



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

Ivana Miklošević, Gabrijela Bosak, studentica
Sveučilište u Slavanskom 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.

Glavne 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.

H₀: Ne postoje statistički značajne razlike prema spolu ispitanika u stavovima o pitanjima vezanima uz umjetnu inteligenciju i kibernetičku sigurnost.

H₁: 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	s 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.

H_2 : 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 CYBERSECURITY: 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