene edukaciji o kibernetičkoj sigurnosti, gamificirani pristupi mogu poticati aktivno učenje i unaprijediti sposobnost donošenja odluka u realnim scenarijima (Jerman Blažič & Jerman Blažič 2022).

U Hrvatskoj, kurikulum informatike prepoznaje važnost kibernetičke sigurnosti (MZO, 2018) a digitalno okruženje i prisutnost računalnih prijetnji u svakodnevnom životu, zahtijevaju pedagoške pristupe koji su prilagođeni novim generacijama (Prensky, 2001).

Ovaj rad kombinira pregledni i empirijski pristup s ciljem analize ozbiljnih igara koje se bave temom kibernetičke sigurnosti te mapiranjem unutar osnovnoškolskog i gimnazijskog nastavnog plana i programa informatike. Analizom sadržaja igara nastojat će se utvrditi koje su igre tematski i didaktički najprikladnije s naglaskom na usklađenost s predviđenim ishodima učenja.

2. Metodologija

Ovaj pregledni rad koristi kvalitativni istraživački pristup temeljen na studiji slučaja, u kojem se analiziraju ozbiljne web-bazirane igre s temom kibernetičke sigurnosti u kontekstu njihove

primjenjivosti u nastavi informatike usklađene s propisanim ishodima. Korištena je metoda deskriptivne analize, pri čemu se svaka igra procjenjuje prema strukturiranim kriterijima koja omogućuje razumijevanje obrazovnog potencijala svake igre.

2.1. Analiza igara i mapiranje

Ukupno je analizirano osam web-baziranih igara koje obrađuju ključne koncepte iz područja kibernetičke sigurnosti, s naglaskom na njihovu obrazovnu primjenjivost u nastavi informatike. Odabir igara temeljen je na kriterijima besplatne dostupnosti bez financijskih ili tehničkih prepreka, te njihovom edukativnom potencijalu i tematskoj povezanosti s ishodima učenja. Svaka od igara procjenjena je pomoću unaprijed definirane tablice omogućujući strukturirano bilježenje relevantnih obilježja igara.

Nakon provedene analize, izvršeno je mapiranje obrazovnih ciljeva analiziranih igara na ishode učenja iz važećeg Kurikuluma nastavnog predmeta Informatika za osnovne škole i gimnazije (MZO, 2018; NN 22/2018). Mapiranje se temeljilo na usporedbi tematskog sadržaja igre s predviđenim ishodima učenja unutar svih domena kurikuluma.

2.2. Ograničenja

Glavna metodološka ograničenja odnose se na subjektivnost procjene i ograničen broj analiziranih igara. Iako je analiza provedena prema strukturiranom obrascu, percepcija prikladnosti može varirati ovisno o iskustvu nastavnika, tehničkoj opremljenosti škole te kognitivnim sposobnostima učenika.

3. Rezultati i rasprava

Analizirane igre obuhvaćaju širok raspon tema iz područja kibernetičke sigurnosti, od tehničkih aspekata poput konfiguracije vatrozida i analize mrežnih prijetnji, do socijalno-pedagoških komponenti kao što su prepoznavanje prijevara i digitalna etika. Igre se razlikuju i u stupnju kognitivne složenosti: naglašavaju prepoznavanje i donošenje osnovnih sigurnosnih odluka u svakodnevnim scenarijima i zahtijevaju analitičko razmišljanje, povezivanje podataka i višestupanjsko odlučivanje.

Tablica 1. Pregled web-baziranih ozbiljnih igara

Naziv igre	Tip igre	Trajanje	Opis teme igre i link
Permission Impossible	Narativna simulacija Vizualni blokovi	15–40 min	Pravila pristupa mreži, konfiguracija vatrozida, sigurnosne politike https://tulipslab.org
CS4G Netism	Tekstualno-grafička 2D simulacija	15–60 min	IP adrese, spoofing, smurf napadi, mrežni uređaji; Računalno razmišljanje https://netsim.erinn.io
Cybersecurity Lab	Tekstualno-grafička simulacija	60-90 min	Gradacija prijetnji, zaštite, sigurnosni rizici https://www.pbs.org
KC7 – Cyber Detective	Interaktivna simulacija	30–45 min	Forenzika, analiza prijetnji, obrana sustava https://kc7cyber.com
Interland	Arkada / Grafička / Edukativna avantura	40–45 min	Zaštita podataka, lozinke, prepoznavanje prijevara, digitalna etika https://beinternetawesome.withgoogle.com
Traveling Securely	Kviz Interaktivna simulacija	3–5 min	Sigurnost u javnim prostorima https://www.terranovasecurity.com
Cyber Awareness	Simulirani scenariji	20–30 min	Phishing, sigurnosne politike, zaštita podataka https://public.cyber.mil

Većina igara usmjerenih na tehničke aspekte izravno je primjenjiva u području Računalnog razmišljanja, dok su igre s naglaskom na ponašanje korisnika,

sigurnosne politike i prepoznavanje prijetnji prikladnije za područje Digitalne sigurnosti i Digitalnog građanstva.
Sve igre su prikladne za izvođenje unutar jednog školska sata, osim Cybersecurity Lab, čije trajanje od 60-90 minuta u kontinuitetu zahtijeva izričito blok sat implementaciju, ili integraciju u potencijalni projektni rad u okviru ispunjenja zadatka u obliku zadaće.

Tablica 2 prikazuje mapiranje pojedinih razina igre Interland na konkretne ishode učenja i vremenska razdoblja izvođenja nastave u razrednoj nastavi. Važno je napomenuti da oznake ishoda, prema pravilima kurikula informatike (NN 22/2018), sadržavaju broj razreda kao drugi znak unutar oznake (npr. D.1.2 odnosi se na prvi razred), što omogućava jasan uvid u očekivanu razinu postignuća učenika u određenom školskom razredu. Ta je metodologija dosljedno primijenjena, čime je osigurana transparentnost i preciznost u kurikularnom mapiranju.

Valja istaknuti da mapiranje pojedinih razina igre nije provedeno jednostavnom linearnom logikom (prvi razred – prvi nivo), već su nivoi igre pažljivo odabrani prema njihovoj tematskoj rezonanciji s ishodima i razvojnim karakteristikama učenika određenog razreda. Tako, primjerice, učenici prvog razreda ne igraju prvi nivo igre, nego drugi nivo (Kraljevstvo dobrote), budući da taj nivo tematski bolje odgovara ishodima prvog razreda i naglašava socijalno prihvatljivo i odgovorno ponašanje u digitalnom prostoru, što je ključna odgojno-obrazovna zadaća u toj razvojnoj fazi.

Tablica 2. Kurikularno mapirane igre – Osnovne Škole, razredna nastava

razred	ishod	mjesec nastave	igra	nivo
1.	D.1.2	studeni/prosinac	Interland	2 - Kraljevstvo dobrote
2.	D.2.4	siječanj/veljača	Interland	1 - Toranj s blagom
3.	D.3.2/1	rujan	Interland	3 - Rijeka Java
4.	D.4.2	rujan/listopad	Interland	4 - Dijeli pažljivo

Posebno je značajna činjenica da je igra Interland dostupna na hrvatskom jeziku, što omogućava izravnu i nesmetanu implementaciju u nastavi nižih razreda osnovne škole bez potrebe za dodatnim jezičnim posredovanjem. To je izuzetno važno u razrednoj nastavi gdje su jezične barijere još uvijek izražene, a izloženost učenika stranom jeziku može otežati razumijevanje sadržaja i smanjiti didaktičku učinkovitost aktivnosti.

Ovakav pristup ukazuje na potrebu za dubinskim razumijevanjem obrazovnih ciljeva i dizajna i sadržaja igre, što omogućuje efektivnu i smisleno integriranu uporabu digitalnih alata u ranom razdoblju školovanja. Time se ujedno podržava razvoj digitalnih kompetencija učenika na način koji je usklađen i utemeljen u njihovim kognitivnim, socijalnim i emocionalnim sposobnostima.

Tablica 3. Kurikularno mapirane igre – Osnovne Škole, predmetna nastava

razred	ishod	mjesec nastave	igra	nivo
5.	D.5.1	rujan/listopad	Traveling Securely	Kviz: javni prostori (5 situacija)
6.	A.6.2	siječanj/veljača	Permission Impossible	9 nivoa vježbi + 1 testni
7.	D.7.1	ožujak	Cybersecurity Lab	Svi nivoi + izazovi
8.	A.8.3	studeni/prosinac	CS4G Netism	5 nivoa u skupini: Basics

Tablica 3 prikazuje kurikularno mapiranje ozbiljnih igara za učenike od 5. do 8. razreda osnovne škole, gdje je vidljivo da se koriste igre na engleskom jeziku. Ova odluka temelji se na pedagoškoj pretpostavci da su učenici u ovoj obrazovnoj dobi već razvili temeljne kompetencije u stranom jeziku, čime jezična barijera više ne predstavlja ozbiljno ograničenje za razumijevanje i izvođenje zadataka unutar igara.

Za razliku od razredne nastave, gdje je bila korištena samo jedna igra (Interland) s ciljem stvaranja osjećaja poznatog i sigurnog okruženja na koje se mogu nadovezivati, u predmetnoj nastavi uvode se raznolikije igre. Ova strategija promjene didaktičkog pristupa u višim razredima ima snažno razvojno uporište: učenike se postupno uvodi u šire i kompleksnije digitalne svjetove kroz više različitih igara.
Promjena dinamike — od ponovljivosti i sigurnosti prema raznolikosti i istraživanju — odgovara kognitivnim i emocionalnim potrebama učenika viših razreda osnovne škole. Na taj način igre podržavaju ishode iz područja digitalne sigurnosti i računalnog razmišljanja, dok pridonose razvoju viših razina kritičkog mišljenja, sposobnosti povezivanja i razumijevanja apstraktnih koncepata.
Takvo postupno povećanje razine složenosti i raznolikosti digitalnih sadržaja je karakteristika daljnjeg mapiranja unutar kurikuluma srednjih škola, vođeno činjenicom o pridonošenju izgradnji samopouzdanja učenika u korištenju digitalnih alata, što je ključna kompetencija u suvremenom obrazovanju i informatički pismenom društvu.

Tablica 4. Opće, jezične, klasične i prirodoslovne gimnazije – 70 sati godišnje

razred	**ishod**	**mjesec nastave**	**igra**	**nivo**
1.	D.1.2	studeni	CS4G Netism	Nivo: 2 nivoa u skupini: Spoofs
2.	A.2.2	siječanj/veljača	CS4G Netism	Nivo: Man-in-the-middle u Skupini: Attacks

Tablica 5. Prirodoslovno-matematička gimnazija – 4 x 70 sati godišnje (inačica A)

razred	**ishod**	**mjesec nastave**	**igra**	**nivo**
1.	D.1.2	studeni	CS4G Netism	Nivo: 2 nivoa u skupini: Spoofs
2.	A.2.1	travanj/svibanj	CS4G Netism	Nivo: Traceroute u Skupini: Attacks
3.	B.3.6/5	svibanj/lipanj	CS4G Netism	Nivo: Man-in-the-middle u Skupini: Attacks

Tablica 6. Prirodoslovno-matematička gimnazija – 4 x 105 sati godišnje (inačica B)

razred	**ishod**	**mjesec nastave**	**igra**	**nivo**
1.	D.1.2	studeni	CS4G Netism	Nivo: 2 nivoa u Skupini: Spoofs
2.	A.2.1	travanj/svibanj	CS4G Netism	Nivo: Traceroute u Skupini: Attacks
2.	A.2.4	siječanj/veljača	CS4G Netism	Nivo: Man-in-the-middle u Skupini: Attacks
3.	B.3.2	siječanj-ožujak	KC7	odabrani nivoi
4.	B.4.4	siječanj-travanj	Cyber Awareness	odabrani nivoi

Tablice 4, 5 i 6 prikazuju kurikularno mapiranje ozbiljnih igara u različite gimnazijske programe. Vidljivo je da je najveći broj mapiranja usmjeren na igru CS4G Netism, čije su razine precizno povezane s ishodima.

U gimnazijskim programima zamjećuje se nedostatak dovoljno kurikularnih ishoda koji rezoniraju s razvojem vještina kibernetičke sigurnosti. Ishodi koji se odnose na tehničke aspekte i vještine informatičke pismenosti su prisutni, ali često nisu specifično usmjereni na sigurnosne kompetencije.

Očita je neusklađenost sadržaja u nekim gimnazijskim usmjerenjima: tehnički zahtjevni ishodi pojavljuju se čak i u općim i klasičnim gimnazijama, gdje priroda programa ne podrazumijeva snažno tehničko usmjerenje. Iako dublja rasprava o prikladnosti i opravdanosti takvih kurikularnih postavki prelazi okvire ovog rada, važno je istaknuti kako ista može otežati sustavnu implementaciju tema iz kibernetičke sigurnosti u formalno obrazovanje.

Dvije igre — KC7 i Cyber Awareness — zbog svoje širine tema i opsega sadržaja ostavljene nastavnicima na slobodan

izbor razina i dijelova igre koje će uključiti u nastavu. Iako ova fleksibilnost može biti korisna za iskusne nastavnike, ona smanjuje mogućnost standardizirane implementacije i povećava rizik da ključne teme ostanu neobrađene.

Ove igre pokrivaju značajne sadržaje u pogledu klasifikacije informacija i odgovornog rukovanja prema sigurnosnim smjernicama Ministarstva obrane SAD-a (DoD guidelines). S obzirom na važnost razumijevanja digitalne sigurnosti, njihova prisutnost u nastavnom procesu predstavlja vrijednu nadopunu obrazovanju.

4. Zaključak

Ovaj rad pokazao je da ozbiljne igre o kibernetičkoj sigurnosti mogu predstavljati vrijedan i učinkovit alat za integraciju sadržaja digitalne sigurnosti u nastavu informatike na svim razinama obrazovanja. Analiza je potvrdila širok raspon dostupnih igara koje tematski pokrivaju ključne aspekte kibernetičke sigurnosti i omogućuju razvijanje tehničkih, društvenih i kritičkih kompetencija učenika.

Mapiranje igara pokazalo je kako je moguće u značajnoj mjeri povezati obrazovne potencijale ozbiljnih igara s važećim ishodima učenja, osobito u području digitalne sigurnosti i računalnog razmišljanja. Ipak, analiza je ukazala i na strukturne izazove, poput ograničenog broja ishoda koji izravno podržavaju razvoj sigurnosnih kompetencija u gimnazijskom programu te na problem fleksibilne implementacije kod igara koje pokrivaju kompleksnije i šire teme.

Unatoč metodološkim ograničenjima, rezultati rada potvrđuju da pažljivo odabrane ozbiljne igre mogu doprinijeti suvremenijem izvođenju nastave informatike. Daljnja istraživanja i praktične implementacije trebale bi se usmjeriti na razvoj standardiziranih smjernica za integraciju ozbiljnih igara u nastavni proces te na prilagodbu kurikuluma u svrhu sustavnijeg uključivanja sadržaja iz područja kibernetičke sigurnosti. U tom kontekstu, važnu ulogu može imati CARNET (Hrvatska akademska i istraživačka mreža), kao ključna institucija koja razvija i provodi sigurnosne smjernice u školama, čime se otvara prostor za povezivanje postojećih inicijativa s novim oblicima digitalnog obrazovanja.

5. Literatura

European Union Agency Cybersecurity. (2023). Cybersecurity Education and Skills. https://www.enisa.europa.eu/topics/cybersecurity-education

Jerman Blažič, B., & Jerman Blažič, A. (2022). Cybersecurity Skills among European High-School Students Sustainability, 4763. https://doi.org/10.3390/su14084763

Ministarstvo znanosti i obrazovanja (MZO). (2018). Kurikulum nastavnog predmeta Informatika za osnovne škole i gimnazije. Narodne novine, broj 22/2018. https://narodne-novine.nn.hr/clanci/sluzbeni/2018_03_22_436.html

Prensky, M. (2001). Digital Natives, Digital Immigrants. On the Horizon, 9(5). https://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf

Erinn.io. (n.d.). CS4G Netism [Igra]. https://netsim.erinn.io/

Google. (n.d.). Interland – Be Internet Awesome [Igra]. https://beinternetawesome.withgoogle.com/hr_hr/interland/

KC7 Cyber. (n.d.). KC7 – Cyber Detective Game [Igra]. https://kc7cyber.com/

PBS. (n.d.). Cybersecurity Lab [Igra]. https://www.pbs.org/wgbh/nova/labs/lab/cyber/

Terranova Security. (n.d.). Traveling Securely [Igra]. https://www.terranovasecurity.com/products/security-awareness-platform/cyber-games/play

Tulip Lab. (2017). Permission Impossible [Igra]. https://tulipslab.org/projects/1617/PermissionImpossible/

U.S. Department of Defense. (n.d.). Cyber Awareness Challenge [Igra]. https://public.cyber.mil/training/cyber-awareness-challenge/

SERIOUS GAMES ON CYBERSECURITY IN THE COMPUTER SCIENCE CURRICULUM

Abstract: This paper analyzes the possibilities for implementing serious games on cybersecurity in computer science education and their curricular integration into primary and secondary school programs. A qualitative approach and descriptive analysis of eight web-based games were applied, mapping their content to the outcomes prescribed by the current curriculum. The results indicate that there is some potential for aligning the games' content with the expected learning outcomes, although certain limitations within the curricular structure were identified. Serious games are recognized as a potentially valuable tool for modern planning and enrichment of computer science education.

Keywords: cybersecurity, gamification, informatics, curriculum, serious games

Ovaj rad je licenciran pod Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International.

Zaprimljen: 16.6.2025.
Odobren za objavu: 13.10.2025.
Prethodno priopćenje

MARKETINŠKE STRATEGIJE I SIGURNOSNI IZAZOVI U FAZI LANSIRANJA DIGITALNOG BANKARSKOG PROIZVODA

Mirjana Kraljević[1], Andreja Katolik Kovačević[2]
[1] Sveučilište u Slavonskom Brodu, Trg I. B. Mažuranić 2, 35000 Slavonski Brod, Hrvatska, ePošta: mkraljevic@unisb.hr
[2] Sveučilište u Slavonskom Brodu, Trg I. B. Mažuranić 2, 35000 Slavonski Brod, Hrvatska, ePošta: akkovacevic@unisb.hr

Sažetak: Ovaj rad istražuje marketinške strategije u fazi uvođenja digitalnih bankarskih proizvoda, fokusirajući se na mobilnu aplikaciju Addiko banke za osobne financije. U kontekstu digitalizacije bankarskog sektora i promjene korisničkih navika, cilj rada je analizirati na koji način Addiko banka promovira svoju mobilnu aplikaciju, kako je pozicionira na tržištu te koliko su primijenjene strategije uspješne. Kroz teorijski okvir objašnjavaju se faze razvoja i uvođenja novog proizvoda, te se analizira primjena digitalnog marketinga, uključujući alate poput društvenih mreža, SEO-a i korisničkih recenzija. U empirijskom dijelu rada provodi se studija slučaja Addiko aplikacije i usporedba s konkurencijom. Rezultati ukazuju na ključne izazove i prednosti digitalnog marketinga u bankarstvu te pružaju preporuke za učinkovitiju implementaciju marketinških aktivnosti u digitalnom okruženju.

Ključne riječi: Addiko banka, digitalno bankarstvo, marketing strategije, mobilne aplikacije, sigurnost korisnika

1. Uvod

Bankarski sektor prolazi kroz značajne promjene, potaknute ubrzanim razvojem digitalnih tehnologija i promjenama u navikama korisnika. Digitalne banke i mobilne aplikacije za osobne financije postaju sve važniji dio financijskog ekosustava, a tržišna predviđanja pokazuju da će neto prihod od kamata digitalnih banaka rasti stabilnom stopom, dosežući gotovo 2,09 bilijuna dolara do 2029. godine (Bondarenko & Skorobogatova, 2015). U takvom kontekstu, sposobnost banke da razvije i učinkovito plasira digitalni proizvod postaje ključna za konkurentnost i dugoročno povjerenje korisnika.
Digitalni marketing u bankarskom sektoru više nije ograničen samo na oglašavanje, već podrazumijeva dublje razumijevanje potreba klijenata, stvaranje stvarne vrijednosti i izgradnju snažnijih odnosa.

Razvoj novih tehnologija neizbježno dovodi do transformacije svih poslovnih sektora i promjena u odnosima između komercijalnih banaka i njihovih postojećih i potencijalnih klijenata (Bondarenko & Skorobogatova, 2015). Dok se ranije digitalno bankarstvo povezivalo s tehničkim unapređenjima i automatizacijom operacija, danas ono obuhvaća ciljno i interaktivno kreiranje, promociju i pružanje proizvoda i usluga putem digitalnih tehnologija, s ciljem privlačenja i zadržavanja korisnika (Kovalev & Golovenchik 2018).

2. Metodologija

U istraživanju se koristi kombinacija kvalitativne i kvantitativne metode. Provodi se pregled relevantne literature i dosadašnjih istraživanja iz područja digitalnog bankarstva i marketinga. Zatim se analizira konkretan slučaj mobilne aplikacije Addiko banke kroz dostupne sekundarne podatke

(internetske kampanje, recenzije korisnika, izvještaji i promotivni materijali banke). Također se provodi komparativna analiza s mobilnim aplikacijama konkurentskih banaka (PBZ, Erste, ZABA, Raiffeisen) s ciljem prepoznavanja sličnosti i razlika u strategijama pozicioniranja i promocije. Uz to, koriste se dostupni statistički podaci Hrvatske narodne banke kako bi se poduprli trendovi rasta i korištenja mobilnog bankarstva. Rezultati se interpretiraju kroz prizmu ključnih elemenata marketinškog miksa: cijena, promocija, distribucija i korisničko iskustvo.

3. Teorijski okvir

Razvoj i lansiranje novog bankarskog proizvoda ključni su za opstanak i konkurentnost banke na tržištu. Budući da tržište postaje sve dinamičnije, tehnološki napredak i promjene u potrebama klijenata zahtijevaju kontinuirano inoviranje. Prema Kotleru (2008) novi proizvodi omogućuju banci proširenje asortimana, diferencijaciju od konkurencije te dugoročni rast i održivost poslovanja. Prvi korak u razvoju novog proizvoda je detaljna analiza tržišta radi prepoznavanja potreba, želja i problema ciljanih klijenata. Segmentacija tržišta omogućuje identifikaciju homogeni(h) skupina korisnika s različitim potrebama. Zbog velikih ulaganja, ali i rizika neuspjeha budući da više od 75% novih proizvoda ne uspije na tržištu banke često pažljivo tempiraju ulazak, a neke čekaju rezultate konkurencije prije vlastitog lansiranja (Hamilton, 2000). Upravo zbog kompleksnosti i visokih ulaganja, inoviranje postojećih proizvoda kratkoročno je isplativije, ali ne može biti temelj dugoročne strategije (Kotler & Keller, 2006). Banke se suočavaju s posebnim izazovima zbog specifičnosti usluga koje ne mogu biti fizički opipljive, a svaki proizvod ima svoju osobitost, što zahtijeva prilagodbu marketinške strategije i spleta (Franković, 2006 &. Vranešević, Vignali & Vrontis, 2004).

3.1. Marketing strategije

Analiza marketinga temelji se na ponašanju klijenata i njihovim očekivanjima. Klijenti formiraju svoja očekivanja iz različitih izvora, poput prošlih iskustava, preporuka ili oglasa. Ako se stvarna usluga ne podudara s obećanjima, može doći do nezadovoljstva. Klijenti danas imaju veću moć zbog pristupa informacijama putem Interneta, što uključuje recenzije, usporedbe i komentare drugih korisnika (Kandžija & Živko, 2004). Banke moraju učinkovito koristiti svoja sredstva i upravljati njima kroz sustavni pristup koji uključuje tri faze: planiranje, provođenje i vrednovanje rezultata (Hamilton, 2000). Banke pružaju različite financijske usluge koje su temelj za marketinške programe. Kvaliteta tih usluga ovisi o stručnosti zaposlenika, organizaciji i tehnologiji. Klijenti banaka su heterogeni, pa je važno segmentirati tržište i odabrati ciljne skupine.

4. Digitalno bankarstvo

Pojava novih tehnoloških distribucijskih kanala značajno mijenja način na koji banke distribuiraju svoje proizvode i usluge, te omogućava novim igračima da uđu na tržište. Tradicionalne granice između banaka i njihovih klijenata počinju se smanjivati, jer tehnologija omogućava bržu, jeftiniju i fleksibilniju interakciju s korisnicima. Klijenti sada mogu pristupiti svojim bankovnim uslugama bilo kada i bilo gdje putem interneta i mobilnih aplikacija (Gutić & Broz, 2011). Inovacije u distribuciji bankarskih usluga, poput internetskog bankarstva, mobilnog bankarstva (m-bankarstva) i automatiziranih bankomata, omogućuju veću efikasnost i smanjenje troškova poslovanja. Osim toga, elektronski prijenos sredstava i sustavi za elektroničko plaćanje na mjestu prodaje omogućuju brzu obradu transakcija u realnom vremenu, čime se smanjuju greške i ubrzava cijeli proces (Gutić & Broz, 2011). Jedan od ključnih faktora koji potiče ovu digitalnu

transformaciju je smanjenje troškova povezanih s tradicionalnim distribucijskim kanalima. Banke ulažu u nove tehnologije kako bi održale konkurentsku prednost na tržištu i zadovoljile rastuće zahtjeve svojih korisnika.

4.1. Mobilno bankarstvo

Mobilno bankarstvo predstavlja jedan od najznačajnijih oblika digitalnog bankarstva, omogućujući korisnicima pristup financijskim uslugama putem pametnih telefona i mobilnih aplikacija. Riječ je o disruptivnoj inovaciji koja mijenja način pružanja bankarskih usluga, smanjujući potrebu za fizičkim poslovnicama, papirologijom i brojem zaposlenih, dok istovremeno snižava operativne troškove banaka (Nicoletti, 2014). Banke koje uspješno implementiraju inovacije imaju konkurentske prednosti, jer mogu brže prilagoditi svoje usluge novim tržišnim uvjetima i potrebama korisnika (Veid, 2025.). Tri glavne ciljne skupine mobilnog bankarstva su prema Tiwari, Buse i Herstatt (2006) mladi od 14 – 18 godina koji iako još nisu korisnici, predstavljaju buduće klijente koji odrastaju uz tehnologiju. Zatim mladi od 18 – 26 godina – otvoreni za tehnologije, zapošljavaju se, počinju karijere te poslovni ljudi 26 – 50 godina – obrazovani, zaposleni, koriste mobilno bankarstvo za privatne i poslovne svrhe. Prema istraživanju Mihovilić, Hunjet i Vuković (2021). koje je provedeno u Hrvatskoj, od 174 ispitanika, 21 osoba ne koristi mobilno bankarstvo, a od tih 21, njih 14 (57,14%) ima više od 40 godina. Među onima koji koriste mobilno bankarstvo, 92 osobe (60,13%) mlađe su od 40 godina.

4.2. Sigurnosni rizici

Sigurnosni rizici predstavljaju jedan od ključnih izazova u razvoju i svakodnevnoj upotrebi internet bankarstva. Iako digitalne bankarske usluge nude brojne prednosti poput dostupnosti 24 sata dnevno, uštede vremena i smanjenja potrebe za fizičkim poslovnicama korisnici i banke suočeni su s nizom prijetnji u digitalnom okruženju (Hossain et al., 2025). Kako bi se zaštitili od ovih prijetnji, banke kontinuirano ulažu u sigurnosne tehnologije, kao što su:

- višefaktorska autentifikacija (MFA);
- enkripcija podataka;
- sustavi za otkrivanje prijevara temeljenih na umjetnoj inteligenciji;
- edukacija korisnika o digitalnoj sigurnosti.

Unatoč tim mjerama, potpuna eliminacija rizika nije moguća. Prema podacima Addiko banke (2025) zbog toga se sigurnost internet bankarstva temelji na zajedničkoj odgovornosti banke moraju osigurati tehnološku zaštitu i informirati korisnike, dok korisnici trebaju primjenjivati sigurne navike (npr. korištenje snažnih lozinki, izbjegavanje javnih Wi-Fi mreža, redovito ažuriranje uređaja).

5. Analiza studije slučaja

Addiko Banka predstavlja ključnu instituciju na hrvatskom financijskom tržištu, specijaliziranu za pružanje financijske podrške građanima te malim i srednjim poduzetnicima. S posebnim fokusom na gotovinske kredite, platni promet i financiranje malog i srednjeg gospodarstva, banka se ističe kao pouzdan partner u obavljanju svakodnevnih financijskih transakcija i podršci poslovanju poduzetnika. Addiko Banka posluje kroz mrežu od 35 poslovnica širom Hrvatske, za 260 000 klijenata, uz podršku virtualne poslovnice i mobilnih timova. Prema godišnjem izvješću (2023) Addiko banke u 2023. godini marketing je imao ključnu ulogu u poslovanju Addiko Banke, ne samo u sticanju novih klijenata, već i u jačanju brenda i povećanju prepoznatljivosti banke kao specijalizirane institucije za brze kredite. Kroz kreativnu upotrebu 3D animiranog lika Oskara, banka je uspješno komunicirala svoje poruke i ponude putem različitih medijskih kanala. Nova

kampanja pod sloganom „nemam vremena" bila je dinamična i inovativna, odražavajući brzinu i efikasnost koju Addiko nudi svojim klijentima. Osim toga, banka je kroz Program ubrzanja analizirala tržište i segmentaciju klijenata, što je omogućilo preciznije donošenje marketinških odluka temeljeno na konkretnim podacima. To je omogućilo bolju targetiranost ciljanih skupina klijenata, što je povećalo učinkovitost marketinških aktivnosti.

5.1. Mobilna aplikacija

Mobilna aplikacija Addiko Banke dizajnirana je s ciljem poboljšanja korisničkog iskustva, jednostavnosti i sigurnosti, te pruža funkcionalnosti koje omogućuju korisnicima učinkovito upravljanje financijama (Addiko Banka, 2023).
Aplikacija je dizajnirana tako da bude jednostavna za korištenje, s intuitivnim sučeljem i jasnim navigacijama. Korisnici mogu lako pristupiti svim funkcijama aplikacije, a procesi su optimizirani za mobilne uređaje. Brzi krediti, plaćanja i praćenje transakcija mogu se obaviti u nekoliko klikova, a aplikacija je optimizirana kako bi bila brza i efikasna u svim svojim funkcijama. Mobilna aplikacija Addiko Banke predstavlja ključnu komponentu njezinog poslovnog modela i digitalne strategije.

5.2. Usporedba mobilnih aplikacija za osobne financije Addiko Banka i konkurentske banke u Hrvatskoj

U sve dinamičnijem digitalnom okruženju, kvaliteta mobilnih aplikacija za osobne financije postaje ključna konkurentska prednost banaka. U nastavku se analizira kako se mobilna aplikacija Addiko Banke pozicionira u odnosu na aplikacije vodećih banaka u Hrvatskoj: Privredne banke Zagreb (PBZ), Zagrebačke banke (ZABA), Erste banke i Raiffeisenbank Austria (RBA). Analiza je rađena prema istraživanju Dragojević (2024).

1. Korisničko sučelje i jednostavnost korištenja

Mobilna aplikacija Addiko Banke ističe se jednostavnim i preglednim korisničkim sučeljem. Fokus je na brzoj dostupnosti osnovnih funkcionalnosti – provjeri stanja, plaćanjima i podnošenju zahtjeva za kredit. Usporedno, aplikacije PBZ-a i ZABA-e nude šire funkcionalnosti, ali ponekad po cijenu veće kompleksnosti, što može biti izazovno za tehnološki manje vješte korisnike.
Erste i RBA aplikacije pružaju moderan dizajn s naglaskom na personalizaciju i korisničko iskustvo, no Addiko se ističe specijalizacijom za gotovinske kredite koji se mogu ugovoriti u svega nekoliko koraka, bez potrebe za fizičkom prisutnošću.
2. Funkcionalnost
Addiko aplikacija u nekim aspektima zaostaje za konkurencijom u području automatiziranih savjetnika (npr. chatbot, upravljanje budžetom), no specijalizacija za kreditne proizvode i brzina procesa daje joj prednost kod korisnika kojima je važna funkcionalnost bez složenosti.

Tablica 1. Funkcionalnosti mobilnih aplikacija banaka u Hrvatskoj

Funkcionalnost	**Addiko**	**PBZ**	**ZABA**	**Erste**	**RBA**
Provjera računa i transakcija	✔	✔	✔	✔	✔
Plaćanje računa i QR plaćanja	✔	✔	✔	✔	✔
Ugovaranje kredita putem aplikacije	(brzi)	(ograničeno)	(ograničeno)	✔	✔
Mobilno plaćanje (Google/Apple Pay)	✔	✔	✔	✔	✔

Funkcionalnost	Addiko	PBZ	ZABA	Erste	RBA
Upozorenja/push notifikacije	✔	✔	✔	✔	✔
Digitalna asistencija (chatbot)	✔	✔	✔	✔	✔
Ulaganja/štednja kroz aplikaciju	✔	✔	✔	✔	✔
Personalizacija i upravljanje karticama	✔	✔	✔	✔	✔

3. Sigurnost
Sve analizirane aplikacije koriste višestruke sigurnosne slojeve: biometrijsku autentifikaciju (otisak prsta, prepoznavanje lica), PIN pristup, tokenizaciju i enkripciju podataka. Addiko dodatno komunicira sigurnosne preporuke kroz aplikaciju i web stranicu te edukativne materijale, čime gradi povjerenje kod korisnika.
4.Ciljana korisnička skupina
Dok Erste i PBZ nude širok spektar usluga i ciljaju sve segmente tržišta, Addiko se jasno profilira kao banka za jednostavne i brze financijske usluge – posebno gotovinske kredite. Ova strategija omogućuje joj da diferencira svoju aplikaciju kroz specijalizaciju i jednostavnost.

5.3. Anliza učinkovitosti marketinških strategija Addiko mobilne aplikacije

U analizi učinkovitosti marketinških aktivnosti Addiko banke vezanih uz promociju njihove mobilne aplikacije za osobne financije korišteni su javno dostupni podaci iz online trgovina aplikacijama, uzimajući u obzir broj preuzimanja, ocjene korisnika te najčešće komentare i pritužbe. Prema podacima iz Google Play trgovine, mobilna aplikacija Addiko Mobile Hrvatska ima više od 100.000 preuzimanja i prosječnu ocjenu 3,6 od 5 na temelju 7 000 recenzija. Korisnici u komentarima često ističu preglednost sučelja i jasan ispis stanja i transakcija kao pozitivne strane aplikacije. Međutim, veći broj recenzija s nižim ocjenama ukazuje na značajne tehničke poteškoće, poput učestalog zamrzavanja, padanja sustava, blokiranja aplikacije te njene nedostupnosti i po nekoliko dana u mjesecu.
Ovi podaci ukazuju na kontrast između dobro osmišljenog korisničkog sučelja i nedovoljno stabilnog tehničkog funkcioniranja. Unatoč marketingu koji naglašava brzinu i jednostavnost korištenja, iskustva korisnika pokazuju da stvarna upotrebljivost aplikacije nije uvijek pouzdana. To može negativno utjecati na povjerenje korisnika i dugoročno narušiti učinke marketinških kampanja.
S druge strane, aplikacija ima visoku ocjenu od 4,6 na Apple App Storeu, na temelju više od 5.000 recenzija, što ukazuje da je korisničko iskustvo stabilnije na iOS platformi. Ova razlika dodatno ističe potrebu za tehničkim unaprjeđenjem Android verzije aplikacije. U nastavku je prikazan pregled mobilnih aplikacij bamaka u RH prema podacima Google Playa.

Tablica 2. Pregled mobilnih aplikacija banaka u Hrvatskoj: Broj preuzimanja, ocjena i broj recenzija (Google Play)

Banka/Aplikacija	Broj preuzimanja	Prosječna ocjena	Broj recenzija
Addiko Mobile	100,000+	3,6	7,000+
RBA Mobile Banking	100,000+	4,7	40,000+
PBZ Mobile	500,000+	4,3	44,000+
ZABA m-zaba	500,000+	4,9	49,000+

Banka/Aplikacija	Broj preuzimanja	Prosječna ocjena	Broj recenzija
Erste mBanking	500,000+	3,5	8,000+

6. Zaključak

Studija slučaja pokazala je da Addiko banka ulaže u digitalne kanale i koristi zanimljive pristupe u oglašavanju, poput brendiranja s likom Oskara i kampanje "Nemam vremena", čime nastoji približiti usluge korisnicima na jednostavan i prepoznatljiv način. Njihova mobilna aplikacija ističe se prije svega jednostavnošću korištenja i fokusom na brze kredite, što odgovara onima koji traže praktičnost i brzinu bez odlaska u poslovnicu.
Iako postoje elementi gdje konkurencija nudi više funkcionalnosti, poput digitalnih savjetnika ili složenijih alata za upravljanje budžetom, Addiko se jasno pozicionira kao banka za korisnike kojima je važna brzina, sigurnost i jednostavnost. Usporedba s drugim bankama pokazuje da Addiko kroz aplikaciju pokriva sve osnovne potrebe korisnika, a dodatno se ističe komunikacijom sigurnosnih savjeta i edukacijom klijenata kako bi se smanjili rizici digitalnih prijevara.

7. Literatura

Addiko Bank. (2023). Addiko Bank d.d. Hrvatska – Godišnje izvješće za 2023. godinu. https://www.addiko.hr/static/uploads/Addiko-Bank_Godisnje-izvjesce_2023.pdf

Addiko.hr. (2025, travanj 2). Sigurnost na internetu. https://www.addiko.hr/sigurnost-na-internetu/

Addiko.hr. (2025, travanj 7). Upoznajte Addiko banku. https://www.addiko.hr/o-nama/

Bondarenko, T. N., & Skorobogatova, A. A. (2015). The role of marketing strategies in the organization of the commercial bank clients. International Journal of Applied and Fundamental Research, (3-3), 419–423.

Dragojević, F. (2024). Usporedba sustava mobilnog bankarstva u RH [Završni rad, Sveučilište Josip Juraj Strossmayer u Osijeku, Ekonomski fakultet].

Franković, I. (2006). Upravljanje odnosima s klijentima u bankama. Rijeka: Ekonomski fakultet u Rijeci.

Gutić, D., & Broz, D. (2011). Marketing u praksi. Osijek: Grafika d.o.o.

Hamilton, A. (2000). Upravljanje marketingom i prodajom. Zagreb: Potecon.

Hossain George, M. Z., Hasan, M. T., Alam, M. K., Munira, M. S. K., & Siddiqui, N. A. (2025). Assessing the influence of cybersecurity threats and risks on the adoption and growth of digital banking: A systematic literature review. arXiv. https://arxiv.org/

Kandžija, V., & Živko, I. (2004). Poslovna politika banaka. Rijeka: Ekonomski fakultet, Sveučilište u Rijeci.

Kovalev, M., & Golovenchik, G. (2018). Digital transformation of banks. Banking Bulletin, (11) (664), 50–60.

Kotler, P. (2008). Upravljanje marketingom (12. izd.). Zagreb: Mate d.o.o.

Nicoletti, B. (2014). Mobile banking (pp. 19–79). London: Palgrave Macmillan UK.

Šerić, N. (2009). Razvoj i dizajn proizvoda i upravljanje markom. Split: Sveučilište u Splitu, Ekonomski fakultet Split.

Tiwari, R., Buse, S., & Herstatt, C. (2006). Mobile banking as business

strategy. In 2006 Technology Management for the Global Future – PICMET 2006 Conference (Vol. 4, pp. 1935–1946).

Veid, J. (2025, travanj 8). The future of digital banking: How AI and cloud computing are shaping the transformation. https://www.linkedin.com/pulse/future-digital-banking-how-ai-cloud-computing-shaping-j%C3%B6rg-veidt-vlakc

Vranešević, T., Vignali, C., & Vrontis, D. (2004). Upravljanje strateškim marketingom. Zagreb: Accent.

MARKETING STRATEGIES AND SECURITY CHALLENGES IN THE LAUNCH PHASE OF A DIGITAL BANKING PRODUCT

Abstract This paper examines marketing strategies in the introduction phase of digital banking products, focusing on Addiko Bank's personal finance mobile application. In the context of the digitalization of the banking sector and changing consumer habits, the aim of the paper is to analyze how Addiko Bank promotes its mobile application, how it positions it in the market, and how successful the applied strategies are. The theoretical framework explains the phases of development and introduction of a new product, and analyses the application of digital marketing, including tools such as social media, SEO, and user reviews. In the empirical part of the paper, a case study of the Addiko app is conducted, along with a comparison with competitors. The results highlight key challenges and advantages of digital marketing in banking and provide recommendations for more effective implementation of marketing activities in a digital environment.

Keywords: Addiko Bank, digital banking, marketing strategies, mobile applications, user security.

Ovaj rad je licenciran pod Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International.

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

Ovaj rad je licenciran pod Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International.

Zaprimljen: 10.6.2025.
Odobren za objavu: 13.10.2025.
Pregledni rad

RAZVOJ PAMETNIH GRADOVA

Anita Kulaš Mirosavljević[1], Valentina Vuleta[1]
[1] Sveučilište u Slavonskom Brodu, Trg I. B. Mažuranić 2, 35000 Slavonski Brod, Hrvatska,
ePošta: akmirosavljevic@unisb.hr

Sažetak: U posljednjih nekoliko godina pametni gradovi postali su svjetski fenomen s različitim oblicima koji se pojavljuju u različitim dijelovima svijeta. Pametni grad se definira kao metropolitansko područje koje primjenom moderne tehnologije omogućuje veću kvalitetu života svojim stanovnicima. Njegov glavni cilj je poboljšati urbani život korištenjem informacijske tehnologije u pogledu prometa, sigurnosti, energije, otpada, pa čak i zdravstvenih usluga. Svrha rada je istražiti na koji način funkcioniraju pametni gradovi i kako dolaze do podataka. Cilj rada je istražiti koliko su građanima jasne dobrobiti pametnih gradova te prednosti digitalnih tehnologija. Ovo istraživanje temelji se na kvalitativnoj i deskriptivnoj metodologiji, s fokusom na analizu sekundarnih podataka. Pristup uključuje pregled relevantne znanstvene i stručne literature, strateških dokumenata Europske unije, nacionalnih razvojnih strategija te javno dostupnih izvješća vezanih uz razvoj pametnih gradova. Glavni izvori podataka uključuju dokumente politike EU-a, akademske članke, institucionalna izvješća i provjerene internetske platforme. Rezultati su pokazali kako je kombinacija digitalnih tehnologija s urbanom infrastrukturom povećala stupanj ovisnosti pametnih gradova o ogromnim količinama podataka prikupljenih od građana, senzora i drugih digitalnih sustava. Rad je omogućio predstavljanje svih izazova i perspektiva razvoja pametnih gradova opisujući izazove sigurnosti podataka i zaštita privatnosti, društvene izazove i digitalnu uključenost te buduće tehnologije u razvoju pametnih gradova.

Ključne riječi: pametni gradovi, razvoj, sigurnost

1. Uvod

Ovaj rad bavi se izazovima s kojima se susreću pametni gradovi. Pozornost se posvećuje tome kako gradovi asimiliraju informacijsku i komunikacijsku tehnologiju (IKT) u gradske sustave i usluge za poboljšanje života građana. Istraživanje ima za cilj proučiti koliko su građanima jasne dobrobiti pametnih gradova te prednosti digitalnih tehnologija. Štoviše, cilj nastoji procijeniti doprinose projekata pametnih gradova postizanju ciljeva kao što su uključivost u digitalne tehnologije i građansko sudjelovanje, uz obraćanje pozornosti na druge jednako važne čimbenike kao što su privatnost podataka i kibernetička sigurnost. Ovim istraživanjem autori žele proširiti znanje o procesima i koracima poduzetim prema razvoju pametnih gradova strateškim korištenjem tehnologija i inovacija kako bi se gradovima omogućilo rješavanje urbanih problema i povećanje društvenih, ekonomskih i ekoloških potreba stanovništva.

2. Metodologija

Ovo istraživanje temelji se na kvalitativnoj i deskriptivnoj metodologiji, s fokusom na analizu sekundarnih podataka. Pristup uključuje pregled relevantne znanstvene i stručne literature, strateških dokumenata Europske unije, nacionalnih razvojnih strategija te javno dostupnih izvješća vezanih uz razvoj pametnih gradova. Glavni izvori podataka uključuju

dokumente politike EU-a, akademske članke, institucionalna izvješća i provjerene internetske platforme.

3. Pojmovno određenje pametnih gradova

Počevši od sredine 20. stoljeća, diljem svijeta dogodile su se brojne društvene, ekonomske i ekološke krize koje su imale razoran utjecaj na razvojni napredak gradova. Međutim, u posljednja dva desetljeća, metropolitanske regije diljem svijeta poduzele su brojne projekte usmjerene na poboljšanje urbane infrastrukture i javnih sadržaja, što zauzvrat pokušava poboljšati socio-ekonomske uvjete i cjelokupno okruženje metropolitanskih područja (Lee i sur., 2014). Pametni gradovi razvijeni su s namjerom korištenja digitalne informacijske tehnologije u raznim aspektima postojanja, uključujući, ali ne ograničavajući se na zdravstvo, mobilnost, energetiku, obrazovanje, širenje znanja, pa čak i upravljanje građanskim resursima (Deakin & Al Waer, 2012).

Pojam „pametnog grada" funkcionira kao krovna fraza koja obuhvaća mnoštvo poddomena kao što su pametniji urbani razvoj, novo gospodarstvo, zeleniji i inteligentniji okoliš, visoke tehnologije, inteligentno upravljanje energijom, bolja mobilnost, poboljšana zdravstvena skrb, između ostalog (Galati, 2018). Caragliu i sur. (2009) konceptualiziraju pametni grad sa sljedećim glavnim karakteristikama:
(a) poboljšana administrativna i ekonomska učinkovitost koja omogućuje razvoj kulture i društva korištenjem umrežene infrastrukture;
(b) temeljni naglasak na poslovno orijentiranom urbanom razvoju;
(c) snažan fokus na cilju ostvarivanja socijalne uključenosti različitih vrsta urbanih stanovnika u javne usluge;
(d) naglasak na značajnoj ulozi visokotehnoloških i kreativnih industrija u dugoročnom rastu; (e) perspektiva da se velika pažnja posveti funkciji društvenog i relacijskog kapitala u razvoju grada, i;
(f) vizija da se društvena i ekološka održivost smatra važnim aspektom razvoja pametnog grada.

Marsal-Llacuna i sur. (2015) ističu važnost procjene pametnih gradova koja integrira lekcije iz već postojećih ekološki prihvatljivih i ugodnih urbanih područja te njihov fokus na održivost i kvalitetu života u kombinaciji s potrebnim tehnološkim komponentama. Osim toga, Lazaroiu i Roscia (2012) sugeriraju da bi pametni grad trebalo smatrati međusobno povezanom tehnološkom zajednicom koja je izdržljiva, udobna, privlačna i sigurna.

Općenito, pametni grad ima šest međusobno povezanih dimenzija, a to su gospodarstvo temeljeno na znanju, pametna mobilnost, ekološka održivost, ljudski i društveni kapital, kvaliteta života i participativno upravljanje (Lee i sur., 2014). Međutim, nijedan grad do danas nije ni blizu potpunom uključivanju svih šest dimenzija u jedan grad.

4. Tehnološki aspekt pametnog grada

Pametni grad ne samo da integrira informacijske i komunikacijske tehnologije (IKT), već ih i inovativno koristi za poboljšanje kvalitete života svojih građana, što daleko nadilazi jednostavno usvajanje tehnologija. Internet stvari (IoT) je primarna komponenta koja integrira urbane sustave poput semafora, ulične rasvjete i vodoopskrbe u jednu digitalnu mrežu. IoT analitika ne samo da pruža uvide već i praktične informacije usmjerene na to kako grad funkcionira; od prometnih obrazaca, potrošnje energije do sigurnosnih mjera.

Fizičke aspekte pametnih gradova temeljno poboljšava umjetna inteligencija (AI), koja pojednostavljuje predviđene tokove skupova podataka u potrazi za informacijama koje bi mogle

ukazivati na potencijalni problem, rizik ili prijetnju društvu. Decentralizirana priroda blockchain tehnologije povećava stupanj sigurnosti za pametne gradove. Svaka transakcija u vezi s distribucijom energije, odlaganjem otpada ili čak prijevozom postaje sigurna, provjerljiva i nepromjenjiva putem blockchaina. Cijela infrastruktura izgrađena je na računalstvu u oblaku čime se smanjuje ovisnost o lokalnim poslužiteljima, pružajući pristup s gotovo bilo kojeg mjesta. Ova jednostavnost pristupa omogućuje veću razmjenu podataka među dionicima i bolju integraciju iz različitih dijelova urbanih sustava.

5. Društveni izazovi

5.1. Sigurnost podataka i zaštita privatnosti

Kombinacija digitalnih tehnologija s urbanom infrastrukturom povećala je stupanj ovisnosti pametnih gradova o ogromnim količinama podataka prikupljenih od građana, senzora i drugih digitalnih sustava. Iako urbano upravljanje temeljeno na podacima omogućuje veću učinkovitost u pružanju usluga, održivost i transparentnost, upravljanje i zaštita privatnosti osobnih podataka predstavlja veliki izazov za gradske menadžere. Smanjenje tih rizika nužno je za izgradnju povjerenja javnosti i osiguravanje funkcioniranja sustava unutar pravnih i etičkih okvira. Obično platforme za pametne gradove primaju podatke iz različitih izvora koji često uključuju osjetljive informacije poput geolokacije, obrazaca korištenja energije, slika lica i zdravstvenih pokazatelja. Bez odgovarajućih zaštitnih mjera, tim će informacijama vjerojatno pristupiti ili neovlaštene osobe, ili će biti zlonamjerno nadzirane ili podvrgnute kibernetičkim napadima, što će ugroziti sigurnost i prava pojedinca (European Data Protection Supervisor, 2022). U Europskoj uniji, Opća uredba o zaštiti podataka (GDPR) temeljna je regulativa za svaku obradu osobnih podataka na području Europske unije. Prema GDPR-u, poznato je da su gradovi „kontrolori podataka" na temelju svoje odgovornosti za održavanje procesa prikupljanja podataka i kao takvi moraju primijeniti ograničavajuće mjere poput minimiziranja podataka, enkripcije i pseudonimizacije (European Commission, 2020, 2023). Osim toga, građani trebaju biti svjesni koji se podaci od njih prikupljaju, namjeravanoj svrsi takvog prikupljanja i postupcima koji su im dostupni za pristup, izmjenu ili brisanje svojih podataka. Također, načelo privatnosti po dizajnu i prema zadanim postavkama, koje je također postavljeno GDPR-om, navodi da bi tehnologije pametnih gradova trebale biti projektirane sa zaštitom podataka kao ključnom komponentom od samog početka. Takvo je načelo, međutim, teško ostvarivo u praksi, posebice kada u osmišljavanju i implementaciji pametnih rješenja sudjeluje niz javnih i privatnih dionika. Sofisticirane strukture upravljanja mogu zamagliti odgovornost za kontrolu podataka i, kao rezultat toga, mogućnost nepoštivanja propisa ili sigurnosnih propusta postaje vjerojatnija (European Data Protection Supervisor, 2022). Druga bitna komponenta je kibernetička sigurnost. Integracija urbanih sustava, koji često ovise o cloud sustavima i integracija podataka u stvarnom vremenu, povećava mogućnost izloženosti kibernetičkim prijetnjama kao što su hakiranje, napadi ransomwarea i prekidi usluga. Kibernetički napadi koji su na neko vrijeme paralizirali javne službe Atlante, Baltimorea i Barcelone i iz kojih su procurile vitalne informacije pokazuju što bi se moglo dogoditi u nedostatku odgovarajućih zaštitnih mjera (European Union Agency for Cybersecurity, 2023). Kao rješenje, Europska unija usvojila je NIS2 Direktivu (Direktiva o sigurnosti mrežnih i informacijskih sustava) koja postavlja strože obveze pružateljima osnovnih i digitalnih usluga, uključujući i gradske vlasti odgovorne za pametnu infrastrukturu. Pametni gradovi moraju usvojiti strategije upravljanja rizikom, obavljati periodične revizije sustava i prijaviti kršenja sigurnosti određenim tijelima (European Commission, 2022). No, izvješća ENISA-e 2022. pokazala su

da je, unatoč sve većoj svijesti o kibersigurnosnim rizicima, njezina primjena i dalje nasumična među državama članicama sa značajnim razlikama između regija velikih gradova i ostalih gradova (European Union Agency for Cybersecurity, 2022).

Osim toga, postoje etička pitanja u vezi s masovnim prikupljanjem podataka i potencijalnom špijunažom. Korištenje prepoznavanja lica, praćenja u stvarnom vremenu i praćenja ponašanja na javnim mjestima stvara dilemu između javne sigurnosti i prava pojedinca. Organizacije civilnog društva i tijela zadužena za zaštitu osobnih podataka izrazili su zabrinutost zbog neregulirane i nedemokratske uporabe takvih tehnologija (European Data Protection Board, 2021). Kako bi se borile protiv ovih problema, neki su pametni gradovi osmislili povelje o urbanim podacima i etičke okvire za usmjeravanje upotrebe pametnih tehnologija. Neki od njih su Amsterdam i Barcelona.

5.2. Društveni izazovi i digitalna uključenost

Stvaranje pametnih gradova ne samo da obećava automatizaciju, već postavlja i vrlo ozbiljne društvene izazove, posebno u pogledu digitalnog sudjelovanja, pristupačnosti i jednakosti. Implementacija pametnih usluga koje od korisnika zahtijevaju digitalnu povezanost i relativno poznavanje interneta stavlja mnoge društvene skupine u opasnost od daljnje marginalizacije. Bez proaktivnih inovativnih politika, neki ljudi mogu postati žrtve društvenog e-upravljanja, mobilnih aplikacija javnog prijevoza u stvarnom vremenu ili pametnih aplikacija za zdravstvenu skrb te postati društveno nenormalniji (European Commission, 2023). To je osobito slučaj u gradovima srednje i istočne Europe, uključujući niz hrvatskih gradova koji daleko zaostaju u pogledu digitalnih kompetencija i internetske pokrivenosti (Ministry of Regional Development and EU Funds, 2023). U isto vrijeme još jedan značajan faktor je dostupnost samih usluga. Kako bi se osigurala inkluzivnost, višejezične mogućnosti, korisničko testiranje i standardi dizajna trebali bi biti integrirani u platforme pametnih gradova od samog početka (European Commission, 2021). Kako bi premostila te nedostatke, Europska unija usredotočuje se na povećanje proračunskih izdvajanja za skladno uključivanje građana u prednosti koje dolaze s inovacijama kroz dizajn pametnih gradova. Inicijative poput Akcijskog plana za digitalno obrazovanje i Digitalnog kompasa EU-a naglašavaju potrebu za širim pružanjem javnog Wi-Fi-ja, gradske tehnologije prilagođene korisniku i obuke digitalnih vještina (European Commission, 2021). Štoviše, potiče se angažman građana u razvoju i evaluaciji usluga i tehnologija. Relevantnost usluge je poboljšana, ali povjerenje unutar zajednica i javne digitalne infrastrukture postiže se participativnim pristupima (European Commission, 2022).

5.3. Buduće tehnologije u razvoju pametnih gradova

Predviđa se da će integracija naprednih tehnologija u pametne gradove dramatično promijeniti način na koji gradovi funkcioniraju, a te tehnologije zasigurno će poboljšati dostupnost i pružanje javnih usluga. Pomoći će im u promjeni odnosa između građana i države, transformaciji upravljanja resursima i planiranju održivog razvoja. Gradovi će se morati uhvatiti ukoštac s novim mogućnostima i preprekama koje nude te tehnologije. Svaki od njih ima neviđene prilike za pozitivan napredak. Međutim, oni također nude nepredviđene rizike i probleme koje treba procijeniti i riješiti. Jedan od najznačajnijih razvoja je integracija umjetne inteligencije i strojnog učenja u urbane operacije. Primjer bi bili sustavi za kontrolu prometa koji koriste kamere pokretane umjetnom inteligencijom koje prate i analiziraju obrasce zagušenja kako bi odlučili kada automatski produžiti ili skratiti vrijeme signala za zaustavljanje na minimalne moguće granice kako bi se

smanjila kašnjenja i emisije. Isto se može dogoditi s komunalnim mrežama u kojima algoritmi umjetne inteligencije mogu otkriti abnormalne uzorke unutar njih, a kvarovi infrastrukture se obično predviđaju prije nego što se pojave, što omogućuje proaktivno održavanje (World Economic Forum, 2023).

Tehnologija digitalnih blizanaca još je jedan alat koji brzo napreduje i omogućuje gradovima stvaranje virtualnih replika fizičkih urbanih sustava u stvarnom vremenu. Politike dinamičkog urbanog razvoja mogu se analizirati korištenjem simulacija scenarija koje pomažu planerima u procjeni politike i analizi infrastrukture. Kako bi ublažili utjecaj poplava, Singapur i Rotterdam eksperimentiraju s digitalnim gradovima blizancima za optimizaciju energije, prijevoza i potrošnje. Europska komisija je razvila inicijativu Destination Earth (DestinE), koja nastoji stvoriti vrlo precizne digitalne prikaze Zemlje za promicanje poboljšanih ekoloških i urbanih politika (European Commission, 2023).

Hiperpovezani urbani ekosustavi imat će 5G tehnologiju kao svoju jezgru, a njezina niska latencija s velikom propusnošću omogućit će integraciju automobila s autonomnom vožnjom, prikupljanje podataka o okolišu u stvarnom vremenu, usluge zdravstvene skrbi na daljinu i usluge pametnog hitnog odgovora. Napredak u 6G već je u tijeku s još većom predviđenom latencijom i ugradnjom AI sustava koji omogućuju holografsku komunikaciju i precizno praćenje lokacije (European Telecommunications Standards Institute, 2024).

Blockchain tehnologija označava još jedno područje za inovacije jer pruža pouzdane metode za pohranjene i transakcijske podatke zbog svoje decentralizirane prirode. Neke lokalne vlasti već testiraju pilot projekte blockchaina za praćenje otpada i trgovanje energijom u zajednici (OECD, 2022). Kombinacija pametnih mreža i decentraliziranih izvora obnovljive energije pomoći će gradovima da učinkovitije upravljaju svojom potražnjom i opskrbom energijom. Inovativno skladištenje energije, uključujući napredne baterije i vodik, vjerojatno će poboljšati stabilnost mreže, čime će gradovi postati otporniji na klimatske promjene (World Economic Forum, 2023).

6. Zaključak

Napredak pametnih gradova leži u novom sjecištu digitalnih inovacija, brige za okoliš i društvenih promjena. Služi kao osjetljiva aktivna mjera za složene izazove urbanog života (brzi porast stanovništva, klimatske promjene, tehnološki napredak, povećana građanska potražnja za transparentnošću, učinkovitošću i aktivnim angažmanom u upravljanju). Integracija novih tehnologija glavna je komponenta za razvoj pametnog grada. Građanski angažman ima važnu ulogu u modelima pametnih gradova. Stoga su sudjelovanje, povratne informacije i povjerenje imperativni čimbenici. Bez odgovarajuće razine građanskog rada, čak i najnapredniji alati koji su nam na raspolaganju osuđeni su na neučinkovitost.

Iz današnje perspektive, pametni gradovi morat će prevladati niz problema kako bi ostali održivi i u budućnosti. Neka od tih pitanja su upotreba etike umjetne inteligencije, zaštita osobnih i digitalnih informacija, izazovi kibernetičke sigurnosti i digitalni jaz. Umrežavanje urbanih sustava dovodi do veće mogućnosti pojave kibernetičkih prijetnji koje mogu paralizirati javne službe. Stoga se ove nove tehnologije moraju pažljivo implementirati uz odgovarajuće upravljanje, zakone i odredbe socijalne pravde. Postavlja se pitanje kako te tehnologije povećavaju dobrobit, mogućnosti i kolektivni napredak građana.

7. Literatura

Caragliu, A., Del Bo, C., & Nijkamp, P. (2009). Smart cities in Europe. In Proceedings of the 3rd Central European Conference in Regional Science, Košice, Slovak Republic, October 7-9.

Deakin, M., & Al Waer, H. (Eds.). (2012). From intelligent to smart cities. New York: Routledge

ENISA (2022). State of Cybersecurity in the EU Public Sector, https://www.enisa.europa.eu/publications/state-of-cybersecurity-in-public-sector

European Commission (2020). European Data Strategy: Shaping Europe's digital future, https://digital-strategy.ec.europa.eu/en/policies/data-strategy

European Commission (2021). Digital Education Action Plan 2021–2027., https://education.ec.europa.eu/focus-topics/digital

European Commission (2022). 100 Climate-Neutral and Smart Cities by 2030., Horizon Europe Missions, https://mission-cities.eu

European Commission (2022). NIS2 Directive – Cybersecurity in the EU, https://digital-strategy.ec.europa.eu/en/policies/nis-directive

European Commission (2023). Data protection in the EU, https://ec.europa.eu/info/law/law-topic/data-protection_en

European Commission (2023). Digital inclusion and skills gap in Europe, https://digital-strategy.ec.europa.eu

European Commission (2023). Destination Earth (DestinE) Initiative, https://digital-strategy.ec.europa.eu/en/policies/destination-earth

European Data Protection Board (2021). Guidelines on facial recognition and surveillance in public spaces, https://edpb.europa.eu

European Data Protection Supervisor (2022). Smart Cities and Data Protection, https://edps.europa.eu

European Telecommunications Standards Institute (ETSI) (2024). 6G Research Outlook, https://www.etsi.org

European Union Agency for Cybersecurity (ENISA) (2023). Threat Landscape for Smart Cities, https://www.enisa.europa.eu

Galati SR (2018) Funding a smart city: from concept toactuality. In: Smart cities. Springer, Cham, pp 17–39

Lazaroiu, G. C., & Roscia, M. (2012). Definition methodology for the smart cities model. Energy, 47(1), 326–332

Lee, J. H., Hancock, M. G., & Hu, M. C. (2014). Towards an effective framework for building smart cities: Lessons fromSeoul and San Francisco. Technological Forecasting and Social Change, 89,80–99.

Marsal-Llacuna, M. L., Colomer-Llinàs, J., & Meléndez-Frigola, J. (2015). Lessons in urban monitoring taken fromsustainable and livable cities to better address the smart cities initiative. Technological Forecasting and SocialChange, 90, 611–622.

Ministry of Regional Development and EU Funds (2023). Smart Cities in Croatia – Overview and Strategic Orientation, https://razvoj.gov.hr

OECD (2022). Blockchain Technologies and Smart Cities, https://www.oecd.org

World Economic Forum (2023). Top 10 Emerging Technologies in Smart Cities, https://www.weforum.org

DEVELOPMENT OF SMART CITIES

Abstract: In recent years, smart cities have become a global phenomenon with different forms appearing in different parts of the world. A smart city is defined as a metropolitan area that, through the application of modern technology, enables a higher quality of life for its inhabitants. Its main goal is to improve urban life by using information technology in terms of traffic, security, energy, waste and even health services. The purpose of the paper is to investigate how smart cities work and how they get data. The aim of the paper is to investigate how citizens understand the benefits of smart cities and the advantages of digital technologies.

This research is based on a qualitative and descriptive methodology, with a focus on secondary data analysis. The approach includes a review of relevant scientific and professional literature, strategic documents of the European Union, national development strategies and publicly available reports related to the development of smart cities. The main sources of data include EU policy documents, academic articles, institutional reports and verified online platforms. The results showed that the combination of digital technologies with urban infrastructure has increased the degree of dependence of smart cities on huge amounts of data collected from citizens, sensors and other digital systems. The work enabled the presentation of all the challenges and perspectives of smart city development, describing the challenges of data security and privacy protection, social challenges and digital inclusion, and future technologies in the development of smart cities.

Keywords: development, security, smart cities

Ovaj rad je licenciran pod Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International.

Zaprimljen: 15.6.2025.
Odobren za objavu: 13.10.2025.
Pregledni rad

ULOGA KIBERNETIČKE SIGURNOSTI U JAČANJU REGIONALNE GOSPODARSKE OTPORNOSTI: INSTITUCIONALNE I GEOPOLITIČKE PERSPEKTIVE

Sanela Ravlić[1], Ivana Unukić[2]
[1] Sveučilište u Slavonskom Brodu, Trg I. B. Mažuranić 2, 35000 Slavonski Brod, Hrvatska, ePošta: sravlic@unisb.hr
[2]Sveučilište J. J. Strossmayera u Osijeku, Ekonomski fakultet u Osijeku, Trg Lj. Gaja 7, 31000 Osijek, Hrvatska, ePošta: ivana.unukic@efos.hr

Sažetak: Ovaj rad istražuje ulogu sigurnosti i kibernetičke sigurnosti unutar šire analize regionalne ekonomije jugoistočne Europe, s fokusom na geopolitičke i društvene izazove koji oblikuju gospodarske procese u Hrvatskoj i susjednim zemljama. U digitaliziranom gospodarstvu, sigurnosna infrastruktura – uključujući zaštitu informacijskih sustava, podataka i komunikacijskih kanala – postaje ključan preduvjet za održivi regionalni razvoj, gospodarsku stabilnost i prekograničnu suradnju.
Kibernetička sigurnost razmatra se ne samo kao tehnički zahtjev, već i kao element koji je duboko povezan s institucionalnim kapacitetima sigurnosnih protokola i razinom međusobnog povjerenja među državama regije. Jezične barijere dodatno otežavaju usklađivanje sigurnosnih mjera i krizne komunikacije, čime se povećava rizik od digitalne fragmentacije prostora koji teži integraciji.
U radu se analizira kako različite razine kibernetičke otpornosti i sigurnosne politike među državama utječu na investicijsku atraktivnost, inovacijsku suradnju i digitalnu transformaciju unutar regije. Rad nudi interdisciplinarni pristup koji spaja ekonomske, sigurnosne, jezične i tehnološke perspektive, s ciljem oblikovanja preporuka za stvaranje otpornije i sigurnije regionalne gospodarske arhitekture.
U ovom radu je primijenjen kvalitativni, komparativni pristup koji uključuje sustavni pregled literature, analizu nacionalnih strategija i institucionalne studije slučaja relevantne za regiju jugoistočne Europe.

Ključne riječi: geopolitička stabilnost, kibernetička sigurnost, regionalni razvoj

1. Uvod

U sve digitaliziranijem svijetu, kibernetička sigurnost postala je temelj ekonomske otpornosti, posebno u regijama obilježenim institucionalnom fragmentacijom i geopolitičkim napetošću. Jugoistočna Europa, koja uključuje Hrvatsku i susjedne zemlje, suočava se s jedinstvenim izazovima u usklađivanju nacionalnih infrastruktura kibernetičke sigurnosti sa širim ciljevima regionalnog razvoja. Iako je Europska unija (EU) uvela sveobuhvatne regulatorne okvire poput Zakona o kibernetičkoj otpornosti (Europska komisija, 2024), njihova provedba ostaje neujednačena u navedenoj regiji.

Kibernetička sigurnost često se shvaća kao isključivo tehničko pitanje, ali njezina uloga u poticanju ekonomske stabilnosti, atraktivnosti ulaganja i inovacijskog potencijala proteže se dalje od samog IT protokola. Prema Sulichu i suradnicima (2021), kibernetička sigurnost mora se shvatiti kao višedimenzionalni izazov koji uključuje institucionalne kapacitete, mehanizme izgradnje povjerenja i adaptivno upravljanje. Cilj ovog

istraživanja jest istražiti kako institucionalne i geopolitičke dimenzije utječu na sposobnost regije da koordinira kibernetičke politike i poboljša prekograničnu gospodarsku suradnju.

Iako su prethodna istraživanja temeljito ispitala politike kibernetičke sigurnosti na razini EU (Bendiek i Bund, 2023), manje je pozornosti posvećeno tome kako ti okviri funkcioniraju u regijama s nižim institucionalnim povjerenjem i izraženim jezičnim barijerama. Ovaj rad rješava taj nedostatak predlažući interdisciplinarnu perspektivu koja kombinira ekonomske, institucionalne i geopolitičke uvide u analizu otpornosti kibernetičke sigurnosti.

2. Metodologija

Istraživanje ovoga rada predlaže kvalitativni, komparativni pristup ispitivanju spremnosti za kibernetičku sigurnost i mehanizama regionalne koordinacije u jugoistočnoj Europi. Prvenstveno, proveden je sustavni pregled literature korištenjem relevantnih akademskih baza podataka poput Scopusa, Web of Science i Science Directa, s naglaskom na recenzirane znanstvene članke objavljene između 2015. i 2024. godine.

Polazeći od ciljeva istraživanja, rad se temelji na sljedećim istraživačkim pitanjima: (1) Kako institucionalni kapaciteti i razina povjerenja među državama regije utječu na učinkovitost koordinacije u području kibernetičke sigurnosti? (2) U kojoj mjeri nacionalne strategije kibernetičke sigurnosti doprinose privlačenju ulaganja i inovacijskom potencijalu regije? (3) Kako jezične i regulatorne barijere oblikuju prekograničnu suradnju u upravljanju kibernetičkom sigurnošću?

Drugo, provedena je analiza politika usporedbom nacionalnih strategija kibernetičke sigurnosti iz Hrvatske i nekoliko susjednih zemalja s direktivama EU-a, poput NIS2 i Zakona o kibernetičkoj otpornosti. Analizirani su ključni dokumenti s obzirom na njihovu usklađenost s regionalnim ciljevima i institucionalnim kapacitetima.

Treće, institucionalne studije slučaja preuzete su iz aktivnosti regionalnih projekata poput CyberSEE projekata Vijeća Europe i EU-a, koji promiču kibernetičku koordinaciju i razmjenu znanja (Vijeće Europe, 2024).

Ograničenja ovog istraživanja uključuju nedostatak empirijskih podataka za sve zemlje u regiji, jezične pristranosti u dostupnosti literature i brzo promjenjivu prirodu zakonodavstva EU u području kibernetičke sigurnosti.

3. Pregled literature

Kibernetička sigurnost je disciplina koja se još uvijek razvija na presjeku informacijske tehnologije, prava, upravljanja i ekonomske politike. Europska komisija (2024) naglašava kako je kibernetička otpornost ključna za zaštitu, ne samo digitalne imovine, već i demokratskih institucija i ekonomske infrastrukture. Međutim, prijelaz s politike i *slova na papiru* na praksu ostaje neravnomjeran među regijama, posebno u jugoistočnoj Europi.

Prema Sulichu i suradnicima (2021), otpornost u kibernetičkoj sigurnosti treba promatrati kao dinamičan sustav sposoban predvidjeti, apsorbirati i prilagoditi se digitalnim prijetnjama. Njihov model, koji se sastoji od otkrivanja, odgovora, prilagodbe i učenja, pruža korisnu analitičku perspektivu, iako zahtijeva regionalnu prilagodbu na temelju institucionalne spremnosti.

Bendiek i Bund (2023) tvrde da je regulatorni pristup EU prvenstveno namijenjen državama članicama s jakim administrativnim kapacitetima, a to može predstavljati izazove za manje razvijena institucionalna okruženja. Ovakva regulatorna neusklađenost

postaje još izraženija pri ispitivanju prekograničnih digitalnih rizika, posebno onih povezanih s kritičnom infrastrukturom i tokovima podataka.

Odebade i Benkhelifa (2023) ističu razlike u nacionalnim strategijama kibernetičke sigurnosti, napominjući da mnoge zemlje usvajaju okvire visoke razine bez specificiranja metrika provedbe. U regijama s ograničenim fiskalnim i ljudskim kapitalom, ovi nedostaci mogu rezultirati *papirnatom usklađenošću*, odnosno formalnim usvajanjem politika bez odgovarajućih operativnih kapaciteta.

Khan i suradnici (2024) u *Cybersecurity as a geopolitical tool* analiziraju kako države upotrebljavaju kibernetičke napade i digitalnu sabotažu kao instrument geopolitičke strategije – što može pogoršati nesigurnost i nestabilnost, osobito u geopolitički napetim regijama poput Zapadnog Balkana.

Još jedna zanemarena dimenzija je jezična interoperabilnost, koju Diplomacy.edu i DCAF (2016) identificiraju kao ključnu prepreku u regionalnoj suradnji. Dostupnost obuke za kibernetičku sigurnost i tehničkih standarda na materinskim jezicima je ograničena, što često dovodi do isključenja manjih gospodarstava ili država izvan EU iz ključnih inicijativa.

Nadalje, Kalisz (2023) naglašava ulogu javno-privatnih partnerstava (JPP) u izgradnji kibernetičke otpornosti. Njegovo istraživanje sugerira da lokalni ekosustavi u kojima surađuju poduzeća, akademska zajednica i vlade mogu značajno poboljšati izgradnju operativnih kapaciteta. Međutim, takvi su modeli još uvijek nerazvijeni u jugoistočnoj Europi, gdje je povjerenje u javne institucije često nisko.

Konačno, OECD (2022) izvještava da mala i srednja poduzeća (MSP) ostaju vrlo ranjiva zbog ograničene svijesti i nedovoljnih ulaganja u kibernetičku sigurnost. Navedeno je posebno problematično s obzirom na to da MSP-ovi čine gospodarsku okosnicu mnogih zemalja jugoistočne Europe, a što ih čini i metama i slabim karikama u lancu kibernetičke obrane.

4. Rezultati i rasprava

Nalazi ovog istraživanja ističu složen odnos između kibernetičke sigurnosti i regionalne ekonomske otpornosti, posebno u jugoistočnoj Europi. U zemljama poput Hrvatske, Slovenije i Srbije, strategije kibernetičke sigurnosti postoje na papiru, ali praktična provedba znatno varira zbog institucionalnih ograničenja, nedostatka povjerenja u institucije i ekonomskih asimetrija.

Kako tvrde Sulich i sur. (2021), kibernetičku sigurnost ne može se promatrati isključivo kroz prizmu nacionalne obrane, već ona mora biti ugrađena u ekonomsku politiku kao sistemski faktor rizika. To se posebno odnosi na posttranzicijska gospodarstva, gdje je digitalna infrastruktura često nedovoljno financirana, a institucije se suočavaju s izazovima u međusektorskoj koordinaciji.

Kritična ranjivost je niska uključenost MSP-ova u nacionalne inicijative za kibernetičku sigurnost. Prema OECD-u (2022), malim i srednjim poduzećima u jugoistočnoj Europi često nedostaju resursi i svijest za provedbu čak i osnovnih protokola kibernetičke sigurnosti. Navedeni nedostatak pripremljenosti izlaže cijele lance opskrbe riziku, posebno u prekograničnoj trgovini i digitalnim uslugama. Nedostatak ciljane podrške za MSP u nacionalnim strategijama (primjerice, financiranje obuke, pojednostavljeni mehanizmi usklađenosti) odražava jaz između namjere politike i ekonomske strukture (OECD, 2022, 2023).

Nadalje, JPP koja su se pokazala učinkovitima u provedbi politike

kibernetičke sigurnosti u zapadnoj Europi još uvijek su nerazvijena u regiji. Kalisz (2023) naglašava da su povjerenje, pravna jasnoća i uzajamna korist preduvjeti za uspješna JPP-a. Međutim, na Zapadnom Balkanu, povijesno nepovjerenje između privatnih aktera i vlada često potkopava tu suradnju; što dovodi do fragmentiranih napora i dupliciranih sustava, a ne do koherentnih, isplativih obrana.

Druga dimenzija zabrinutosti je nedostatak operativne interoperabilnosti između nacionalnih institucija, posebno timova za odgovor na računalne hitne slučajeve (CERT), što ometa koordinirane odgovore na kibernetičke incidente. Čak i kada zemlje dijele geopolitičke interese, razlike u regulatornim okvirima, tehničkim kapacitetima i jeziku ometaju suradnju u stvarnom vremenu (Diplomacy.edu i DCAF, 2016). Ove se prepreke pojačavaju tijekom kriza, a gdje su učinkovita komunikacija i povjerenje u zajedničke protokole ključni.

Što se tiče institucionalne spremnosti, Slovenija se ističe integriranim pristupom koji povezuje akademska istraživanja, industrijske partnere i javne institucije u jedinstveni okvir kibernetičke sigurnosti (Sulich i sur., 2021). Hrvatska je ostvarila napredak kroz Strategiju kibernetičke sigurnosti 2022. – 2026., no njezina provedba ostaje fragmentirana, posebice u pogledu međuagencijske koordinacije i angažmana dionika.

Kibernetička sigurnost također utječe na investicijsku klimu u regiji. Kao što su primijetili Osula i Rõigas (2017), investitori sve više procjenjuju kibernetičko upravljanje zemlje kao dio svoje analize rizika. Zemlje s transparentnim politikama, učinkovitom provedbom i međunarodnom suradnjom doživljavaju se kao sigurnija okruženja za digitalna ulaganja i inovacije. Suprotno tome, nedosljedni ili nerazvijeni okviri izazivaju zabrinutost zbog zaštite podataka, kontinuiteta poslovanja i pravnih sredstava.

Na kraju, pitanje jezične fragmentacije dodatno pogoršava regionalnu kibernetičku ranjivost. Različiti jezici, terminologija i administrativne tradicije predstavljaju prepreke standardiziranoj kriznoj komunikaciji i usklađenom regulatornom usklađivanju (Diplomacy.edu i DCAF, 2016). Navedeno može odgoditi ili iskriviti komunikaciju tijekom kibernetičkog incidenta, što zauzvrat utječe na ekonomsku stabilnost.

Ova istraživanja i njihovi zaključci sugeriraju da se kibernetička sigurnost više ne bi trebala tretirati kao sekundarno pitanje, već kao strateški prioritet za regionalnu otpornost. Integrirani pristup; onaj koji uključuje mala i srednja poduzeća, promiče javno-privatno povjerenje i potiče prekograničnu suradnju, mogao bi uvelike ojačati i ekonomsku i institucionalnu snagu u jugoistočnoj Europi.

Odgovori na postavljena istraživačka pitanja proizašli su iz analize literature i institucionalnih dokumenata. Prvo, institucionalni kapaciteti i razina međusobnog povjerenja uvelike određuju učinkovitost koordinacije kibernetičkih politika: zemlje s jačim administrativnim okvirima i razvijenim modelima javno-privatne suradnje (poput Slovenije) pokazuju bolju implementaciju sigurnosnih protokola. Drugo, nacionalne strategije koje sadrže konkretne mehanizme potpore malim i srednjim poduzećima te koje promiču transparentnu komunikaciju o rizicima kibernetičke sigurnosti pozitivno utječu na percepciju investicijskog rizika, čime postaju konkurentnije na regionalnoj razini. Treće, jezične razlike, regulatorne neusklađenosti i tehnička neujednačenost među državama značajno otežavaju uspostavu učinkovitih prekograničnih mehanizama suradnje, što se posebice očituje u

nedostatku interoperabilnosti CERT timova i slaboj operativnoj integraciji u kriznim situacijama.

4. Zaključak

Ovaj rad istražio je ulogu kibernetičke sigurnosti u jačanju regionalne ekonomske otpornosti kroz interdisciplinarnu prizmu koja kombinira ekonomske, institucionalne i geopolitičke perspektive. Zaključci pokazuju kako kibernetička sigurnost nije samo tehničko ili obrambeno pitanje, već i strukturna komponenta održivog razvoja u jugoistočnoj Europi. Slaba institucionalna koordinacija, niska uključenost MSP-a i ograničeno prekogranično povjerenje ključne su ranjivosti koje smanjuju spremnost regije za kibernetičke prijetnje.

Analiza istraživačkih pitanja pokazuje da institucionalna spremnost i razina povjerenja među dionicima predstavljaju temeljne preduvjete za uspješnu koordinaciju kibernetičke sigurnosti u regiji. Strategije koje uključuju konkretne mjere za MSP-ove, kao i transnacionalnu usklađenost s EU direktivama, djeluju kao čimbenici jačanja regionalne privlačnosti za ulagače. Međutim, složenost jezičnih i regulatornih barijera zahtijeva dodatne napore u izgradnji operativnih mehanizama suradnje, osobito u kriznim okolnostima kada brzina i jasnoća komunikacije postaju ključne. Stoga, daljnji razvoj regionalne otpornosti mora se temeljiti na jačanju institucionalne interoperabilnosti i uspostavi zajedničkih protokola djelovanja.

Da bi kibernetička sigurnost postala pravi pokretač regionalnog gospodarskog razvoja, mora biti ugrađena u šire strategije digitalne transformacije, privlačenja ulaganja i inovacijske politike. Jačanje javno-privatnog povjerenja, usklađivanje koordinacije CERT-a i izgradnja uključivih institucionalnih okvira nužni su koraci prema otpornijoj regionalnoj ekonomskoj arhitekturi.

Izvorni doprinos ovog istraživanja leži u naglasku na ekonomskim implikacijama kibernetičke sigurnosti kao faktora regionalnog razvoja, jer naglašava hitnost usklađivanja upravljanja kibernetičkom sigurnošću s izgradnjom institucionalnih kapaciteta i geopolitičkom suradnjom, posebno u digitalno povezanim, ali politički fragmentiranim regijama.

Buduća istraživanja trebala bi dodatno istražiti operativne stvarnosti kibernetičke sigurnosti u jugoistočnoj Europi putem empirijskih metoda, uključujući ankete i intervjue s institucionalnim akterima i MSP-ovima. Poseban naglasak trebalo bi staviti na procjenu učinkovitosti javno-privatnih partnerstava, jezičnih barijera u prekograničnoj koordinaciji i uloge kibernetičkog upravljanja u privlačenju stranih ulaganja. Razvoj regionalnog indeksa otpornosti na kibernetičku sigurnost i analiza uspješnih studija slučaja (poput slovenskog integrativnog modela) mogli bi pružiti prenosive strategije za jačanje institucionalne i ekonomske otpornosti u cijeloj regiji.

5. Literatura

Bendiek, A., & Bund, J. (2023). Shifting paradigms in Europe's approach to cyber defence: ambitions to disrupt malicious cyber activity need to protect norms as well as networks.

Diplomacy.edu & DCAF (2016). Cybersecurity in the Western Balkans: Policy gaps and cooperation. Geneva Centre for the Democratic Control of Armed Forces. https://www.diplomacy.edu/resource/cybersecurity-western-balkans-policy-gaps-cooperation/

Europska komisija (2024). Regulation (EU) 2024/2847 on Cyber Resilience Act. Official Journal of the European Union.

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R2847

Kalisz, A. (2023). Public-Private Partnerships on Cybersecurity and International Law: Finding Multilateral Solutions. In Symposium on'Public and Private Governance of Cybersecurity: Challenges and Potential'. Cambridge University Press.

Khan, A. W., Saeed, S., & Kakar, M. S. (2024). CYBERSECURITY AS A GEOPOLITICAL TOOL: THE GROWING INFLUENCE OF DIGITAL WARFARE IN STATECRAFT. International Research Journal of Social Sciences and Humanities, 3(2), 345-357.

OECD (2022). OECD Policy Framework on Digital Security, OECD Publishing, Paris, https://doi.org/10.1787/a69df866-en

OECD (2023).NEW PERSPECTIVES ON MEASURING CYBERSECURITY. OECD DIGITAL ECONOMY PAPERS. Dostupno na: https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/06/new-perspectives-on-measuring-cybersecurity_6069c1b9/b1e31997-en.pdf (pristupljeno: 4.6.2025.)

Odebade, A. T., & Benkhelifa, E. (2023). A comparative study of national cyber security strategies of ten nations. arXiv preprint arXiv:2303.13938.

Osula, A. M., & Rõigas, H. (2017). International Cyber Norms: Legal, Policy & Industry Perspectives. NATO Cooperative Cyber Defence Centre of Excellence.

Sulich, A., Rutkowska, M., Krawczyk-Jezierska, A., Jezierski , J., Zema, T. (2021). Cybersecurity and Sustainable Development.Procedia Computer Science. https://doi.org/10.1016/j.procs.2021.08.003

Vijeće Europe (2024). CyberSEE: Enhanced action on cybercrime and electronic evidence in South-East Europe and Türkiye – Project Summary and Activity Report. Council of Europe. Dostupno na: https://www.coe.int/en/web/cybercrime/cybersee (pristupljeno: 5.6.2025.)

THE ROLE OF CYBERSECURITY IN STRENGTHENING REGIONAL ECONOMIC RESILIENCE: INSTITUTIONAL AND GEOPOLITICAL PERSPECTIVES

Abstract: This paper explores the role of security and cybersecurity within a broader analysis of the regional economy of Southeast Europe, with a focus on the geopolitical and societal challenges that shape economic processes in Croatia and neighboring countries. In an increasingly digitalized economy, security infrastructure—including the protection of information systems, data, and communication channels—has become a key prerequisite for sustainable regional development, economic stability, and cross-border cooperation.

Cybersecurity is examined not only as a technical requirement, but also as an element closely linked to institutional capacities, security protocols, and the level of mutual trust among countries in the region. Language barriers further complicate the harmonization of security measures and crisis communication, increasing the risk of digital fragmentation within a space striving for integration.

The paper analyzes how varying levels of cyber resilience and security policies among countries affect investment attractiveness, innovation collaboration, and digital transformation across the region. An interdisciplinary approach is applied, combining economic, security, linguistic, and technological perspectives, with the aim of formulating recommendations for building a more resilient and secure regional economic architecture.

In this paper, a qualitative, comparative approach is applied, which includes a systematic literature review, analysis of national strategies and institutional case studies relevant to the region of Southeast Europe.

Keywords: cybersecurity, regional development, geopolitical stability

Ovaj rad je licenciran pod Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International.

Zaprimljen: 22.6.2025.
Odobren za objavu: 13.10.2025.
Stručni rad

KIBERNETIČKA SIGURNOST INDUSTRIJSKIH SUSTAVA

Mato Galović [1], Ivan Matasović [2], Mato Kokanović [3], Zoran Crnac [4]
[1] Tehnička škola, Eugena Kumičića 55, Slavonski Brod 35000, Republika Hrvatska, mgalovic@unisb.hr
[2] Tehnička škola, Eugena Kumičića 55, Slavonski Brod 35000, Republika Hrvatska, imatasovic@unisb.hr
[3] Tehnička škola, Eugena Kumičića 55, Slavonski Brod 35000, Republika Hrvatska, mkokanovic@unisb.hr
[4] Tehnička škola, Eugena Kumičića 55, Slavonski Brod 35000, Republika Hrvatska, zcrnac @unisb.hr

Sažetak: Koncept Industrije 4.0 se temelji na inteligentnom umrežavanju strojeva i drugih proizvodnih sustava koristeći napredne informacijsko – komunikacijske tehnologije. Korištenjem napredne informacijsko – komunikacijske tehnologije tvornice postaju sve više izložene kibernetičkim napadima i prijetnjama, koji imaju za cilj gubitak podataka neophodnih za odvijanje proizvodnih procesa, a posredno i usporavanje procesa proizvodnje, dok u nekim slučajevima rezultiraju oštećenjem opreme koja se koristi. Analizom utjecaja na informacijsko – komunikacijske tehnologije moguće je razviti preventivni sustav kibernetičkih utjecaja i time osigurati određenu zaštitu procesa.

Cilj ovog rada je upoznavanje sa osnovnim aktivnostima i tehnologijama kibernetičke sigurnosti u provođenju koncepta Industrije 4.0. U radu je provedena analiza Europskog izvješća o kibernetičkoj sigurnosti, kao i predložena rješenja zaštite od kibernetičkih napada u industriji. Detaljnije su objašnjeni oblici kibernetičkih prijetnji, te načini njihovog sprječavanja korištenjem industrijskih sigurnosnih standarda koji preciziraju načine i metode kibernetičke zaštite u različitem sferama djelovanja.

Ključne riječi: Industrija 4.0, informatičko – komunikacijske tehnologije, kibernetička sigurnost, sigurnosni standardi

1. Uvod

Glavno obilježje četvrte industrijske revolucije je umrežavanje pametnih digitalnih uređaja bežičnim putem, pri čemu međusobna povezanost proizvodnih sustava omogućava veći stupanj umjetne inteligencije, kvalitetniju komunikaciju pametnih uređaja međusobno kao i njihovu komunikaciju sa sudionicima proizvodnog procesa. U zahtijevanoj komunikaciji razmjenjuju se bitni podaci za odvijanje proizvodnih procesa koji moraju očuvati svoj integritet kako bi se osigurala pouzdana kvaliteta industrijske proizvodnje.

Zbog toga je kibernetička sigurnost industrijskih sustava ključna za zaštitu kritične infrastrukture i industrijskih pogona od digitalnih prijetnji.
Sigurnost i pouzdanost korištenja informacijske tehnologije (IT) odnosi se na zaštitu podataka, sustava i mreža od prijetnji te osiguravanje kontinuiranog i nesmetanog rada IT infrastrukture. Zaštita podataka je bitna iz dva osnovna razloga:

- krađa i neovlašteno korištenje podataka;
- utjecaj na podatke koji može štetno djelovati na njihovo korištenje;

- Razvojem IT tehnologije u cilju unapređenja industrijske proizvodnje, kibernetički napadi postaju sve sofisticiraniji, te je potrebna kontinuirana aktivnost u cilju njihovog otkrivanja, te sprječavanja utjecaja na odvijanje proizvodnje.
- Prema izvješću Agencije Europske unije za kibernetičku sigurnost (ENISA), postoji nekoliko glavnih kibernetičkih prijetnji (2022.) (Europski parlament 2023)
- ucjenjivački softver (ransomware). Prema podacima ENISA-e, iznos otkupnine je porastao s 13 milijuna eura u 2019. na 62 milijuna u 2021., a prosječna pojedinačna otkupnina se udvostručila sa 71 tisuće eura u 2019. na 150 tisuća eura u 2020. Procjenjuje se da je ucjenjivački softver u 2021. na globalnoj razini izazvao 18 milijardi eura štete, što je čak 57 puta više nego 2015. (Europski parlament 2023);
- zlonamjerni softver (malware) koji trajno ili privremeno oštećuje sustav, omogućava neovlašteni pristup, ometa rad sustava ili mreže, sve do krađe podataka. Prema podacima ENISA-e, u prvoj polovici 2022. se dogodilo više napada vezanih za Internet stvari nego u prethodne četiri godine;
- društveni inženjering koji se manifestira kroz iskorištavanje ljudske pogreške otvaranjem zlonamjernih dokumenata, nesigurne e-pošte ili posjećivanjem sigurnosno neprovjerenih web stranica;
- prijetnje podacima kroz povredu podataka ili njihovo objavljivanje bez dopuštenja vlasnika;
- prijetnje dostupnosti ili uskraćivanja pristupa podacima i uslugama. Jedan od najčešćih oblika ove vrste prijetnji je preopterećenje mrežne infrastrukture u cilju nedostupnosti potrebnih podataka;
- Internetska dostupnost. Sprječavanje dostupnosti interneta bitno smanjuje komunikaciju u cilju prikupljanja potrebnih informacija, a time i mogućnost njihovog korištenja;

Kibernetički napadi na industrijske sustave mogu uzrokovati zastoj i kvarove u proizvodnji, gubitak podataka za rad automatiziranih upravljačkih sustava (PLC, SCADA), a u određenoj mjeri mogu utjecati na sigurnost ljudi i okoliša.

Izvješće Nozomi Network Labs, koji proučava utjecaj kibernetičkih napada na industrijske sustave bilježi da je tijekom prve polovice 2024. godine broj kibernetičkih prijetnji bio najveći u sektoru proizvodnje, slijedi sektor energetike, komunikacija i transportnih sustava (IoT Cyber Security 2025)

Istraživanja Agencije Europske unije za kibernetičku sigurnost pokazalo je da je razina kibernetičkih prijetnji tijekom jednogodišnjeg razdoblja (srpanj 2023. do lipanj 2024.) u značajnom porastu. U svom izvješću o stanju kibernetičke sigurnosti u Europskoj uniji za 2024. godinu definirana je količina incidenata prema vrsti prijetnje u navedenom vremenskom razdoblju (Izvješće 2024).

Najviše incidenata je uzrokovano Dos/Ddos/Rdos prijetnjama koje za posljedicu imaju uskraćivanje usluga korištenja potrebnih podataka iz jednog zlonamjernog izvora (Dos) kako bi se oslabila pozicija korisnika, više njih (Ddos) ili uskraćivanja usluga u cilju iznude otkupnine.

Značajan broj incidenata je vezan za ransomware prijetnje. Nakon zaraze *ransomware* može šifrirati datoteke ili onemogućiti njihovo korištenje. Od korisnika čije je računalo zaraženo traži se otkupnina u zamjenu za daljnje normalno korištenje računala. (CARNet 2025)
Jednako tako je značajan zlonamjerni utjecaj na podatke u prijenosu koji se

manifestira kroz krađu podataka, sprječavanje njihovog korištenja ili aktivnosti usmjerene na izmjenu podataka.

Uz sve ostale evidentirane prijetnje, kao i činjenice da razvoj novih kibernetičkih prijetnji prati razvoj informacijskih tehnologija, potrebno je posebnu pažnju posvetiti kibernetičkoj sigurnosti.

Osnivanjem stručnih organizacija na globalnoj razini , kao što je Agencija Europske unije za kibernetičku sigurnost (ENISA), ili onih na razini država, kao što je Nacionalni centar za kibernetičku sigurnost (NCSC – HR) , razvijaju se regulativni okviri za razvoj i praćenje provedbe kibernetičke sigurnosti. Jedan od njih je i industrijski sigurnosni standard ISA/IEC 62443.

ISA/IEC 62443 je međunarodni niz standarda koje je razvila Međunarodna elektrotehnička komisija (IEC) za kibernetičku sigurnost u industrijskoj automatizaciji i upravljačkim sustavima (IACS). Primarna svrha norme IEC 62443 je zaštita industrijskih okruženja od rastućih kibernetičkih prijetnji. Serija standarda ISA/IEC 62443 definira zahtjeve i procese za implementaciju i održavanje elektronički sigurnih industrijskih automatizacijskih i upravljačkih sustava (IACS). (ISA 2025)

2. Materijali i metode

Usporedno sa ubrzanim razvojem informacijskih tehnologija koje omogućavaju kvalitetnu i nesmetanu komunikaciju komponenti procesnih sustava Industrije 4.0, razvijaju se i različite vrste računalnih napada koji imaju za cilj nanijeti štetu ili osigurati pristup, a samim time i steći kontrolu nad važnim dokumentima vezanim za odvijanje procesa.

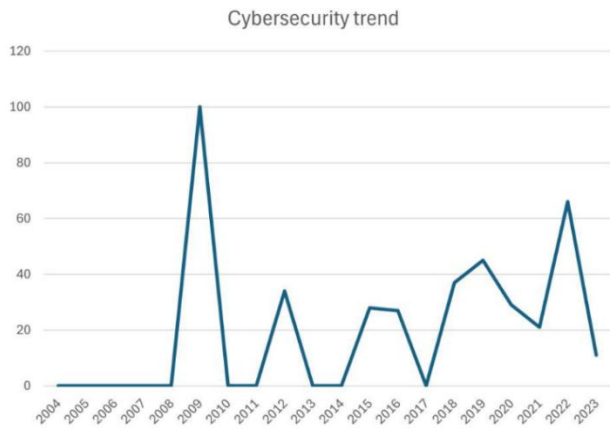
Kako je cilj implementacije i razvoja Industrije 4.0 povećanje učinkovitosti proizvodnje, a to se postiže prilagodbom novim tehnologijama i tehnologijama u razvoju, potrebno je osigurati zaštitu podataka koji su bitni za relevantno funkcioniranja koncepta Industrije 4.0. Prvi i osnovni zadatak je osigurati pouzdano korištenje i prijenos podataka, što podrazumijeva ostvarenje adekvatne kibernetičke sigurnosti.

Jedna od glavnih briga u kontekstu kibernetičke sigurnosti Industrije 4.0 jest mogućnost da kibernetički napadi poremete proizvodni proces. U proizvodnom okruženju, čak i manji poremećaj može imati značajne posljedice, uključujući kašnjenja i financijske gubitke. Osim toga, integracija umjetne inteligencije i strojnog učenja u proizvodne procese znači da postoji mogućnost da zlonamjerni akteri manipuliraju ili poremete te sustave, što dovodi do neispravnih ili čak opasnih proizvoda (Teixiera, Asencao 2025).

Prema definiciji, kibernetička sigurnost je umijeće zaštite mreža, uređaja i podataka od neovlaštenog pristupa ili kriminalne upotrebe te praksa osiguranja povjerljivosti, integriteta i dostupnosti informacija (Pochmara, Sietlicka 2024).

Prema J. Pochmara i A. Swietlicka (Pochmara, Sietlicka 2024), interes za kibernetičku sigurnost u kontekstu Industrije 4.0 doživio značajan porast počevši oko 2009. godine, s vrhuncem u 2022. godini. Interes je ostao relativno nizak od 2004. do 2008. godine, postupno se povećavajući u 2009. godini, a zatim ima promjenjivi trend u sljedećim godinama. Postoje povremeni skokovi interesa, kao što su bili 2012., 2015., 2016., 2018. i 2019. godine, ali najznačajniji vrhunac događa se 2022. godine, što ukazuje na pojačan fokus na kibernetičku sigurnost unutar Industrije 4.0 tijekom tog razdoblja.

Prema slici 1, vrijednost 100 označava najveći interes za kibernetičku sigurnost, dok vrijednost 50 znači da je interes upola manji. Vrijednost 0 označava da nema dovoljno dostupnih podataka za zadani pojam.



Slika 1. Trend kibernetičke sigurnosti na temelju Google Trendsa (Pochmara, Sietlicka 2024)

2.1. Vrste kibernetičkih prijetnji

Prema Oumaima El Kouari, Saiida Lazaar i Tarik Achoughi, najčešći tipovi prijetnji vezanih za Industrijski Internet (IIoT) [8] su:

- napadi s naprednim trajnim prijetnjama (*Advanced Persistent Threat* - APT);
- napadi uskraćivanja usluge (Denial of Service - DoS);
- napadi tipa "čovjek u sredini" (*Man In The Middle*- MitM);
- malware softver;
- *phishing napadi*;
- napadi autentifikacije;

2.2. Sigurnost i pouzdanost korištenja informacijske tehnologije

Sigurnost i pouzdanost korištenja informacijske tehnologije (IT) odnosi se na zaštitu podataka, sustava i mreža od prijetnji, te osiguravanje kontinuiranog i nesmetanog rada IT infrastrukture. U suvremenim organizacijama i društvu, IT sustavi igraju ključnu ulogu u poslovanju, zbog čega je važno implementirati sveobuhvatan pristup za osiguranje njihovog ispravnog i sigurnog rada.

Industrijska informacijska tehnologija (IIT) funkcionira kao veza između područja informacijske tehnologije (IT) i područja operativne tehnologije (OT) (Kouari, Lazaar 2025) . Pomaže u prikupljanju podataka iz OT područja i njihovom prijenosu u IT područje. Ovi podaci nisu izravno povezani s upravljanjem strojevima i sustavima, ali su ključni za kontrolu i optimizaciju procesa, praćenje kvalitete, logistiku i protok materijala. Stoga se koncept sigurnosti i pouzdanosti informacijske tehnologije općenito primjenjuje i na industrijsku informacijsku tehnologiju koju koriste sustavi Industrije 4.0.

Ključni koncepti sigurnosti informacijske tehnologije su pokazani slikom 2.

Slika 2. Koncepti sigurnost i pouzdanosti informacijske tehnologije

Sigurnost informacija odnosi se na praksu zaštite informacija od neovlaštenog pristupa, otkrivanja ili izmjene i uništenja informacija. Sigurnost mreže ima za cilj zaštititi mreže od neovlaštenog pristupa, što omogućuje krađu podataka i izvođenje zlonamjernih napada.

Fizička sigurnost interneta odnosi se na zaštitu fizičke infrastrukture koja omogućuje funkcioniranje internetske mreže.

Malware zaštita - Zlonamjerni program općenito je poznat malware, namjerno je dizajniran da uzrokuje probleme u mrežama i šteti na razne načine. Primarni cilj malwarea je poremetiti

normalno izvršavanje ili dobiti neovlašteni pristup (Gupta et al 2025). U ovisnosti o načinu na koji zlonamjerni softver napada podatke, i rezultatu njegovog djelovanja postoje različite vrste prema kojim se posljedično određuje i način zaštite od njihovog djelovanja. Upravljanje identitetom i pristupom (Identity and access management - IAM) je složen i ključan proces identificiranja, pažljivog praćenja, učinkovite kontrole. Obuhvaća sveobuhvatan raspon aktivnosti koje omogućuju nesmetano funkcioniranje sustava kontrole pristupa, diktirajući i regulirajući dozvole za dopušteni i ograničeni pristup (Ghadge 2024).

Backup podataka (sigurnosna kopija podataka) je proces izrade kopije podataka kako bi se osigurala njihova dostupnost i zaštita u slučaju gubitka podataka, oštećenja, tehničkog kvara, prirodnih katastrofa ili drugih problema. Backup je ključan dio svake strategije za oporavak od katastrofa (Disaster Recovery) i osigurava kontinuitet poslovanja.

Enkripcija (ili šifriranje) je kodiranje informacija tako da im neovlaštene osobe ne mogu pristupiti. Ako se podaci u šifriranom obliku izgube ili ukradu, postoji minimalan rizik od otkrivanja jer napadač neće imati ključ za dešifriranje (ESET 2025).

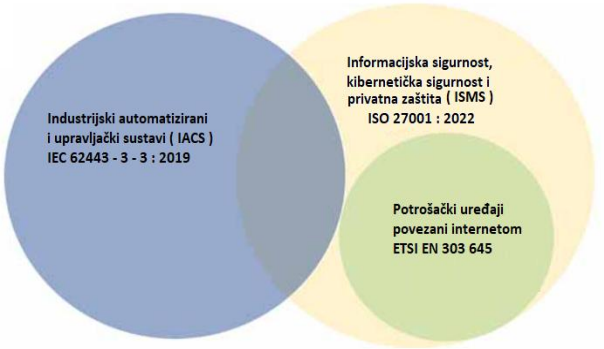
Ažuriranje softvera odnosi se na proces nadogradnje postojećih programa i operativnih sustava kako bi se poboljšala njihova funkcionalnost, sigurnost, stabilnost i performanse. Ažuriranja mogu uključivati ispravke grešaka, sigurnosne zakrpe, nove značajke i optimizacije.

Praćenje i nadzor sustava (eng. Monitoring) je proces kontinuiranog praćenja rada i performansi računalnih sustava, mreža, aplikacija i drugih IT resursa kako bi se osiguralo njihovo optimalno funkcioniranje, sigurnost i dostupnost.

Edukacija korisnika je bitna iz razloga sigurnosti korištenja IT tehnologije. Također, kao posljedica brzog razvoja IT sustava, potrebno je provoditi kontinuiranu edukaciju sa ciljem stjecanja kompetencija vezanih za nove situacije.

3. Rezultati i rasprava

Standardi kibernetičke sigurnosti pružaju strukturirani pristup upravljanju i procjeni rizika kibernetičke sigurnosti. Oni su primarni izvor sigurnosnih zahtjeva i kontrola koje organizacije koriste za smanjenje vjerojatnosti i utjecaja kibernetičkih napada. Postoji velik broj sigurnosnih standarda. Na primjer, samo serija ISO/IEC 27000 obuhvaća preko 60 standarda koji se bave širokim spektrom problema sigurnosti informacija (Džebar, Nordstorm, 2023) . Iako su standardi kibernetičke sigurnosti, ISO/IEC 27001, ETSI EN 303 645 i ISA/IEC 62443-3-3, izvorno dizajnirani za različita okruženja, oni dijele brojne zajedničke i generičke zahtjeve kibernetičke sigurnosti koji su valjani i primjenjivi u različitim industrijama i ICT okruženjima (Džebar, Nordstorm, 2023).



Slika 3. Povezanost standarda kibernetičke sigurnosti (Džebar, Nordstorm, 2023)

3.1. Standard ISO/IEC 27001

Standard ISO/IEC 27001 predstavlja se kao standard koji specificira zahtjeve za uspostavljanje, provedbu, održavanje i kontinuirani razvoj strategije sigurnosti informacija. Osim toga, uključuje

potrebne okolnosti koje su prilagođene kako bi ispunile očekivanja tvrtke za procjenu i upravljanje prijetnjama sigurnosti podataka. Ovi preduvjeti su bitni za osiguravanje učinkovitog ublažavanja rizika sigurnosti informacija. Uvjeti navedeni u ISO/IEC 27001 nisu specifični, što znači da se očekuje da će se primjenjivati na sve organizacije, bez obzira na vrstu, veličinu ili prirodu poslovanja (Kitsios, Chatzidimitriou, Kamariotou, 2025).

Norma ISO 27001 osigurava povjerljivost, integritet i dostupnost, što su glavni sigurnosni ciljevi ove norme. Povjerljivost je namijenjena osiguravanju da su informacije dostupne samo ovlaštenim osobama primjenom mehanizama šifriranja i kontrole pristupa. Integritet osigurava da se podaci mijenjaju samo na ovlaštene načine, što štiti organizaciju od napadača koji pokušavaju promijeniti informacije, a također štiti od nenamjernih tehničkih pogrešaka. Dostupnost osigurava da su informacije dostupne sustavu ili ovlaštenim osobama kad god su potrebne (Junaid, 2025).

Analizirajući ciljeve standarada ISO/IEC 27001, njegova učinkovitost se pokazuje kroz smanjenje utjecaja kibernetičkih napada, te osiguranje integriteta svih relevantnih podataka bitnih za organizaciju koja ga provodi. Posredno , standard omogućava veću učinkovitost i ekonomičnost proizvodnje te smanjenje tehnoloških rizika u odvijanju proizvodnih procesa.

Standard ETSI EN 303 645 definira osnovne sigurnosne zahtjeve, takozvane odredbe, za potrošačke IoT uređaje. Prema uvodu u normu ETSI EN 303 645, norma sa svojim osnovnim sigurnosnim zahtjevima „nije namijenjena rješavanju svih sigurnosnih izazova povezanih s potrošačkim IoT-om. Također se ne usredotočuje na zaštitu od napada koji su dugotrajni/sofisticirani ili koji zahtijevaju trajni fizički pristup uređaju. Umjesto toga, fokus je na tehničkim kontrolama i organizacijskim politikama koje su najvažnije u rješavanju najznačajnijih i najraširenijih sigurnosnih nedostataka" (Körner et al 2025). Korištenje norme ETSI EN 303 645 omogućuje proizvođačima da osiguraju niz značajki u IoT uređajima za zaštitu osobnih podataka korisnika, kao što je na primjer davanje potrošačima jasnih i transparentnih informacija o tome koji se osobni podaci obrađuju, kako se koriste, od koga i u koje svrhe.

3.2. Industrijski sigurnosni standard ISA/IEC 62443

Standard ISA/IEC 62443 (serija standarda) definira zahtjeve i procese za implementaciju i održavanje elektronički sigurnih industrijskih automatizacijskih i upravljačkih sustava (IACS). ISA/IEC standardi postavljaju standarde kibernetičke sigurnosti u svim industrijskim sektorima koji koriste IACS, uključujući automatizaciju zgrada, proizvodnju i distribuciju električne energije, medicinske uređaje, transport i procesne industrije poput kemikalija te nafte i plina (ISA, 2025).
Temeljno načelo standarda ISA/IEC 62443 je koncept zajedničke odgovornosti kao ključnog elementa kibernetičke sigurnosti u području automatizacije. Ključne skupine dionika moraju se uskladiti kako bi osigurale sigurnost, integritet, pouzdanost i zaštitu upravljačkih sustava. Standardi definiraju zahtjeve za ključne skupine dionika koje su uključene u kibernetičku sigurnost upravljačkih sustava. Serija ISA/IEC 62443 bavi se sigurnošću industrijskih automatizacijskih i upravljačkih sustava (IACS) tijekom cijelog njihovog životnog ciklusa (što se odnosi na sve automatizacijske i upravljačke sustave, ne samo industrijske) (ISA, 2025).
Standardi ISA/IEC 62443 pružaju smjernice koje uključuju:

- Definiranje zajedničkih pojmova, koncepata i modela koje mogu koristiti svi dionici odgovorni za kibernetičku sigurnost kontrolnih sustava;

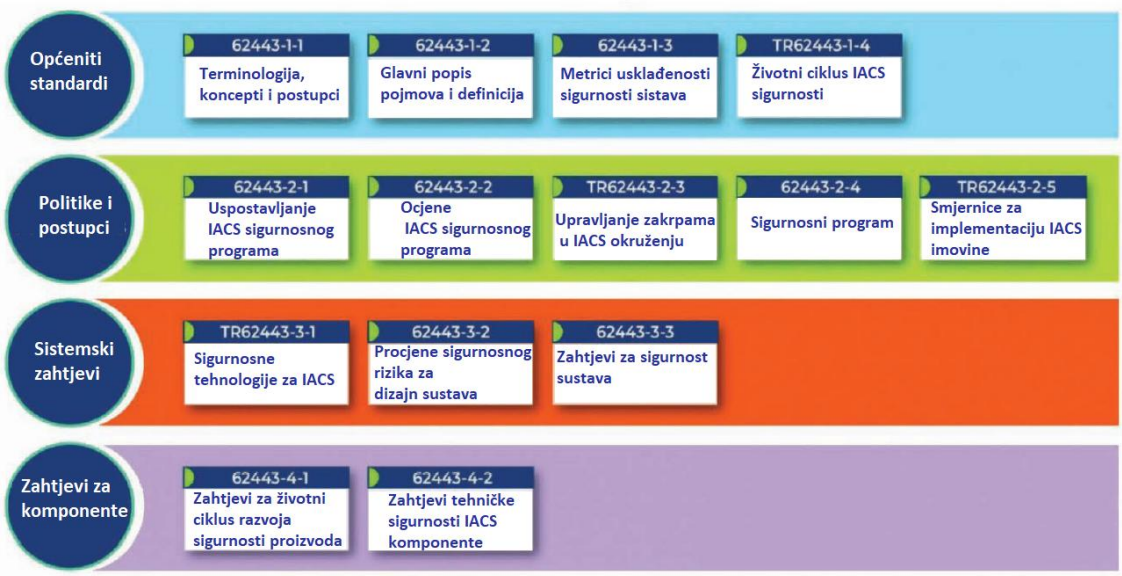
- Pomaganje vlasnicima imovine u određivanju razine sigurnosti potrebne za zadovoljavanje njihovih jedinstvenih poslovnih potreba i potreba u vezi s rizikom;
- Uspostavljanje zajedničkog skupa zahtjeva i metodologije životnog ciklusa kibernetičke sigurnosti za razvojne programere proizvoda, uključujući mehanizam za certificiranje proizvoda i procesa razvoja dobavljača;
- Definiranje procesa procjene rizika koji su ključni za zaštitu kontrolnih sustava(ISA, 2025);

Serija standarda ISA/IEC 62443 raspoređena je u četiri osnovne skupine koje odgovaraju fokusu njihove primjene (ISA, 2025):

1. skupina – Općeniti standardi koji obuhvaćaju dokumente koji su zajednički za cijelu seriju standarda.
2. skupina – Politike i postupci sadrži dokumente koji su usmjereni na politike i postupke povezane sa sigurnošću IACS-a.
3. skupina – Sistemski zahtjevi sadrže dokumente vezane za zahtjeve na razini sustava
4. skupina – Zahtjevi za komponente – sadrže dokumente koji daju informacije o specifičnim i detaljnim zahtjevima povezanim s razvojem IACS proizvoda.

ISA/IEC 62433 je ključan za industrijsku kibernetičku sigurnost jer pruža sveobuhvatan okvir za rješavanje rizika od kibernetičkih napada. Obuhvaća procjenu rizika, dizajn sustava, siguran razvoj i uloge dionika sustava, pomažući industrijskim organizacijama da poboljšaju svoju sigurnost i održe kontinuitet rada.

Detaljni prikaz politike pojedinih skupina je pokazan na slici 4.



Slika 4. Serija ISA/IEC 62334 standarda (ISA, 2025).

4. Zaključak

U radu se analiziraju aktivnosti i tehnologije kibernetičke sigurnosti sustava u konceptu Industrije 4.0. Bitan naglasak je stavljen na kibernetiku informacijsko-komunikacijskih tehnologija. Ranjivost ovih sustava je uzrokovana zlonamjernim aktivnostima u cilju krađe i neovlašteno korištenje podataka, te utjecaja na podatke koji može štetno djelovati na njihovo korištenje. Kako je razvoj sustava za zlonamjerno djelovanja proporcionalan razvoju sustava industrijske proizvodnje, potreban je kontinuirani i svrsishodan mehanizam zaštite. Koncepti sigurnosti i pouzdanosti informacijske tehnologije su definirani standardima kibernetičke sigurnosti koji pružaju strukturirani pristup upravljanju i procjeni rizika kibernetičke sigurnosti.

Oni definiraju razinu sigurnosnih zahtjeva i kontrola koje je potrebno koristiti za smanjenje vjerojatnosti i utjecaja kibernetičkih napada. Primjenom navedenih standarda uz kontinuirano praćenje i edukaciju u području kibernetičke sigurnosti, omogućuje se kvalitetan okvir za nesmetan razvoj i provođenje aktivnosti Industrije 4.0.

5. Literatura

Europski parlament, Cybersigurnost: glavne i rastuće prijetnje, https://www.europarl.europa.eu/topics/hr/article/20220120STO21428/kibersigurnost-glavne-i-rastuce-prijetnje (21. ožujka 2023.)

https://www.nozominetworks.com/ot-iot-cybersecurity-trends-insights-february-2025 (veljača 2025.)

Izvješće o stanju kibernetičke sigurnosti u Uniji za 2024. – sažeta verzija .pdf https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union (3. prosinac 2024.)

Hrvatska akademska i istraživačka mreža CARNET - https://www.cert.hr/19795-2/ransomware/ (veljača 2025.)

Međunarodno društvo za automatizaciju (ISA) https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards (veljača 2025.)

Henrique Teixiera, Claudia Asencao, Joao Goncalves, ergio Francisco Sargo Ferreira Lopes - Kibernetička sigurnost u Industriji 4.0. i IoT : Izazovi i prilike https://www.researchgate.net/publication/381349261_Cybersecurity_in_Industry_40_and_Internet_of_Things_Challenges_and_Opportunities (svibanj 2025.)

Janusz Pochmara i Aleksandra Swietlicka : Kibernetička sigurnost industrijskih sustava – izvješće za 2023. godinu (25. ožujak 2024.) https://www.mdpi.com/2079-9292/13/7/1191

Oumaima El Kouari, Saiida Lazaar i Tarik Achoughi : Jačanje industrijske kibernetičke sigurnosti: nova arhitektura industrijskog interneta stvari poboljšana integracijom honeypota , Međunarodni časopis za elektrotehniku i računarstvo (IJECE) Svezak 15, br. 1, veljača 2025., str. 1089 – 1098, https://ijece.iaescore.com/index.php/IJECE/article/view/36124

Nikhil Ghadge - Poboljšanje otkrivanja prijetnji u sustavima upravljanja identitetom i pristupom (IAM), Međunarodni arhiv časopisa za znanost i istraživanje, 2024., 11(02), 2050–2057, travanj 2024.

Ketan Gupta ; Nasmin Jiwani ; Md Haris Uddin Sharif ; Ripon Datta ; Neda Afreen - Pristup neuronskih mreža za klasifikaciju zlonamjernog softvera, https://ieeexplore.ieee.org/abstract/document/10037653 (svibanj 2025.)

https://ijsra.net/content/enhancing-threat-detection-identity-and-access-management-iam-systems (svibanj 2025.)

ESET korisnička aplikacija, https://help.eset.com/glossary/hr-HR/encryption.html (svibanj 2025.)

Fatiha Džebar, Kim Nordström - Komparativna analiza standarda industrijske kibernetičke sigurnosti, Objavljeno u: IEEE Access (Svezak: 11), kolovoz 2023. https://ieeexplore.ieee.org/abstract/document/10210561 (svibanj 2025.)

Fotis Kitsios, Elpiniki Chatzidimitriou i Maria Kamariotou - Standard upravljanja sigurnošću informacija ISO/IEC 27001: Kako izvući vrijednost iz podataka u IT sektoru, izdanje Upravljanje kvalitetom i održivost https://ideas.repec.org/a/gam/jsusta/v

15y2023i7p5828-d1108964.html (svibanj 2025.)

Ta-Seen Junaid - ISO 27001: Upravljanje sigurnošću informacija, Fakultet računalnih znanosti i inženjerstva Sveučilište primijenjenih znanosti Frankfurt Frankfurt na Majni, Njemačka https://www.researchgate.net/profile/Ta-Seen-Junaid/publication/367166657_ISO_27001_Information_Security_Management_Systems/links/63c4e6536fe15d6a5722c964/ISO-27001-Information-Security-Management-Systems.pdf (svibanj 2025.)

Felix Körner, Pascal Schäfer, Holger Zwingmann, Bettina Schnor, Samim Ahmadi - Trenutni izazovi implementacije ETSI EN-a 303 645 kao osnovni sigurnosni standard za certifikaciju sigurnosti potrošačkog IoT-a, Institut za računalne znanosti, Sveučilište u Potsdamu, Njemačka https://www.techrxiv.org/doi/full/10.36227/techrxiv.24711672 (svibanj 2025.)

Međunarodno društvo za automatizaciju (ISA), https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

Međunarodno društvo za automatizaciju (ISA), Sigurnost industrijskih automatizacijskih i upravljačkih sustava Pregled standarda ISA/IEC 62443 https://21577316.fs1.hubspotusercontent-na1.net/hubfs/21577316/2023%20ISA%20Website%20Redesigns/ISAGCA/PDFs/ISAGCA%20Quick%20Start%20Guide%20FINAL.pdf (svibanj 2025.)

CYBER SECURITY OF INDUSTRIAL SYSTEMS

Summary: The concept of Industry 4.0 is based on intelligent networking of machines and other production systems using advanced information and communication technologies. Through the use of advanced information and communication technology, factories become increasingly exposed to cyber attacks and threats, which aim at the loss of data necessary for the development of production processes, and indirectly also the slowing down of the production process, while in some cases it results in damage to the equipment being used. By analyzing the impact on information and communication technologies, it is possible to develop a preventive system of cybernetic influences and thereby ensure a certain protection of the process.

The aim of this paper is to familiarize with the basic activities and technologies of cyber security in the implementation of the concept of Industry 4.0. The paper contains an analysis of the European report on cyber security, as well as proposed solutions for protection against cyber attacks in the industry.

The forms of cyber threats and the ways of their use are explained in more detail using industrial security standards that specify the ways and methods of cyber protection in different spheres of activity.

Keywords: Industry 4.0, IT - communication technologies, cyber security, security standards

Ovaj rad je licenciran pod Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International.

Zaprimljen: X.X.XXXX.
Odobren za objavu: X.X.XXXX.
Klasifikacija rada

14pt

NASLOV RADA (Verdana, 14pt, Bold)

14pt

14pt

Ime Prezime[1], Ime Prezime[2],…

[1] Sveučilište u Slavonskom Brodu, Trg I. B. Mažuranić 2, 35000 Slavonski Brod, Hrvatska, ePošta: festung@unisb.hr (Verdana, 10pt)

14pt

Sažetak: Naslov rada može imati najviše 15 riječi. Nakon naslova potrebno je navesti puna imena i prezimena autora bez titula. Sažetak može imati najviše 200 riječi i treba vjerno opisati temu rada. Potrebno je navesti svrhu i cilj rada, korištene metode, rezultate te doprinose rada. Ključne riječi moraju biti vezane uz naslov i sažetak rada. Za jezičnu i gramatičku ispravnost rada odgovoran je autor. Nakon završenog recenzentskog postupka od autora se mogu zatražiti određene ispravke ili dopune sažetka i/ili rada. (Verdana, 10pt).

10pt

Ključne riječi: abecedni popis ključnih riječi (maksimalno 6 ključnih riječi) (Verdana 10pt)

14pt

14pt

1. Uvod (Verdana, 11, Bold)

11pt

Uvod je početni ili pristupni dio radu u kojem autor daje početne informacije o problemu koji je predmetom rješavanja.

11pt

U uvodu se daje prikaz temeljne karakteristike problema, ciljeve koji se žele postići te zadaće koje vode do ostvarenja planiranih ciljeva. Dobro je navesti što je o problemu poznato, a što nije. Uvod ne bi trebao biti suviše opsežan.

11pt

2. Metodologija(Verdana, 11, Bold)

11pt

Navesti kraći prikaz mogućih metoda, načina i putova rješavanja problema kao i ograničenja koja su se u radu morala uzeti u obzir i uvažavati.

11pt

2.1. Upute autorima (Verdana, 11, Bold)

11pt

Radovi podliježu postupku dvostruke slijepe recenzije koju provode domaći i strani recenzenti. U okviru postupka recenziranja, radovi objavljeni u časopisu svrstavaju se u jednu od sljedećih kategorija: izvorni znanstveni rad, prethodno priopćenje, pregledni rad i stručni rad. Radovi mogu biti na hrvatskom jeziku ili engleskom jeziku (uz odobrenje odbora), a sažetci te ključne riječi moraju biti i na hrvatskom i na engleskom jeziku.

11pt

Izvorni znanstveni rad (original scientific article) sadrži neobjavljene rezultate izvornih teorijskih ili praktičnih istraživanja koje je autor naveo tako da se mogu provjeriti njihova točnost i točnost analize.

11pt

Prethodno priopćenje (preliminary communication) sadrži građu ili podatke koji zahtijevaju brzo objavljivanje ili dijelove većeg istraživanja.

11pt

Pregledni je rad (review article) kritički i analitički pregled nekog područja istraživanja ili jednog njegova dijela. U članku treba biti vidljiv autorov doprinos proučavanju odabrane problematike, a citirana literatura treba biti cjelovita.

11pt

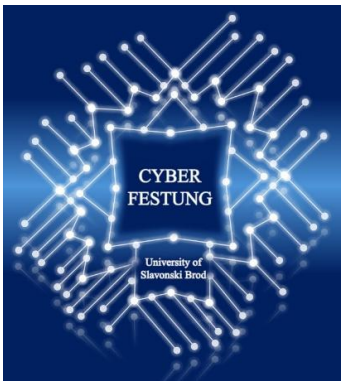
Stručni rad (professional paper) sadržava već poznate, objavljene rezultate znanstvenoga istraživanja i težište usmjerava na njihovu primjenu u praksi ili na njihovo širenje u obrazovne svrhe. Sadrži korisne priloge iz područja struke

koji nisu vezani uz izvorna autorova istraživanja, a iznesena zapažanja ne moraju biti novost u struci. Moraju biti napisani na sustavan i razumljiv način, u skladu s čitateljskim profilom.
11pt
O objavljivanju ostalih radova (prikazi dobrih praksi, skupova i knjiga) odlučuje uredništvo i glavni urednik
11pt

2.2. Oblikovanje rada (Verdana, 11, Bold)
11pt
Opseg rada u pravilu bi trebao biti od 4 do 6 stranica, uključujući tekst, crteže, tablice, dijagrame, fotografije sa popisom literature bez priloga.
11pt
Tekst pisanog dijela rada treba pisati u dva stupca, Verdana 11, jednostruki prored kao što je pisan i ovaj tekst. Rečenice trebaju biti stručno jasne, nedvosmislene i pisane u trećem licu jednine. Svi preuzeti dijelovi teksta, slike i tablice moraju biti citirani sukladno standardima APA stila (APA 7th edition)
11pt

2.3. Potpoglavlje (Verdana, 11, Bold)
11pt
Poglavlje u kojem se razmatraju dobiveni rezultati, vrši vrednovanje vlastitog rješenja problema, razmatra ostale probleme koji su se javili prilikom rješavanja zadatka te na osnovi vlastitog iskustva razmatraju moguća poboljšanja. Kako će točno biti definirani naslovi poglavlja i potpoglavlja ovisi o naravi i vrsti problema
11pt

2.4. Slike i tablice (Verdana, 11, Bold)
11pt
Slike i tablice trebaju biti centrirane i numerirane. Opis slike nalazi se ispod slike a opis tablice iznad tablice.
11pt



Slika 1: Izgled slike (Verdana, 11pt)
11pt
Prilikom postavljanja slike na vrh stranice, vrh slike treba biti u ravnini s donjim rubom prvog retka teksta. Svi simboli i slova trebaju biti visoki najmanje 2 mm. Treba izbjegavati korištenje teških crnih i/ili obojenih podebljanih slova jer će izgledati neugodno tamno prilikom ispisa. Također, moraju biti smješteni blizu prve reference na njih u tekstu i numerirani uzastopno. Natpis slike treba postaviti odmah ispod slika. Fotografije i slike trebaju biti pripremljene u boji pri minimalnoj razlučivosti od 300 dpi. Ne koristite uzorke u vektorskoj grafici. Slike je potrebno pripremiti u PNG ili JPEG formatu.

11pt
Tablica 1. Upute autorima (Verdana 11)

Rd.br.	Naziv	Opis
1.	Veličina papira	Koristiti A4 format papira (210 x 297) bez numeriranja.
2.	Veličina članka	Rad treba biti u opsegu od 4 do 6 stranica
3.	Margine/stupci	Sve margine trebaju biti 2 cm Stupci trebaju biti široki 8, razmak između stupaca 1 cm novi odjeljak ne treba započinjati izravno na dnu stranice, već je sami naslov potrebno prenijeti na vrh sljedećeg stupca; duljinu područja teksta moguće je prekoračiti samo za jedan redak kako bi se dovršio dio teksta ili odlomak.
4.	Izgled stranice	Glavni dio teksta treba biti obostrano poravnat. Stranica ne bi trebala završiti naslovom
5.	Font i prored	Verdana, 12pt, jednostruki prored

Rd.br.	Naziv	Opis
6.	Naslov	Naslov ne bi trebao imati više od 15 riječi i trebao bi biti smješten u dva retka i centriran. Naslov rada (Verdana, 14 pt, bold), imena i prezimena autora, naziv Odjela, Sveučilišta, Adresa, Grad, Država (Verdana, 10pt)
7.	Sažetak	Sažetak može imati najviše 200 riječi i treba vjerno opisati temu rada. Potrebno je navesti svrhu i cilj rada, korištene metode, rezultate te doprinose rada. Ključne riječi moraju biti vezane uz naslov i sažetak rada. Za jezičnu i gramatičku ispravnost rada odgovoran je autor. Nakon završenog recenzentskog postupka od autora se mogu zatražiti određene ispravke ili dopune sažetka i/ili rada. Sažetak pisati na hrvatskom i engleskom jeziku(Verdana, 10pt).
8.	Ključne riječi.	abecedni popis ključnih riječi (do 6 ključnih riječi) (Verdana 10pt)
9.	Stil	Naslovi poglavlja i potpoglavlja (Verdana, 11 pt, Bold), trebaju biti poravnati lijevo i numerirani. Prije i nakon naslova odjeljaka postaviti jedan razmak 11pt. Naslovi tablica i slika (Verdana 11pt) trebaju biti uzastopno numerirani i centrirano poravnati.

11pt

2.4. Jednadžbe (Verdana, 11, Bold)

11pt

Jednadžbe trebaju biti poravnate uz lijevi rub teksta stupca i trebaju imati prazan redak prije i poslije.

11pt

$$P_{\mathrm{e}} = \frac{p_{\mathrm{e}} V_{\mathrm{h}} n i}{30} \qquad (1)$$

11pt

Jednadžbe je potrebno numerirati

11pt

3. Rezultati i rasprava (Verdana, 11, Bold)

11pt

U ovom odjeljku potrebno je detaljno predstaviti postignute rezultate vlastitih istraživanja, npr. istraživanja ili izračune, ilustrirajući ih detaljno i čitljivo slikama, dijagramima, fotografijama, rezultatima, izračunima, tablicama itd., te detaljno navodeći uzročno-posljedične odnose između navedenih činjenica, potvrđujući ili opovrgavajući podatke poznate iz literature. Ovaj odjeljak treba imati karakter znanstvene rasprave, iako se za to može izraditi zaseban odjeljak, a u ovom se mogu uključiti samo informacije o postignutim rezultatima istraživanja."

11pt

4. Zaključak (Verdana, 11, Bold)

11pt

Potrebno je predstaviti glavne zaključke i postignuća iz istraživanja. Treba naglasiti autorova postignuća i originalnost istraživanja te autorov doprinos u obrađenoj problematici i vrijednost studije. Mogu se istaknuti praktična primjena i mogući ishodi, kao i smjerovi daljnjih radova

11pt

5. Literatura (Verdana, 11, Bold)

11pt

Oblikovana sukladno standardima APA stila (APA 7th edition), npr.

11pt

Rad u časopisu:

Van Mol, C. (2016). Migration aspirations of European youth in times of crisis. Journal of Youth Studies 19(10), 1303-1320. https://doi.org/10.1080/13676261.2016.1166192

11pt

Knjiga:

Miljković, D. i Rijavec, M. (2002). Bolje biti vjetar nego list. IEP.

11pt

Urednička knjiga:

Panian, Ž. i Ćurko, K. (ur.) (2010). Poslovni informacijski sustavi. Element.

11pt

Poglavlje u uredničkoj knjizi:

Ciboci, L. i Labaš, D. (2015). Utjecaj medija na igru djece predškolske dobi. U D. Smajić, i V. Majdenić (Ur.), Dijete i jezik danas - dijete i mediji (str. 363-388). Sveučilište Josipa Jurja Strossmayera u Osijeku, Fakultet za odgojne i obrazovne znanosti.

11pt

Objavljena doktorska disertacija ili diplomski rad:

Ergović, Z. (2020). Odnos korištenja društvenih mreža i mentalnog zdravlja kod studenata u vrijeme pandemije koronavirusa [Diplomski rad, Sveučilište u Zagrebu]. Repozitorij Fakulteta hrvatskih studija. https://urn.nsk.hr/urn:nbn:hr:111:312140

11pt

Neobjavljena doktorska disertacija ili diplomski rad:

Bartolović, V. (2020). Radna snaga budućnosti – problemi i prilike studentske populacije [Neobjavljena doktorska disertacija]. Sveučilište Josipa Jurja Strossmayera u Osijeku, Ekonomski fakultet u Osijeku.

11pt

Drugo:

European Commission (2020). Youth employment support, https://ec.europa.eu/social/main.jsp?catId=1036&langId=en&fbclid=IwAR0MP77DM-tSs07vBiC6ROVlY8DPghrMdENwJd5ulIZjRA-4WrKq08gq_38

Državni zavod za statistiku (2020). Migracija stanovništva Republike Hrvatske u 2020.

Zakon o računovodstvu. Narodne novine 47/2020

11pt

Ostali primjeri dostupni su na https://apastyle.apa.org/style-grammar-guidelines/references/examples

14pt
14pt
PAPER TITLE (Verdana, 14pt, Bold)
14pt
14pt

Abstract: The title of the paper can have a maximum of 15 words. After the title, full names of the authors without titles should be listed. The abstract can have a maximum of 200 words and should faithfully describe the topic of the paper. The purpose and objective of the paper, methods used, results, and contributions of the work must be stated. Keywords must be related to the title and abstract of the paper. The author is responsible for the linguistic and grammatical correctness of the paper. After the peer-review process is completed, the authors may be asked to make certain corrections or additions to the abstract and/or the paper. (Verdana 10pt).
10pt
Keywords: Alphabetic list of keywords in British English (max. 6 keywords) (Verdana 10pt)

ERSTE Bank | Cyber Guardian

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Co-funded by the European Union

Festung

Časopis za interdisciplinarna istraživanja u poslovanju

Nakladnik: Sveučilište u Slavonskom Brodu