Festung

Časopis za interdisciplinarna istraživanja u poslovanju

Godište 1, Broj 1/2025

Slavonski Brod, Srpanj, 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

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:

Copyright© 2025.

Prva godina izlaženja: 2025

Časopis izlazi četiri puta godišnje.

CYBER FESTUNG

SVEUČILIŠTE U SLAVONSKOM BRODU

Trg I. B. Mažuranić 2
35000 Slavonski Brod

tel: +385 35 446 188
https://festung.unisb.hr/

OIB: 3302783437
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://cf.unisb.hr/

SADRŽAJ

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 Cobović

Zaprimljen: 22.4.2025.
Odobren za objavu: 23.7.2025.
Izvorni znanstveni rad

PROVJERA ZNANJA O KIBERNETIČKOJ SIGURNOSTI U SREDNJIM ŠKOLAMA POMOĆU DIGITALNOG KVIZA

Ivana Lovrić Senjak[1], Mirko Cobović[2], Žaklina Bender[3], Anita Barišić[4]
[1] Sveučilište u Slavonskom Brodu, Trg I. B. Mažuranić 2, 35000 Slavonski Brod, Hrvatska,
ePošta: ilovricsenjak@unisb.hr
[2] Sveučilište u Slavonskom Brodu, Trg I. B. Mažuranić 2, 35000 Slavonski Brod, Hrvatska,
ePošta: mcobovic@unisb.hr
[3] Gimnazija Požega. Dr. Franje Tuđmana 4A, 34000 Požega, Hrvatska,
ePošta: tajnistvo@gimpoz.hr
[4] Gimnazija Matija Mesić, Naselje Slavonija I 8, 35000 Slavonski Brod, Hrvatska
ePošta: anitaorec2@gmail.com

Sažetak: Ovaj rad istražuje razinu znanja srednjoškolaca o osnovama kibernetičke sigurnosti putem digitalnog kviza. Cilj je bio identificirati područja dobre informiranosti i ona koja zahtijevaju dodatnu edukaciju. U istraživanju je korišten kvantitativni pristup temeljen na strukturiranom digitalnom kvizu, provedenom među 268 učenika iz triju gimnazija, a podaci su analizirani deskriptivnom i korelacijskom statistikom. Rezultati pokazuju visoku ukupnu točnost (87,69 %), s najboljim rezultatima u temama lozinki i digitalnog traga te najslabijima u prepoznavanju osobnih podataka, ransomwarea i 2FA. Nije utvrđena značajna povezanost između točnosti i vremena rješavanja ni između uređaja i uspješnosti. Rad ističe važnost strukturirane edukacije o kibernetičkoj sigurnosti.

Ključne riječi: digitalni kviz, kibernetička sigurnost, gimnazije, obrazovanje, statistička analiza

1. Uvod

Intenzivna izloženost upotrebi digitalnih tehnologija među mladima, zahtijeva pravovremeno obrazovanje o osnovama kibernetičke sigurnosti. Prema izvješću Europske komisije (2022), informatičko obrazovanje u europskim školama postaje ključna komponenta digitalne pismenosti i društvene odgovornosti.
Prema izvješću Europske agencije za kibernetičku sigurnost (ENISA, 2019), Europska unija suočava se s izraženim nedostatkom stručnjaka za kibernetičku sigurnost, što predstavlja izazov za tržište rada i za nacionalnu sigurnost. S naglaskom na visokom obrazovanju, preporuke uključuju ranu implementaciju tema kibernetičke sigurnosti u obrazovni sustav. Analiza školskih kurikuluma u ak.god. 2020/2021 pokazuje da u brojnim državama članicama informatički sadržaji koji obuhvaćaju kibernetičku sigurnost još uvijek nisu sustavno integrirani u sve razine obrazovanja što Navedeno upućuje na potrebu jačeg kurikularnog pristupa u području digitalne sigurnosti u srednjoškolskom uzrastu.

1.1. Prethodna istraživanja

U prethodnim istraživanjima naglašava se važnost uključivanja tema kibernetičke sigurnosti u obrazovni sustav. Jerman Blažič i Jerman Blažič (2022) ističu potrebu za interaktivnim oblicima poučavanja poput edukativnih igara, dok Adams i Makramalla (2015) upozoravaju na neučinkovitost tradicionalnih metoda u području digitalne sigurnosti. Witsenboer i sur. (2022) pokazuju da su nizozemski učenici bolje informirani o lozinkama i

privatnosti, ali slabije razumiju pojmove kao što su phishing i enkripcija. Navedena istraživanja potvrđuju potrebu za ovim radom, koji kroz digitalni kviz procjenjuje znanje hrvatskih srednjoškolaca i identificira područja za dodatnu edukaciju.

2. Metodologija

U ovom se radu ispituju tri ključna aspekta povezana s razinom znanja srednjoškolaca o kibernetičkoj sigurnosti. Primarno, utvrđuju se tematska područja u kojima učenici pokazuju najvišu razinu informiranosti, kao i ona koja zahtijevaju dodatnu edukaciju. Sekundarno, istražuje se postoji li povezanost između točnosti rješavanja kviza i vremena njegova ispunjavanja. Na kraju, analizira se moguće postojanje razlika u uspješnosti rješavanja kviza s obzirom na vrstu korištenog uređaja, konkretno između korisnika Android i iOS sustava.
U svrhu istraživanja razine znanja o kibernetičkoj sigurnosti među učenicima srednjih škola, provedeno je istraživanje kvantitativne metode temeljene na strukturiranom online kvizu. Alat za izradu i distribuciju kviza bio je Quizizz.

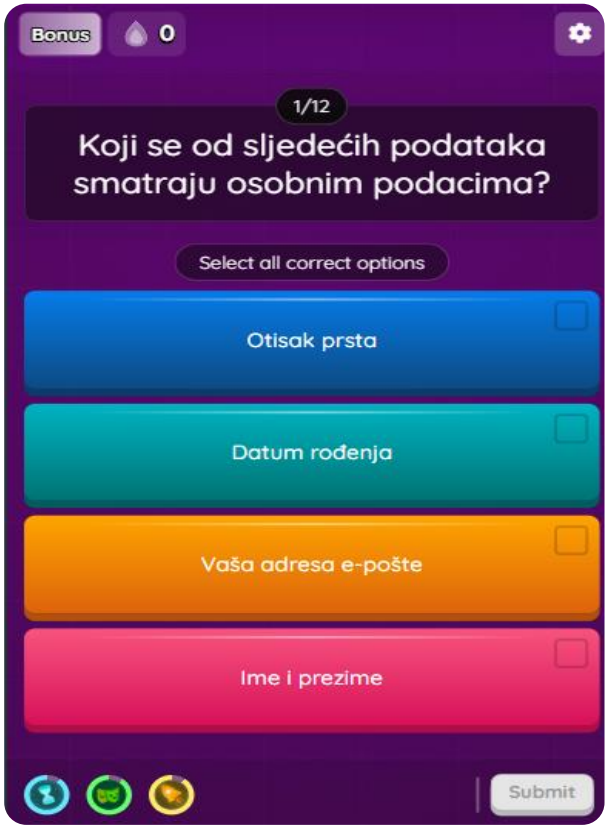
Slika 1: Poster sa QR kodom kviza

Digitalni poster sa QR kodom za pristup kvizu je distribuiran predavačima i suradnicima unutar srednjih škola na području Brodsko-posavske, Požeško-slavonske i Osječko-baranjske županije. Sudjelovanje je bilo anonimno i dobrovoljno. Suradnici škola angažirani u provođenju kviza su bili informirani o svrsi istraživanja i upućeni da savjetuju učenike o mjerama u svrhu anonimnosti. Podaci su prikupljeni u razdoblju 24.03.2025. – 12.04.20205.
Sudionici su bili učenici Gimnazije „Matija Mesić" Slavonski Brod, Gimnazije Požega i I. Gimnazije Osijek. Kvizove su provodili nastavnici i suradnici navedenih škola tijekom nastavnih sati informatike, etike i sata razrednika.
Kviz je sadržavao ukupno 12 pitanja s višestrukim izborom između točnih i netočnih odgovora, podijeljenih u tematske cjeline. Svako od 12 pitanja je sadržavalo četiri ponuđena odgovora, od kojih je za 11 pitanja bio točan samo jedan od ponuđenih odgovora dok su za 1 pitanje bila točna sva četiri ponuđena odgovora. Vrijeme za odgovor je bilo ograničeno na 60 sekundi po pitanju.
Rezultati kviza analizirani su metodama deskriptivne statistike. Za svako pitanje izračunata je učestalost točnih i netočnih odgovora, a ukupni rezultati grupirani su po tematskim područjima s ciljem utvrđivanja koje su teme učenicima najpoznatije, a koje zahtijevaju dodatnu edukaciju. Uz deskriptivne analize, provedene su i korelacijske analize pomoću Pearsonovog i Spearmanovog koeficijenta kako bi se ispitala povezanost između točnosti rješavanja kviza i vremena njegova ispunjavanja. Osim toga, primijenjen je Mann-Whitney U test radi ispitivanja razlika u rezultatima i vremenu rješavanja s obzirom na vrstu korištenog uređaja.

3. Rezultati i rasprava

Rezultati kviza prikazuju različite razine poznavanja temeljnih pojmova kibernetičke sigurnosti među učenicima srednjih škola. Kviz je riješilo 268 učenika sa ukupno zabilježeno 297

pristupa. Izuzeti su svi prazni i polovični zapisi kao i višestruki pokušaji rješavanja kviza zabilježeni na osnovi sesija.
Od ukupno 297 zapisa o pristupu kvizu, iz obrade je izuzeto ukupno 9,76% zapisa. S obzirom na svaku školu zasebno izuzeto je nominalno 9 od 95, tj. 9,47% zapisa iz Gimnazija „Matija Mesić" Slavonski Brod; zatim, nominalno 12 od 163, 7,36% iz Gimnazija Požega i nominalno 8 od 39, 20,51% iz I. Gimnazija Osijek. U obradu je ukupno uzeto 268 zapisa.
Rezultati ovog istraživanja se djelomično podudaraju sa prethodnim nalazima (Witsenboera, Sijtsme i Scheelea 2022), koji su utvrdili da nizozemski srednjoškolci pokazuju osnovno razumijevanje lozinki i privatnosti i slabije rezultate na temama poput phishinga i enkripcije. U našem slučaju, samo 57,84% ispitanih je uspješno prepoznalo sve navedene tipove osobnih podataka.
Ovakav rezultat se djelomično može pripisati činjenici kako je pitanje o prepoznavanju osobnih podataka, prvo od dvanest pitanja – ujedno bilo i jedino pitanje u kojemu su svi navedeni odgovori bili točni što je moguće navelo ispitanike da pretpostave da je barem jedan od navdenih odgovora netočan. Međutim, više od polovice ispitanika je pokazalo nepobitno znanje o raspoznavanju vrsta osobnih podataka.
Od četiri ponuđena odgovora, vidljiva na slici 2, najproblematičniji tip podataka za raspoznavanje je bila E-mail adresa koja je ostala neidentificirana kao osobni podatak u 67,26% od 113 netočnih odgovora na ovo pitanje, zatim otisak prsta u 56,64% odgovora, datum rođenja u 28,32% te ime i prezime u 27,43% netočnih odgovora.



Slika 2: Pitanje o osobnim podacima

Tablica 1. Uspješnost po tematskim cjelinama

Ukupno	Netočno	Točno	Točno %	Pitanja iz tematske cjeline
268	2	266	99,25%	Stvaranje sigurnih lozinki
268	5	263	98,13%	Razumijevanje digitalnog traga
268	7	261	97,39%	Postupanje sa sumnjivim e-mailovima
268	12	256	95,52%	Privatnost na društvenim mrežama
268	13	255	95,15%	Rizici ponovne upotrebe lozinki
268	17	251	93,66%	Važnost ažuriranja uređaja
268	18	250	93,28%	Digitalna higijena i sigurnosne navike
268	34	234	87,31%	Razumijevanje enkripcije
268	40	228	85,07%	Prepoznavanje phishing poruka
268	63	205	76,49%	Prepoznavanje ransomware prijetnji
268	72	196	73,13%	Razumijevanje dvofaktorske autentifikacije
268	113	155	57,84%	Prepoznavanje osobnih podataka

3.1. Ukupna uspješnost

Prosječna točnost rješavanja kviza iznosila je 87,69%, što ukazuje na zadovoljavajuću razinu znanja o osnovnim pojmovima teme digitalne sigurnosti. Najveća koncentracija točnih odgovora zabilježena je kod pitanja vezanih uz odabir najsigurnije forme lozinke i razumijevanje digitalnog traga, dok su najlošiji rezultati postignuti u temama koje se odnose na prepoznavanje vrsta osobnih podataka, dvofaktorsku autentifikaciju i poznavanje pojma ransomwarea.

U cilju dublje evaluacije odnosa između vremena potrebnog za rješavanje kviza i razine točnosti odgovora, provedena je korelacijska analiza. Izračunata su dva koeficijenta korelacije: Pearsonov koeficijent za ispitivanje linearne povezanosti te Spearmanov koeficijent za monotoni odnos između varijabli.

Rezultati analize pokazali su da je Pearsonova korelacija iznosila 0,012, dok je Spearmanova korelacija iznosila 0,015. Oba su koeficijenta vrlo blizu nuli, što upućuje na izostanak značajne linearne i monotone povezanosti između točnosti rješavanja kviza i ukupnog vremena potrebnog za njegovo ispunjavanje. Drugim riječima, brzina odgovaranja učenika nije bila presudan faktor za uspješnost.

Također je uzet u obzir i tip uređaja u odnosu na brzinu rješavanja te je korišten neparametrijski test (Mann-Whitney U) jer je tip uređaja kategorička varijabla. Utvrđeno da nema statistički značajne razlike u vremenu rješavanja između korisnika Android i iOS uređaja ($p > 0.05$) ondosno $p=0.951$.

Mann-Whitney U test je korišten i pri analizi korelacije točnosti i tipa uređaja. Rezultati analize po tipu uređaja ukazuju na blagu razliku u točnosti između korisnika Android i iOS uređaja. Kao što je prikazano u Tablici 2., sudionici koji su pristupili kvizu putem Android uređaja postigli su višu prosječnu točnost (83,84 %) i viši medijan točnosti (93 %), u usporedbi s korisnicima iOS uređaja, čija je prosječna točnost iznosila 79,94 %, a medijan 80 %. Raspon točnosti bio je širi kod iOS korisnika (33 % – 100 %) nego kod Android korisnika (47 % – 100 %), što ukazuje na veću varijabilnost rezultata unutar te skupine.

Kako bi se ispitala statistička značajnost ove razlike, proveden je Mann-Whitney U test, koji je prikladan za usporedbu dviju nezavisnih skupina kada se ne može pretpostaviti normalna distribucija. Rezultati testa pokazali su da razlika nije statistički značajna ($U=9820,5$; $p= 0,075$), iako se može uočiti trend u korist Android korisnika. Stoga se razlike u postotku točnih odgovora po tipu uređaja ne mogu tumačiti kao sustavne, ali rezultati mogu poslužiti kao polazište za buduća istraživanja o utjecaju korisničkog sučelja, veličine zaslona ili operacijskog sustava na izvedbu u digitalnim obrazovnim alatima.

Za buduća istraživanja preporučuje se detaljnija analiza potencijalnog utjecaja tehničkih čimbenika, poput veličine zaslona, responzivnosti sučelja i brzine prikaza kviza na različitim operacijskim sustavima, s ciljem boljeg razumijevanja kako tehnološki aspekti mogu oblikovati izvedbu učenika u digitalnim edukacijskim okruženjima.

Tablica 2. Rezultati analize točnosti po tipu uređaja

Tip uređaja	Broj sudionika	Prosječna točnost	Medijan točnosti	Raspon točnosti
Android	149	83,84 %	93 %	47 % – 100 %
iOS	119	79,94 %	80 %	33 % – 100 %

3.2. Obrasci razumijevanja

Rezultati ukazuju na to da forma pitanja s višestrukim točnim odgovorima može utjecati na uspješnost odgovaranja, što sugerira postojanje kognitivne pristranosti među učenicima. Naime, značajan broj učenika nije prepoznao sve osobne podatke, iako su svi ponuđeni odgovori bili točni. Takva pristranost, gdje učenici sumnjaju u mogućnost da su svi odgovori točni, može se povezati s iskustvom iz školskog konteksta gdje se rijetko koristi ta struktura pitanja. Buduće obrazovne strategije mogle bi uključivati eksplicitno upoznavanje učenika s različitim vrstama ispitnih formata kako bi se minimizirao utjecaj pretpostavki na točnost odgovora.

4. Zaključak

Doprinos rada očituje se u primjeni digitalnog kviza kao suvremenog alata za evaluaciju znanja o kibernetičkoj sigurnosti među srednjoškolcima u Hrvatskoj, što predstavlja empirijski utemeljenu osnovu za razvoj obrazovnih strategija u području digitalne sigurnosti. Istraživanje je pokazalo da srednjoškolci posjeduju zadovoljavajuću razinu znanja o osnovnim konceptima kibernetičke sigurnosti. Najbolje rezultate učenici su postigli u temama koje se odnose na stvaranje sigurnih lozinki i razumijevanje digitalnog traga, dok su slabiji rezultati zabilježeni kod pitanja prepoznavanja osobnih podataka, dvofaktorsku autentifikaciju i ransomware. Rezultati upućuju na potrebu za edukacijom u tehnički zahtjevnijim aspektima digitalne sigurnosti.
Analize su pokazale da ne postoji značajna povezanost između vremena rješavanja kviza i točnosti odgovora, kao ni između tipa uređaja i uspješnosti. Zapaženo je da su učenici iskazali nižu uspješnost na pitanju koje je sadržavalo višestruke točne odgovore, što može ukazivati na prisutnost kognitivne pristranosti uvjetovane iskustvom sa tradicionalnim evaluacijskim formama.

Dobiveni rezultati potvrđuju važnost ranog i strukturiranog uključivanja tema kibernetičke sigurnosti u srednjoškolski kurikulum, uz primjenu suvremenih i interaktivnih obrazovnih alata poput digitalnih kvizova. Nadalje, predložena su buduća istraživanja koja bi mogla ispitati utjecaj tehničkih čimbenika i različitih formata pitanja na učenikovu izvedbu, čime bi se doprinijelo oblikovanju učinkovitijih obrazovnih strategija u području digitalne sigurnosti.

5. Literatura

Adams, M., & Makramalla, M. (2017). Cybersecurity skills training: An attacker-centric gamified approach. Technology Innovation Management Review, 7(4), 12–18. https://timreview.ca/article/861

ENISA. (2020). Cybersecurity skills development in EU. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union

European Commission: European Education and Culture Executive Agency. (2022). Informatics education at school in Europe. Publications Office of the European Union. https://data.europa.eu/doi/10.2797/268406

Jerman Blažič, B., & Jerman Blažič, A. (2022). Cybersecurity skills among European high-school students: A new approach in the design of sustainable educational development in cybersecurity. Sustainability, 14(8), 4763. https://doi.org/10.3390/su14084763

Witsenboer, J. W. A., Sijtsma, K., & Scheele, F. (2022). Measuring cyber secure behavior of elementary and high school students in the Netherlands. Computers & Education, 186, 104536. https://doi.org/10.1016/j.compedu.2022.104536

ASSESSING CYBERSECURITY KNOWLEDGE AMONG HIGH SCHOOL STUDENTS USING A DIGITAL QUIZ

Abstract: This paper examines the level of cybersecurity knowledge among high school students using a digital quiz. The aim was to identify areas of strong awareness as well as those requiring additional education. A quantitative approach was employed, based on a structured digital quiz conducted among 268 students from three grammar schools, with data analyzed using descriptive and correlational statistics. The results indicate a high overall accuracy rate (87.69%), with the highest scores in topics related to password security and digital footprints, and the lowest in identifying personal data, ransomware, and two-factor authentication (2FA). No significant correlations were found between accuracy and completion time, nor between device type and performance. The study highlights the importance of structured cybersecurity education in secondary schools.

Keywords: Cybersecurity, Digital assessment, Educational measurement, Grammar schools, Statistical analysis

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

FISKALIZACIJA 2.0: PRAVNI OKVIR, DIGITALNA TRANSFORMACIJA I UČINCI NA MIKRO I MALE PODUZETNIKE U REPUBLICI HRVATSKOJ

Ivana Miklošević[1]
[1]Sveučilište u Slavonskom Brodu, Trg I. B. Mažuranić 2, 35000 Slavonski Brod, Hrvatska
ePošta: imiklosevic@unisb.hr

Sažetak: Rad analizira pravne, ekonomske i praktične učinke implementacije reforme Fiskalizacije 2.0 u Republici Hrvatskoj, s posebnim fokusom na mikro i male poduzetnike. Pravni okvir Fiskalizacije 2.0 definiran je prijedlogom novog Zakona o fiskalizaciji iz 2025. godine koji jasno propisuje obveze i rokove za poduzetnike, usklađujući nacionalno zakonodavstvo s europskim standardima, ali istovremeno stvara dodatne regulatorne izazove za mikro i male poduzetnike. Kvalitativna analiza provedena je putem metode polustrukturiranih intervjua na uzorku od 15 mikro i malih poduzetnika koji posluju u različitim sektorima. Cilj provedenog istraživanja je identificirati ključne izazove, troškove, koristi te institucionalnu potporu tijekom implementacije novog sustava fiskalizacije temeljenog na elektroničkim računima (eRačunima). Rezultati istraživanja su ukazali na glavne prepreke tijekom implementacije digitalne fiskalizacije kao što su tehnička složenost sustava, dodatni financijski troškovi te nedovoljna edukacija i informacijska podrška. Istodobno, mikro i mali poduzetnici ističu prednosti poput veće razine transparentnosti poslovanja, smanjenje administrativnog opterećenja, brže obrade računa i unaprjeđenja digitalne pismenosti. Unatoč početnim izazovima, dugoročni potencijal digitalne transformacije fiskalnog sustava je značajan, pod uvjetom da se osiguraju kvalitetna institucionalna podrška i pravovremena edukacija poduzetnika.

Ključne riječi: digitalna transformacija, eRačun, Fiskalizacija 2.0, kvalitativno istraživanje, mikro i mali poduzetnici, Republika Hrvatska

1. Uvod

Digitalna transformacija poslovanja u poduzećima posljednjih godina prepoznata je kao jedan od ključnih strateških prioriteta razvijenih gospodarstava svijeta. Fiskalizacija, kao dio poreznog nadzora nad svim poduzećima u zemlji predstavlja važan alat države za suzbijanje sive ekonomije, jačanje razine transparentnosti i osiguranje pravednijeg tržišnog natjecanja. Implementacijom reforme Fiskalizacija 2.0, Republika Hrvatska dodatno usklađuje svoj porezni okvir s digitalnim trendovima i zakonodavstvom Europske unije te odgovara na potrebe suvremenog tržišnog okruženja (European Commission, 2022). Zakon će se primjenjivati postupno, s ključnim rokovima u 2025., 2026. i 2027. godini. Prijedlog novog Zakona o fiskalizaciji iz 2025. godine donosi niz ključnih promjena koje obuhvaćaju sve segmente fiskalizacije: B2C, B2B i B2G, s naglaskom na obveznu implementaciju elektroničkih računa (eRačuna), integraciju digitalnog izvještavanja, korištenje digitalnih certifikata te implementaciju besplatne MIKROeRAČUN aplikacije (pod ingerencijom Porezne uprave Republike Hrvatske) namijenjenu poslovnim subjektima izvan sustava PDV-a (Porezna uprava, 2025). Sve navedeno predstavlja sustavni iskorak Republike Hrvatske prema digitalno utemeljenom poreznom nadzoru koji bi trebao donijeti

brojne koristi u pogledu veće fiskalne discipline, smanjenja administrativnog opterećenja poduzetnika i lakše obrade poslovnih podataka. Međutim, svaka regulatorna promjena, a osobito kada zahtijeva digitalnu prilagodbu, implicira i niz praktičnih izazova u provedbi. Mikro i mali poduzetnici najčešće raspolažu ograničenim resursima i nižom razinom digitalne spremnosti na regulatorne i tržišne promjene. Upravo radi navedenog, razumijevanje percepcija i iskustava mikro i malih poduzetnika od presudne je važnosti za ocjenu izvedivosti i održivost novih zakonskih mjera i propisa. Cilj ovog rada je analizirati ključne odredbe prijedloga Zakona o fiskalizaciji 2025, identificirati pravne i ekonomske aspekte reforme te istražiti izazove i očekivanja mikro i malih poduzetnika. Provedeno istraživanje temelji se na kvalitativnoj analizi 15 polustrukturiranih intervjua s mikro i malim poduzetnicima iz različitih sektora djelatnosti. Fiskalizacija 2.0 dio je šireg okvira digitalne tranzicije Vlade Republike Hrvatske. Razvoj besplatne aplikacije MIKROeRAČUN predstavlja pokušaj smanjenja digitalnog jaza između malih i velikih poduzetnika, ali i izazov u pogledu prilagodbe na promjene korisnika, odnosno mikro i malih poduzetnika koji do sada nisu koristili takve aplikacije.

1.1. Pravni okvir Fiskalizacije 2.0

Prijedlog Zakona o fiskalizaciji iz 2025. godine detaljno uređuje obvezu korištenja elektroničkih računa (eRačuna) u svim poslovnim segmentima (B2C, B2B, B2G), definira rokove postupne primjene te sankcije za nepoštivanje navedenih obveza. Cilj Zakona je usklađivanje nacionalnog zakonodavstva s europskim digitalnim standardima te unaprjeđenje transparentnosti poslovanja u Republici Hrvatskoj te poreznog nadzora. Međutim, novi regulatorni zahtjevi stvaraju dodatni regulatorni teret mikro i malim poduzetnicima zbog potrebe tehničke i administrativne prilagodbe, što ističe važnost pravovremene institucionalne podrške, jasnih uputa u primjeni i edukacije poduzetnika u procesu primjene novog zakonskog okvira. Prema prijedlogu Zakona o fiskalizaciji iz 2025. godine, predviđena je postupna primjena obveze korištenja elektroničkih računa (eRačuna) u poslovanju. Od 1. rujna 2025. godine omogućuje se testiranje sustava za razmjenu eRačuna, fiskalizaciju i eIzvještavanje za sve obveznike. Od 1. siječnja 2026. godine obveznici u sustavu PDV-a dužni su izdavati i zaprimati eRačune za sve tuzemne transakcije. Također, obveza zaprimanja eRačuna proširuje se na subjekte izvan sustava PDV-a, uključujući obrtnike, slobodna zanimanja i proračunske korisnike. Od 1. siječnja 2027. godine svi obveznici fiskalizacije, neovisno o PDV statusu, morat će izdavati i zaprimati eRačune za tuzemne transakcije. Svjetska banka (2022) podržava automatizaciju poreznih sustava. Direktiva 2014/55/EU nalaže da javne vlasti moraju primati i obrađivati eRačune koji su usklađeni s EU standardom. (European Union, 2014). Financijska agencija (2025) navodi kako od 1. siječnja 2026. godine razmjena eRačuna među poslovnim subjektima u Hrvatskoj postaje zakonski obvezna.

2. Metodologija

Istraživanje je provedeno kvalitativnim pristupom, metodom **polustrukturiranih intervjua.** Uzorak obuhvaća **15 mikro i malih poduzetnika** iz različitih sektora (trgovina, ugostiteljstvo, usluge, obrtništvo) s područja Republike Hrvatske, s naglaskom na raznolikost u veličini, djelatnosti i regionalnoj zastupljenosti. Intervjui su provedeni tijekom travnja i svibnja 2025. godine (5 intervjua provedeno je uživo, dok je 10 intervjua provedeno online). Sudionici su odabrani **namjernim uzorkovanjem** na temelju kriterija da su obveznici fiskalizacije, upoznati s postojećim modelom i uključeni u poslovne procese koje zahvaća novi zakonski okvir.

Kvalitativni podaci prikupljeni kroz polustrukturirane intervjue analizirani su metodom tematske analize. Ova metoda omogućava sustavno prepoznavanje, organizaciju i interpretaciju obrazaca (tematika) unutar kvalitativnog skupa podataka. Proces analize obuhvatio je šest osnovnih faza: upoznavanje s podacima, kodiranje, traženje tema, pregledavanje tema, definiranje i imenovanje tema te integracija tematskih nalaza.
Kako bi se osigurala transparentnost i pouzdanost analize, provedeno je dvostruko kodiranje na uzorku od tri intervjua, čime je verificirana konzistentnost u interpretaciji sadržaja. S obzirom na prirodu istraživanja i veličinu uzorka (N = 15), tematska analiza omogućila je dublji uvid u iskustva i percepcije mikro i malih poduzetnika glede implementacije Fiskalizacije 2.0, zadržavajući kontekstualnu složenost svakog pojedinačnog odgovora, što kvantitativne metode ne bi mogle obuhvatiti istom razinom.

2.1. Svrha i cilj provedenog istraživanja

Svrha provedenog istraživanja je produbiti razumijevanje percepcija, iskustava i očekivanja mikro i malih poduzetnika u Republici Hrvatskoj u vezi s implementacijom Zakona o fiskalizaciji iz 2025. godine, u kontekstu reforme Fiskalizacija 2.0. Istraživanje se usmjerava na identifikaciju izazova, koristi i institucionalnih prepreka u primjeni digitaliziranog modela fiskalizacije s posebnim naglaskom na obvezno korištenje eRačuna i aplikacije MIKROeRAČUN. Cilj istraživanja je omogućavanje uvida u stvarna iskustva mikro i malih poduzetnika u poslovnoj praksi te kreiranje zaključaka i preporuka za regulativna i operativna poboljšanja fiskalnog okvira.
Svrha provedenog istraživanja je empirijski utemeljen doprinos razumijevanju učinaka fiskalne digitalizacije na mikro i mala poduzeća koja predstavljaju okosnicu gospodarstva Republike Hrvatske.

2.2. Istraživačka pitanja

U skladu s ciljem rada, definirana su sljedeća istraživačka pitanja:
1. Kako mikro i mali poduzetnici percipiraju glavne izazove implementacije Zakona o fiskalizaciji iz 2025. godine?
2. Koje koristi i prednosti prepoznaju u digitalnom sustavu fiskalizacije (eRačun, MIKROeRAČUN)?
3. Koje su glavne prepreke s kojima se suočavaju u procesu prilagodbe novom sustavu, jesu li to organizacijske, tehničke, regulatorne ili financijske prepreke?
4. U kojoj mjeri mikro i mali poduzetnici smatraju da su institucije pružile dovoljnu potporu (informacijsku, edukativnu, tehničku) za provedbu zakonskih promjena?

2.3. Ograničenja provedenog istraživanja

Ključna ograničenja ovog istraživanja odnose se na veličinu uzorka koja ograničava mogućnost generalizacije rezultata, kontekstualnu specifičnost (primjena samo na mikro i male poduzetnike) i potencijalnu pristranost odgovora radi subjektivne percepcije iskustava ispitanika.

Unatoč tome, dobiveni nalazi provedenog istraživanja omogućuju vrijedan uvid u praktične izazove i mogućnosti provedbe digitalne reforme Fiskalizacije 2.0 iz perspektive ključnih gospodarskih aktera te predstavljaju podlogu za buduća komparativna istraživanja.

3. Rezultati i rasprava

Tablica 1 prikazuje strukturirani pregled svih 15 sudionika istraživanja prema tri osnovna kriterija: veličina poduzeća, sektor poslovanja te regija poslovanja. Istraživanje je provedeno na uzorku od 9 mikro i 6 malih poduzeća, sa vlasnicima

poduzeća, odnosno poduzetnicima. Mikro poduzeća su dominantna u uslužnim i obrtničkim djelatnostima, dok mala poduzeća obuhvaćaju nešto širi spektar sektora. Sudionici su odabrani s ciljem kako bi se u istraživanje uključile različite gospodarske grane, od tradicionalnih (građevina, poljoprivreda, trgovina), do suvremenih (IT, digitalni marketing, zdravstvene usluge). Na taj način se omogućuje šira generalizacija u pogledu različitih izazova implementacije Fiskalizacije 2.0 za poduzetnike.

Tablica 1. Strukturni pregled sudionika provedenog istraživanja

Poduzetnik	**Veličina poduzeća**	**Sektor poslovanja**	**Regija poslovanja**
P1	Mikro	Ugostiteljstvo	Središnja Hrvatska
P2	Malo	Maloprodaja	Istočna Hrvatska
P3	Mikro	Obrtnička proizvodnja	Središnja Hrvatska
P4	Mikro	IT usluge	Grad Zagreb
P5	Malo	Poljoprivreda	Sjeverna Hrvatska
P6	Mikro	Frizerske usluge	Južna Hrvatska
P7	Malo	Građevinarstvo	Zapadna Hrvatska
P8	Mikro	Prijevoz i logistika	Istočna Hrvatska
P9	Malo	Obiteljski hotel	Južna Hrvatska
P10	Mikro	Računovodstvene usluge	Grad Zagreb
P11	Mikro	Trgovina na malo	Središnja Hrvatska
P12	Malo	Proizvodnja	Sjeverna Hrvatska
P13	Mikro	Digitalni marketing	Grad Zagreb
P14	Malo	Zdravstvene usluge	Zapadna Hrvatska
P15	Mikro	Umjetničke djelatnosti	Istočna Hrvatska

Izvor: izrada autorice

Nadalje, u istraživanje su uključene sve glavne hrvatske regije, uključujući Zagreb, čime se ostvaruje reprezentativan uvid u raznolikost izazova i prednosti implementacije Fiskalizacije 2.0.

Tablica 2 prikazuje sažetke odgovora ispitanika (mikro i malih poduzetnika) o složenosti implementacije Fiskalizacije 2.0.

Tablica 2. Složenost implementacije Fiskalizacije 2.0

Poduzetnik	**Sažetak odgovora ispitanika**	**Kategorija**
P1	Potrebna dodatna obuka za korištenje	Potreba za edukacijom
P2	Aplikacija je tehnički zahtjevna	Tehnička složenost
P3	Implementacija zahtijeva puno vremena	Administrativno opterećenje
P4	Nismo imali problema	Neutralan stav
P5	Aplikacija je zbunjujuća	Tehnička složenost
P6	Potrebna je stručna osoba	Potreba za podrškom
P7	Nejasne upute Porezne uprave	Regulacijska nejasnoća
P8	Čini se kompliciran sustav	Tehnička složenost
P9	Nismo imali edukaciju niti podršku	Potreba za edukacijom
P10	Novi sistem je nepotrebno kompliciran	Tehnička složenost
P11	Još nismo krenuli s implementacijom	Odgođena primjena
P12	Složenost ovisi o veličini poduzeća	Veličina poduzeća
P13	Dodatni trošak knjigovođe	Financijski troškovi
P14	Nejasno je što se sve fiskalizira	Regulacijska nejasnoća
P15	Sve se svodi na edukaciju ljudi	Potreba za edukacijom

Izvor: izrada autorice

Kvalitativnom analizom izdvojeno je pet tematskih potkategorija: tehnička složenost, potreba za edukacijom, regulacijska nejasnoća, administrativno opterećenje te veličina poduzeća. Najčešće spominjana kategorija od strane ispitanika bila je tehnička složenost sustava, koja je zabilježena kod četiri ispitanika, dok je potreba za dodatnom edukacijom navedena kod tri ispitanika. Veći broj odgovora implicira da mikro i mali poduzetnici percipiraju fiskalizaciju kao izazov, ponajviše u tehničkom i informacijskom smislu. Ovakav prikaz omogućava transparentan uvid u različite obrasce percepcije ispitanika, pri čemu se kvantitativni aspekt temelji na broju učestalosti izjava ispitanika.

Tablica 3 jasno kategorizira financijske implikacije vezane uz implementaciju novog sustava Fiskalizacije 2.0, temeljene na odgovorima 15 mikro i malih poduzetnika.

Tablica 3. Troškovne prepreke implementacije Fiskalizacije 2.0

Poduzetnik	**Sažetak odgovora ispitanika**	**Kategorija**
P1	Dodatni troškovi radi kupnje softvera	Tehnički troškovi
P2	Morali smo angažirati knjigovođu	Veći računovodstveni troškovi
P3	Plaćanje stručnih savjeta	Stručni troškovi
P4	Veći trošak kroz nadogradnju sustava	Tehnički troškovi
P5	Bilo je troškova koje nismo predvidjeli	Nepredviđeni troškovi
P6	Kupnja softvera je dodatan trošak	Tehnički troškovi
P7	Angažiranje stručne pomoći	Stručni troškovi
P8	U početku viši tehnički troškovi	Tehnički troškovi
P9	Implementacija traži ulaganje	Tehnički troškovi
P10	Novi zakon iziskuje dodatne troškove	Tehnički troškovi
P11	Trošak zamjene aplikacije	Tehnički troškovi
P12	Povećani troškovi radi eRačuna	Tehnički troškovi
P13	Kupnja dodatnih licenci	Tehnički troškovi
P14	Podcijenili smo financijski trošak	Pogrešna procjena troškova
P15	Troškovi implementacija sustava	Tehnički troškovi

Izvor: izrada autorice

Dominantno je prisutna kategorija **tehničkih troškova,** što ukazuje na to da su ispitanici najveće financijsko opterećenje vidjeli u troškovima softvera, nadogradnji sustava i licenci. Ovaj rezultat ukazuje na tehničku dimenziju kao ključni financijski izazov implementacije eRačuna i fiskalizacije u mikro i malim poduzećima. U manjoj mjeri, ali i dalje značajno, javljaju se **stručni troškovi,** poput angažmana vanjskih stručnjaka i savjetnika, što naglašava da je poduzećima potrebna dodatna specijalistička podrška i savjetovanje prilikom implementacije Fiskalizacije 2.0. Manji broj mikro i malih poduzetnika navodi kategorije nepredviđenih troškova, većih računovodstvenih troškova i pogrešne procjene troškova.

Tablica 4 prikazuje pregled stavova mikro i malih poduzetnika o potencijalnim prednostima koje očekuju od implementacije sustava digitalne fiskalizacije temeljenog na eRačunu.

Tablica 4. Očekivani pozitivni učinci digitalne fiskalizacije eRačuna

Poduzetnik	**Veća razina transparentnosti poslovanja**	**Smanjenje administrativnog opterećenja**	**Brža obrada računa**	**Usklađenost s EU standardima**	**Povećanje razine digitalne pismenosti**
P1	✔	✔	✔	✔	✔
P2	✔	✔	✔		✔
P3	✔	✔		✔	✔
P4	✔	✔	✔	✔	✔
P5	✔		✔	✔	✔
P6	✔	✔			
P7	✔	✔	✔	✔	✔
P8		✔		✔	✔
P9	✔	✔	✔		
P10	✔	✔		✔	✔
P11	✔			✔	
P12	✔	✔	✔	✔	✔
P13	✔	✔	✔	✔	✔
P14	✔	✔	✔		✔
P15	✔	✔	✔	✔	✔

Izvor: izrada autorice

Najviše ispitanika (14 od 15) smatra da će nova fiskalizacija pridonijeti **većoj razini transparentnosti poslovanja**, što je u skladu s ciljevima fiskalne politike i borbe protiv sive ekonomije. **Smanjenje administrativnog opterećenja** navedeno je u 13 odgovora, posebno od strane mikro i malih poduzetnika koji upravljanje dokumentacijom često obavljaju samostalno ili uz minimalnu podršku. **Bržu obradu računa** očekuje 10 ispitanika, dok **usklađenost s europskim standardima** prepoznaje 11 ispitanika kao važan dugoročni pozitivni učinak koji pridonosi stabilnosti i međunarodnoj vjerodostojnosti. **Povećanje digitalne pismenosti zaposlenika i vlasnika** spomenuto je od 12 poduzetnika, što potvrđuje da se fiskalizacija doživljava i kao poticaj za opću digitalnu edukaciju i modernizaciju poslovanja. Provedena analiza pokazuje optimizam među poduzetnicima glede dugoročnih koristi fiskalizacije, unatoč početnim izazovima i tehničkim troškovima, što upućuje na važnost institucionalne podrške u prijelaznom razdoblju kako bi se maksimizirao pozitivan učinak reforme Fiskalizacija 2.0.

4. Zaključak i preporuke

Implementacija Fiskalizacije 2.0 prema stavovima mikro i malih poduzetnika u Republici Hrvatskoj kreira dugoročne koristi u poduzećima, poput veće razine transparentnosti poslovanja, smanjenog administrativnog opterećenja i unaprjeđene digitalne pismenosti. Međutim, istraživanje je pokazalo značajne izazove, uključujući tehničku složenost, dodatne financijske troškove, nedovoljnu edukacijsku podršku mikro i malim poduzetnicima te činjenicu da dio ispitanika ne prepoznaje bržu obradu računa kao jasan pozitivni učinak. Ključ uspješne prilagodbe je kvalitetna institucionalna podrška i sustavna edukacija mikro i malih poduzetnika tijekom prijelaznog razdoblja. Preporuke za buduća istraživanja su provođenje kvantitativnog istraživanja na većem uzorku radi generalizacije rezultata istraživanja, usporedba iskustava mikro i malih poduzetnika s iskustvima velikih poduzetnika te dugoročno praćenje

učinaka digitalne fiskalizacije na poslovne performanse.

5. Literatura

European Commission. (2022). *Digital Public Administration factsheet 2022.* https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/DPA_Factsheets_2022_EU_vFinal.pdf

European Union. (2014). *Directive 2014/55/EU on electronic invoicing in public procurement.* https://eur-lex.europa.eu/eli/dir/2014/55/oj

Financijska agencija (2025). Obvezni eRačuni od 2026. https://www.fina.hr/novosti/obvezni-e-racuni-od-2026.-fina-ima-rjesenje-u-paketu

Porezna uprava. (2025). Projekt fiskalizacija 2.0 / eRačun. https://porezna.gov.hr/fiskalizacija/bezgotovinski-racuni/bezgotovinski-racuni-novosti/o/vlada-rh-usvojila-prijedlog-zakona-o-fiskalizaciji

World Bank. (2022). Digital Transformation of Tax and Customs Administrations. Washington, DC: World Bank. https://documents1.worldbank.org/curated/en/099448206302236597/pdf/IDU0e1ffd10c0c208047a30926c08259ec3064e4.pd

FISCALIZATION 2.0: LEGAL FRAMEWORK, DIGITAL TRANSFORMATION AND IMPACT ON MICRO AND SMALL ENTREPRENEURS IN THE REPUBLIC OF CROATIA

Abstract: This paper analyzes the legal, economic, and practical effects of implementing the Fiscalization 2.0 reform in the Republic of Croatia, with a particular focus on micro and small enterprises. The legal framework of Fiscalization 2.0 is defined by the 2025 Draft Fiscalization Act, which clearly outlines the obligations and deadlines for entrepreneurs, aligning national legislation with European digital standards. However, it simultaneously imposes additional regulatory burdens on smaller businesses. A qualitative analysis was conducted using semi-structured interviews with 15 micro and small entrepreneurs operating across various sectors. The primary aim of the research was to identify key implementation challenges, incurred costs, perceived benefits, and the availability of institutional support during the transition to the new digital fiscal system based on electronic invoicing (eInvoices). The findings indicate that the main barriers include the technical complexity of the system, additional financial costs, and insufficient education and informational support. At the same time, entrepreneurs recognize benefits such as increased business transparency, reduced administrative burden, faster invoice processing, and enhanced digital literacy. Despite initial challenges, the long-term potential of digital transformation in the fiscal system is significant—provided that adequate institutional support and timely education are ensured for entrepreneurs.

Keywords: digital transformation, eInvoice, Fiscalization 2.0, micro and small enterprises, qualitative research, Republic of Croatia

Zaprimljen: 29.5.2025.
Odobren za objavu: 23.7.2025.
Izvorni znanstveni rad

EMPIRIJSKA STUDIJA POSTUPAKA STROJNOG UČENJA ZA PREPOZNAVANJE MALICIOZNIH NAPADA

Antonio Carević[1], Mario Dudjak[2]
[1] Sveučilište Josipa Jurja Strossmayera u Osijeku, Fakultet Elektrotehnike, računarstva i informacijskih tehnologija Osijek, Kneza Trpimira 2B, 31000 Osijek, Hrvatska
ePošta: acarevic@etfos.hr
[1] Sveučilište Josipa Jurja Strossmayera u Osijeku, Fakultet Elektrotehnike, računarstva i informacijskih tehnologija Osijek, Kneza Trpimira 2B, 31000 Osijek, Hrvatska
ePošta: mdudjak@etfos.hr

Sažetak: Cilj rada je definirati tok učenja algoritama klasifikacije iz skupova podataka koji opisuju različite vrste malicioznih napada i odrediti pojedinačne procedure unutar tog toka. Primjenom definiranog toka dobiveni su rezultati koji pokazuju visoku kvalitetu klasifikacijskih modela u prepoznavanju malicioznih napada, što potvrđuje njegovu primjenjivost u području kibernetičke sigurnosti, posebno u sustavima za detekciju upada. Korišteni algoritmi strojnog učenja su: naivni Bayesov algoritam, k-najbližih susjeda, stablo odluke, nasumična šuma i logistička regresija. Tijekom odabira značajki korišteni su filtri s Pearsonovim koeficijentom korelacije, zajedničkom informacijom i ANOVA F-vrijednosti te omotač slijedna pretraga unaprijed. Za obradu neuravnoteženih skupova podataka primijenjeni su postupci nasumičnog preuzorkovanja i poduzorkovanja. Najbolje rezultate postigao je algoritam stablo odluke s F1 mjerom od 1.0 na većini skupova podataka, dok je naivni Bayesov algoritam imao znatno slabije performanse, s F1 vrijednostima u rasponu od 0.12 do 0.98. Tehnike odabira značajki uglavnom su poboljšale performanse, pri čemu se posebno istaknuo omotač. Među postupcima za smanjenje neuravnoteženosti podataka, nasumično preuzorkovanje dosljedno je poboljšalo performanse svih algoritama, dok je poduzorkovanje dovelo do značajnog smanjenja performansi kod pojedinih algoritama, uz pad F1 mjere i do 0.22. Predloženi tok učenja omogućuje sustavno vrednovanje utjecaja različitih metoda predobrade podataka i algoritama klasifikacije, čime doprinosi boljem razumijevanju procesa detekcije malicioznih napada u neuravnoteženim i heterogenim podatkovnim skupovima te može poslužiti kao temelj za razvoj učinkovitijih sustava kibernetičke obrane u stvarnim okruženjima.

Ključne riječi: klasifikacija, maliciozni napadi, neuravnoteženi skup podataka, odabir značajki, strojno učenje

1. Uvod

Brz razvoj Interneta omogućio je jednostavan pristup velikoj količini informacija, što ih istovremeno čini izloženima brojnim sigurnosnim prijetnjama. Jedna od glavnih prijetnji su maliciozni napadi, koji se definiraju kao programi čija je svrha probijanje obrambenih sustava računala te ugrožavanje povjerljivosti, integriteta i dostupnosti podataka (Sharp, 2017). Postoji mnogo načina na koje se maliciozni napadi mogu izvesti, a neki od najčešćih medija uključuju zaražene elektroničke poruke te kompromitirane internetske stranice (Ahsan i sur., 2022). Iako su vrste malicioznih napada brojne, ovaj se rad fokusira na neke od najpoznatijih i najčešćih, uključujući: viruse, crve, reklamne programe, ucjenjivačke programe, neželjenu poštu (engl. *spam*), trojanske konje, špijunske programe, napade distribuiranim

uskraćivanjem usluga (engl. *Distributed Denial of Service*, DDOS) te ubrizgavanje zlonamjernih URL-ova. Tradicionalni sustavi obrane ne mogu pratiti sve brži razvoj i sve veću složenost ovih prijetnji. Nedostatak informacija o novim vrstama napada dodatno ograničava učinkovitost klasičnih pristupa. Kao moguće rješenje nameće se primjena strojnog učenja. Strojno učenje bavi se razvojem računalnih algoritama koji na temelju empirijskih podataka izgrađuju modele sposobne za prepoznavanje obrazaca i zaključivanje (Tsiakos i Chalkias, 2023). Zbog te sposobnosti, takvi su modeli osobito prikladni za prepoznavanje različitih vrsta malicioznih napada, uključujući i novonastale napade o kojima postoje ograničeni podaci. Na temelju znanja stečenog iz postojećih primjera napada, modeli mogu naučiti prepoznavati i nove prijetnje. Nadzirano strojno učenje predstavlja oblik strojnog učenja koji se pokazao najprikladnijim za detekciju malicioznih aktivnosti. Kod ovog pristupa algoritmi uče iz unaprijed označenih podataka, pri čemu je poznat ishod za svaki skup ulaznih podataka (Shaukat i sur., 2020). Poseban oblik nadziranog strojnog učenja koji se široko primjenjuje u detekciji napada je klasifikacija.

Većina dosadašnjih radova na ovu temu fokusira se na jedan specifičan problem i prikazuje ostvarene rezultate, no često nedostaje opsežna eksperimentalna analiza koja bi omogućila dublji uvid u prednosti i nedostatke pojedinih algoritama. Rijetko se pritom navodi koji je algoritam učinkovitiji za određene vrste napada, a tek neznatan broj radova obrađuje problem neuravnoteženosti skupova podataka. Taj je problem prisutan u gotovo svim dostupnim skupovima koji opisuju maliciozne aktivnosti, a njegovo rješavanje omogućuje preciznije rezultate i bolji uvid u stvarne performanse klasifikacijskih algoritama.

Cilj ovog rada je definirati prikladan tok učenja algoritama klasifikacije iz skupova podataka koji opisuju različite oblike malicioznih napada te odrediti odgovarajuće postupke unutar tog toka. Odabirom specifičnih algoritama strojnog učenja izgradit će se modeli za detekciju malicioznih aktivnosti. Nadalje, primjenom tehnika predobrade u svrhu odabira značajki pokušat će se poboljšati performanse modela te prikazati utjecaj odabira značajki, aspekt koji je u postojećim radovima često zanemaren. Također, primjenom metoda uzorkovanja nastojat će se ublažiti neželjeni učinak problema neuravnoteženosti klasa.

Struktura rada organizirana je na sljedeći način. U drugom poglavlju prikazan je pregled relevantne literature te su objašnjeni najznačajniji oblici malicioznih napada i postojeći pristupi njihovom prepoznavanju. Treće poglavlje donosi opis eksperimentalnih postavki i korištene metodologije. U četvrtom poglavlju izneseni su rezultati analize te njihova interpretacija. Konačno, peto poglavlje sadrži zaključke rada i prijedloge za buduća istraživanja.

2. Pregled literature

Zahvaljujući sposobnosti prepoznavanja i prilagodbe novim vrstama napada, strojno učenje sve češće se primjenjuje u obrambenim kibernetičkim sustavima. U radu (Martínez Torres i sur., 2019) analizirani su najčešći oblici malicioznih napada, uključujući spam, mrežnu krađu identiteta (engl. *phishing*) i zlonamjerne programe. Kao najučinkovitiji algoritmi istaknuti su naivni Bayesov algoritam, stroj potpornih vektora, stabla odluke, k-najbližih susjeda, neuronske mreže i nasumične šume. Međutim, navedeno istraživanje ne uzima u obzir problem neuravnoteženih podataka, što predstavlja značajno ograničenje. U radu (D'hooge i sur., 2019) fokus je stavljen na DDoS napade, pri čemu su algoritmi temeljeni na stablima odluke postigli najbolje rezultate, dok je algoritam k-najbližih susjeda identificiran kao alternativno rješenje. Za razliku od ovog rada, naše istraživanje obuhvaća širi spektar napada i omogućuje usporedbu učinkovitosti različitih algoritama.

Primjena neuronskih mreža za upravljanje sigurnosnim uređajima istražena je u radu (Fraley i Cannady, 2017), gdje su postignuti obećavajući rezultati. S druge strane, rad (Ahsan i sur., 2022) prikazuje pregled različitih tehnika u području kibernetičke sigurnosti, ističući kao učinkovite algoritme naivni Bayes, logističku regresiju i stabla odluke. Ipak, ni u jednom od ta dva rada nije provedena detaljna evaluacija performansi niti usporedba većeg broja algoritama. Rad (Shaukat i sur., 2020) opisuje napredne tehnike strojnog učenja za unaprjeđenje kibernetičke sigurnosti, pri čemu su istaknuti algoritmi stabla odluke, nasumične šume, k-najbližih susjeda, neuronske mreže i naivni Bayes. Međutim, nedostatak ovog rada ogleda se u nedovoljnoj analizi procesa učenja iz podataka te neobrazloženom odabiru algoritama i tehnika predobrade. Zajednički nedostatak svih navedenih istraživanja jest ograničeno razmatranje utjecaja tehnika odabira značajki. U radu (Walling i Lodh, 2024) autori analiziraju jednu tehniku odabira značajki i njen utjecaj na prepoznavanje malicioznih napada, pri čemu je korišten algoritam nasumične šume. Međutim, rad ne uključuje usporedbu s drugim tehnikama koje bi potencijalno mogle dati bolje rezultate. Slično tome, rad (Kocher i Kumar, 2021) prikazuje utjecaj odabira značajki na algoritme k-najbližih susjeda, nasumične šume, logističke regresije i naivnog Bayesa, ali ne provodi međusobnu usporedbu korištenih tehnika predobrade, čime izostaje jasna procjena njihove učinkovitosti. Za razliku od navedenih radova, istraživanje (Yin i sur., 2023) obuhvaća prepoznavanje šireg spektra malicioznih napada korištenjem algoritama logističke regresije, stroja potpornih vektora, stabla odluke i nasumične šume. Autori su fokus stavili na smanjenje lažno pozitivnih rezultata i poboljšanje ukupnih performansi, ali bez primjene tehnika odabira značajki, što ograničava optimizaciju modela. U radu (Yin i sur., 2023) problem prepoznavanja malicioznih napada adresiran je korištenjem dubokih neuronskih mreža i nasumičnih šuma. Nedostatak ovog istraživanja jest korištenje samo jednog skupa podataka, čime je ograničena generalizacija modela na različite vrste napada. Rad (Sarhan i sur., 2021) prikazuje utjecaj tehnika predobrade na algoritme nasumične šume i dubokih neuronskih mreža. Iako su postignuti relevantni rezultati, rad ne definira cjelovit proces učenja koji uključuje sve faze primjene algoritama na različitim vrstama malicioznih napada, što predstavlja ključnu razliku u odnosu na ovu studiju.

Tablica 1. Skupovi podataka korišteni za potrebe eksperimentalne analize

Naziv	**Vrsta napada**	**Broj instanci**	**Broj značajki**	**Broj klasa**	**Stupanj neuravnoteženosti**
DARPA	DoS	4 554 344	4	2	1.51
KDD99	DoS, ubrizgavanje URL-a, mrežna krađa identiteta i drugi	494 020	42	23	3530.99
NSL-KDD	DoS, ubrizgavanje URL-a, mrežna krađa identiteta i drugi	148 517	42	40	37.27
KYOTO	DDoS	303 849	24	3	50644.17
Malware	Virus, crv, trojanski konj	100 000	35	2	1
DREBIN	Različiti maliciozni napadi operacijskog sustava Android	15 036	215	2	1.70

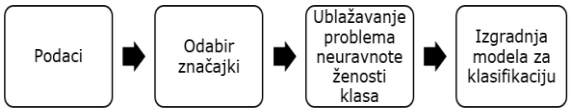
ISCXIDS2012	DoS, ubrizgavanje URL-a, mrežna krađa identiteta i drugi	171380	21	2	44.39
CICIDS2017	DDoS	225 745	79	2	1.31
DS2OS	Ucjenjivački, reklamni i špijunski programi	357 952	13	8	225.23
IMPACT	DoS, mrežna krađa identiteta i drugi	19 940	9	20	11.44
UNSW-NB15	DDoS, ubrizgavanje URL-a, mrežna krađa identiteta i drugi	257 673	45	2	1.77
CIC-DDOS2019	DDoS	300 000	88	19	787.62

3. Postavke i metodologija eksperimentalne analize

U radu je korišteno pet klasifikacijskih algoritama strojnog učenja. Odabrani algoritmi su: k-najbližih susjeda, stablo odluke, nasumična šuma, logistička regresija i naivni Bayesov algoritam (Kotsiantis i sur., 2007). Ovi algoritmi su odabrani kao prevladavajući u dostupnoj literaturi jer su često korišteni u svrhe treniranja modela strojnog učenja te sadrže razne vrste malicioznih napada. Dvanaest skupova podataka korišteno je za vrednovanje odabranih algoritama, a informacije o svakom skupu vidljive su u tablici 1. Skupovi podataka preuzeti su s javno dostupnih repozitorija UCI (Aha, 1987) i Kaggle (Goldbloom i Kaggle, 2010) te s internetskih stranica Instituta za kibernetičku sigurnost Sveučilišta u New Brunswicku (https://www.unb.ca/cic/datasets/ids.html) i grupe za istraživanje inteligentne sigurnosti Sveučilišta UNSW Sydney (https://research.unsw.edu.au/projects/unsw-nb15-dataset).

Svaki skup podataka podijeljen je u omjeru 80:20% na skup za treniranje i skup za testiranje. Za svaki hiperparametar klasifikatora definirane su različite vrijednosti čije su se kombinacije vrednovale pretraživanjem po mreži na podskupu za treniranje kako bi se pronašla optimalna. Nedostajuće vrijednosti su izbrisane, a kategoričke i ordinalne značajke kodirane su pomoću tehnike kodiranja oznaka te su normalizirane u raspon [0,1]. Kako bi se smanjio veliki broj redundantnih i nepotrebnih značajki, upotrijebljene su procedure odabira značajki. Metode koje su korištene u ovu svrhu su: filtri s Pearsonovim koeficijentom korelacije, zajedničkom informacijom i ANOVA F-vrijednosti te SFS omotač (Venkatesh i Anuradha, 2019). Prilikom upotrebe SFS omotača skup za treniranje dodatno je podijeljen na skup za treniranje i skup za validaciju u omjeru 65:35%. Nadalje, za ublažavanje problema neuravnoteženosti klasa primijenjene su metode nasumičnog preuzorkovanja i nasumičnog poduzorkovanja (Dudjak, 2022).

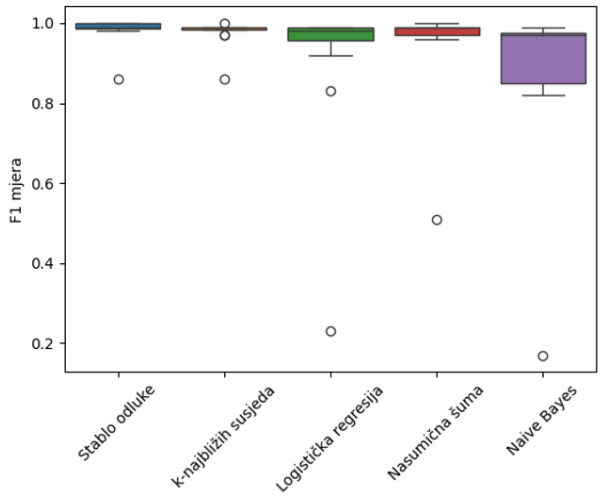
Računalo na kojem je proveden eksperiment opremljeno je sa Ryzen 5 5600 procesorom koji radi na 3.50 GHz, 16 GB RAM-a, AMD Radeon RX 6700 XT grafičku karticu sa 12 GB VRAM memorije te 1 TB SSD memorije. Cjelokupni eksperiment je ponovljen deset puta pri čemu su skupovi podataka različito podijeljeni s ciljem ublažavanja utjecaja stohastičnosti korištenih algoritama na dobivene rezultate. Veličine koje se koriste za evaluaciju dobivenih modela su: točnost, F1 mjera, stopa stvarno pozitivan rezultat (engl. *True Positive Rate*, TPR) i stopa stvarno negativan rezultat (engl. *True Negative Rate*, TNR). Konačne vrijednosti za svaku mjeru dobivene su kao prosječna vrijednost svih vrijednosti iz deset iteracija. Tok eksperimenta prikazan je na slici 1.



Slika 1. Koraci učenja iz skupova podataka koji opisuju maliciozne napade

4. Rezultati i rasprava

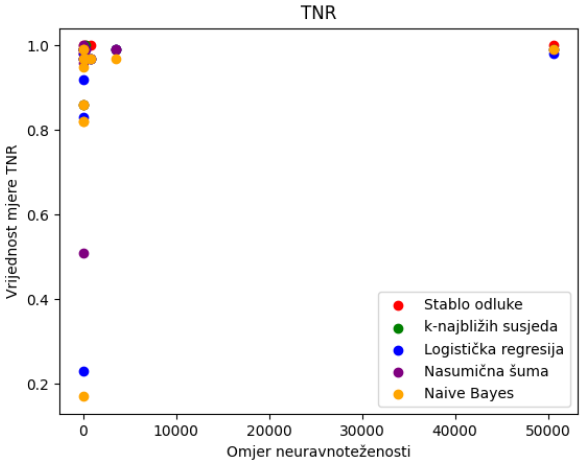
Dijagram pravokutnika (engl. *box plot*) na slici 2. sažeto prikazuje ostvarene vrijednosti F1 mjere na korištenim skupovima podataka. Vrijednosti F1 mjere algoritama stablo odluke, k-najbližih susjeda, nasumična šuma i logistička regresija usko su grupirane oko vrijednosti 1.0. To je pokazatelj kako svi ovi algoritmi ostvaruju visoke performanse za sve skupove podataka. Među njima se može izdvojiti algoritam stablo odluke zbog kontinuirano postignute vrijednosti 1.0 za F1 mjeru. Ostala tri algoritma povremeno ostvaruju lošije performanse na što ukazuje postojanje stršećih vrijednosti. Performanse naivnog Bayesovog algoritma primjetno su slabije kod gotovo svih skupova podataka. To je vidljivo na slici 2, gdje su vrijednosti F1 mjere naivnog Bayesovog algoritma u rasponu [0.80, 0.98] dok su rasponi ostalih algoritama znatno manji i bliže vrijednosti 1.0.



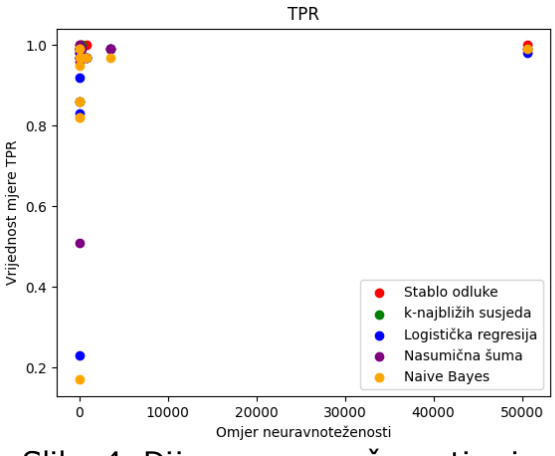
Slika 2. Dijagram pravokutnika vrijednosti F1 mjere

Manje vrijednosti točnosti na pojedinim skupovima podataka također upućuju na slabije performanse ovog algoritma. Na skupu NSL-KDD točnost naivnog Bayesovog algoritma iznosi 0.83, na skupu DREBIN 0.82, dok ostali algoritmi ostvaruju vrijednosti u rasponu [0.97, 0.99].

Zbog neuravnoteženosti podataka, model bolje klasificira većinsku klasu, postižući veće vrijednosti točnosti i TNR, dok se manjinska klasa slabije prepoznaje, što smanjuje F1 i TPR, što je prikazano na slikama 3 i 4. Ovaj trend je posebice vidljiv za algoritam naivnog Bayesa. Na NSL-KDD skupu podatak TNR za ovaj algoritam iznosi 0.93, dok mjere F1 i TPR imaju vrijednosti 0.82 i 0.83.



Slika 3. Dijagram raspršenosti mjere TNR i omjera neuravnoteženosti

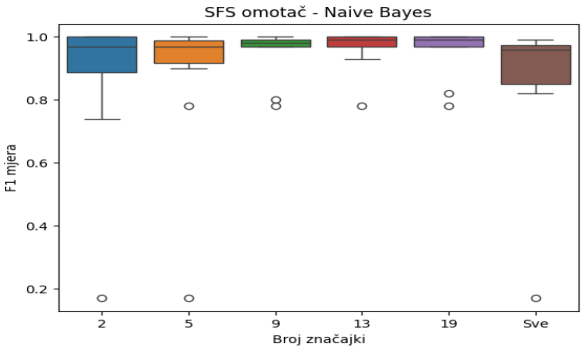


Slika 4. Dijagram raspršenosti mjere TPR i omjera neuravnoteženosti

4.1. Analiza učinka odabira značajki

Tehnike odabira značajki korištene su za poboljšanje performansi modela uklanjanjem irelevantnih značajki. Filtri

zasnovani na Pearsonovoj korelaciji, zajedničkoj informaciji i ANOVA F vrijednosti uglavnom su smanjili broj značajki, ali nisu znatno poboljšale performanse; posebice je Pearsonov filter loše radio na DREBIN skupu zbog velikog broja značajki. Vrijednosti F1 mjere svih algoritama su u padu, a najveći pad primjetan je kod logističke regresije. F1 mjera tog algoritma iznosi 0.90 nakon primjene filtera. Filter zasnovan na zajedničkoj informaciji poboljšao je performanse algoritma k-najbližih susjeda za 0.01, dok ANOVA filter nije imao značajan doprinos. S druge strane, omotač SFS značajno je poboljšao performanse svih algoritama, a posebice naivni Bayesov algoritam koji je postigao prihvatljive rezultate čak i na skupovima gdje je prije imao slabije rezultate. Detaljne performanse SFS metode za naivni Bayesov algoritam prikazane su na slici 5, dok su rezultati za sve algoritme i skupove podataka dostupni u tablici 2. Na dnu tablice izvedeni su rangovi Friedmanova testa za višestruku usporedbu (Derrac i sur., 2011), gdje manje vrijednosti sugeriraju bolju izvedbu uspoređenih algoritama. Dodatno, *post-hoc* statističke procedure ovog testa (poput primjerice, Nemenyove, Holmove, Shafferove te Bergmannove) ukazuju na to da dva najbolja algoritma (stablo odluke i algoritam k-najbližih susjeda) statistički značajno nadmašuju logističku regresiju i naivni Bayesov algoritam, uz razinu značajnosti od 0.05.



Slika 5. Dijagram pravokutnika F1 mjere naivnog Bayesovog algoritma za različit broj značajki odabranih SFS omotačem

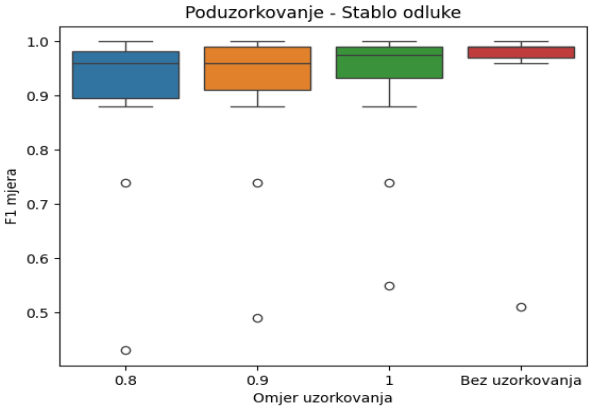
Tablica 2. Rezultati F1 mjere nakon primjene SFS omotača

Naziv	Stablo odluke	k-najbližih susjeda	Logistička regresija	Nasumična šuma	Naivni Bayesov
DARPA	0.99 ± 0.00 (-0.00)	0.99 ± 0.00 (-0.00)	0.83 ± 0.01 (-0.00)	0.99 ± 0.00 (-0.00)	0.91 ± 0.01 (-0.04)
KDD99	1.00 ± 0.00 (+0.01)	1.00 ± 0.00 (+0.01)	0.99 ± 0.01 (+0.01)	0.99 ± 0.01 (-0.00)	0.98 ± 0.01 (+0.01)
NSL-KDD	0.99 ± 0.01 (-0.00)	1.00 ± 0.00 (+0.01)	0.99 ± 0.01 (+0.02)	0.99 ± 0.01 (-0.00)	0.88 ± 0.01 (+0.06)
KYOTO	1.00 ± 0.00 (-0.00)	1.00 ± 0.00 (+0.01)	0.99 ± 0.01 (+0.01)	1.00 ± 0.00 (+0.01)	1.00 ± 0.00 (+0.01)
Malware	1.00 ± 0.00 (-0.00)	1.00 ± 0.00 (+0.01)	1.00 ± 0.00 (+0.01)	1.00 ± 0.00 (-0.00)	1.00 ± 0.00 (+0.03)
DREBIN	0.99 ± 0.01 (+0.01)	0.98 ± 0.01 (-0.01)	0.98 ± 0.01 (-0.00)	0.98 ± 0.01 (+0.01)	0.95 ± 0.01 (+0.13)
ISCXIDS2012	1.00 ± 0.00 (+0.01)	1.00 ± 0.00 (+0.01)	1.00 ± 0.00 (+0.01)	1.00 ± 0.00 (+0.01)	1.00 ± 0.00 (+0.01)
CICIDS2017	1.00 ± 0.00 (+0.01)	1.00 ± 0.00 (+0.01)	0.99 ± 0.01 (-0.00)	1.00 ± 0.00 (+0.01)	0.99 ± 0.01 (-0.00)
DS2OS	1.00 ± 0.00 (-0.00)	1.00 ± 0.00 (+0.00)	0.98 ± 0.01 (-0.02)	1.00 ± 0.00 (+0.01)	0.97 ± 0.01 (-0.00)
IMPACT	0.87 ± 0.01 (+0.01)	0.88 ± 0.01 (+0.01)	0.22 ± 0.01 (-0.01)	0.54 ± 0.01 (+0.03)	0.16 ± 0.01 (-0.01)
UNSW-NB15	1.00 ± 0.00 (+0.02)	1.00 ± 0.00 (+0.03)	0.95 ± 0.01 (+0.03)	1.00 ± 0.00 (+0.04)	1.00 ± 0.00 (+0.14)

CIC-DDOS2019	1.00 ± 0.00 (-0.00)	0.99 ± 0.01 (+0.02)	0.98 ± 0.01 (+0.01)	0.98 ± 0.01 (+0.01)	0.96 ± 0.01 (+0.09)
FR	2.125	2.125	3.875	2.75	4.125

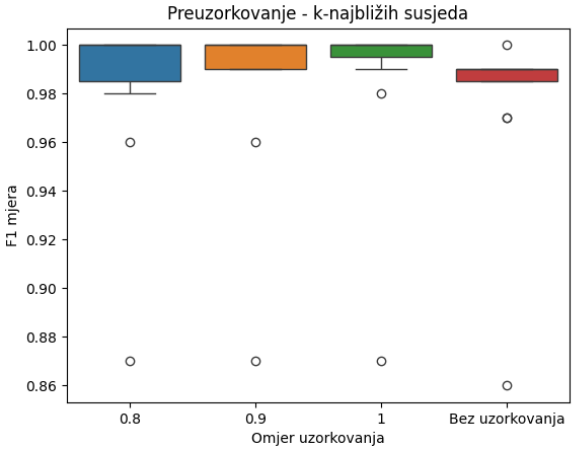
4.2. Analiza učinka uzorkovanja

Tehnike uzorkovanja imaju ključnu ulogu u prepoznavanju malicioznih napada zbog neuravnoteženosti većine skupova podataka gdje su primjeri manjinske klase često najvažniji za prepoznavanje (Krawczyk, 2016). Za rješavanje ovog problema koriste se nasumično preuzorkovanje i poduzorkovanje. Poduzorkovanje je uglavnom smanjilo performanse zbog dodatnog smanjenja već malog broja primjera. Isto se može primijetiti na KYOTO skupu podataka. Algoritmi k-najbližih susjeda, logistička regresija i nasumična šuma bilježe pad F1 vrijednosti za 0.75 te su njihove ostvarene vrijednosti 0.22, 0.25 i 0.24. Jedino kod skupova DARPA i CICIDS2017 se zamjećuje da je izjednačavanje kardinalnosti klasa poboljšalo rezultate, te algoritmi kod ovih skupova ostvaruju F1 vrijednosti oko 1.00. Suprotno tome, na skupu NSL-KDD primjetan je značajan pad performansi od oko 0.51, zbog velikog broja klasa s malim brojem primjera. Stablo odluke jedini je algoritam koji je zadržao vrijednosti F1 mjere veće od 0.9 kod većine skupova podataka, što je vidljivo na slici 6.



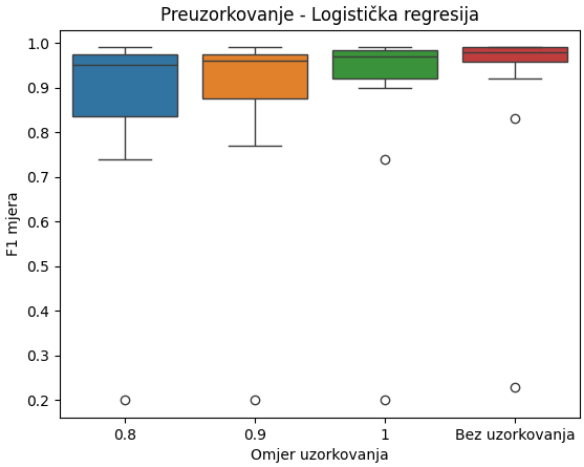
Slika 6. Dijagram pravokutnika F1 mjere algoritma stablo odluke za različite omjere uzorkovanja

Nasumično preuzorkovanje dosljedno je poboljšalo performanse svih algoritama na svim skupovima podataka, pri čemu stablo odluke na gotovo svim skupovima ostvaruje vrijednosti 1.0 za mjeru F1. Algoritam k-najbližih susjeda također bilježi značajna poboljšanja u odnosu na originalne skupove, kao što je prikazano na slici 7.



Slika 7. Dijagram pravokutnika F1 mjere algoritma k-najbližih susjeda za različite omjere uzorkovanja

S druge strane, kod logističke regresije i naivnog Bayes algoritma nasumično preuzorkovanje nije značajno doprinijelo performansama, pri čemu logistička regresija pokazuje varijabilne rezultate (slika 8).



Slika 8. Dijagram pravokutnika F1 mjere algoritma logistička regresija za različite omjere uzorkovanja

Algoritam naivni Bayes ima loše performansama na većini skupova podataka. Za Malware skup podataka vrijednost F1 mjere iznosi 1.0, na NSL-KDD skupu 0.51, a za IMPACT skupu podataka vrijednost je vrlo niskih 0.12. Iz navedenih brojeva primjećuje se nekonstantnost u prepoznavanju malicioznih napada, čak i nakon postignute ravnoteže u skupovima podataka.

5. Zaključak

U ovom radu prikazan je cjelovit pristup učenju algoritama klasifikacije na skupovima podataka s informacijama o malicioznim napadima, s ciljem ispitivanja mogućnosti primjene strojnog učenja u području kibernetičke sigurnosti. Znanstveni doprinos rada ogleda se u definiranju i evaluaciji toka učenja koji uključuje različite faze predobrade podataka, odabira značajki i uzorkovanja skupova podataka, čime se omogućuje sustavno vrednovanje utjecaja pojedinih metoda na performanse klasifikacijskih modela.
Rezultati eksperimentalne analize pokazuju da svi korišteni algoritmi ostvaruju zadovoljavajuće rezultate na većini skupova podataka, pri čemu se stablo odluke istaknulo kao najuspješniji algoritam. Uz stablo odluke, dobre rezultate pokazali su i algoritmi k-najbližih susjeda te nasumična šuma. Nasuprot tome, naivni Bayesov algoritam imao je najslabije performanse, što je posljedica njegove pretpostavke o međusobnoj neovisnosti značajki, uvjeta koji rijetko vrijedi za podatke o malicioznim napadima. Unatoč tome, upravo je kod ovog algoritma zabilježeno najveće poboljšanje u točnosti nakon primjene tehnika odabira značajki i uzorkovanja podataka. Od korištenih metoda za odabir značajki, SFS omotač pokazao se najuspješnijim, dok su i filter metode dale usporedive, ali nešto slabije rezultate. Kod rješavanja problema neuravnoteženosti skupova, učinkovitijom se pokazala tehnika nasumičnog preuzorkovanja.

Na temelju dobivenih rezultata može se zaključiti da strojno učenje ima značajan potencijal za unaprjeđenje kibernetičke sigurnosti. Predloženi tok učenja omogućuje primjenu klasifikacijskih modela visoke točnosti za prepoznavanje malicioznih aktivnosti u različitim podatkovnim okruženjima. Budući rad trebao bi se usmjeriti na razvoj kvalitetnijih i reprezentativnijih skupova podataka, uključivanje dodatnih izvora informacija kao što su mrežni dnevnici, vremenski obrasci i kontekstualni podaci, te primjenu i evaluaciju naprednijih modela dubokog učenja. Nadalje, potrebno je ispitati učinkovitost predloženog toka učenja u stvarnim, dinamičnim i distribuiranim okruženjima kibernetičke obrane, čime bi se dodatno potvrdila njegova praktična primjenjivost i robusnost.

6. Literatura

A., Goldbloom, Kaggle [online], San Francisco, 2010., dostupno na: https://www.kaggle.com/

Ahsan, M., Nygard, K. E., Gomes, R., Chowdhury, M. M., Rifat, N., & Connolly, J. F. (2022). Cybersecurity Threats and Their Mitigation Approaches Using Machine Learning—A Review. Journal of Cybersecurity and Privacy, *2*(3), 527-555.

Ahsan, M., Nygard, K. E., Gomes, R., Chowdhury, M. M., Rifat, N., & Connolly, J. F. (2022). Cybersecurity threats and their mitigation approaches using Machine Learning—A Review. Journal of Cybersecurity and Privacy, *2*(3), 527-555.

D., Aha, UCI Machine Learning Repository, California, 1987., dostupno na: https://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html

Derrac, J., Garcia, S., Molina, D., Herrera, F. (2011). A practical tutorial on tthe use of nonparametric statistical tests as a methodology for comparing evolutionary and swarm intelligence algorithms. Swarm Evol. Comput., 1, 3-18.

D'hooge, L., Wauters, T., Volckaert, B., & De Turck, F. (2019). In-depth comparative evaluation of supervised machine learning approaches for detection of cybersecurity threats. In 4th International Conference on Internet of Things, Big Data and Security (IoTBDS*)* (pp. 125-136).

Dudjak, M. (2022). Učenje iz neuravnoteženih podataka unaprijeđenim postupcima za odabir značajki, preuzorkovanje i izgradnju radijalnih neuronskih mreža [Disertacija, Sveučilište Josipa Jurja Strossmayera u Osijeku]

Fraley, J. B., & Cannady, J. (2017, March). The promise of machine learning in cybersecurity. In SoutheastCon 2017 (pp. 1-6). IEEE.

Kocher, G., & Kumar, G. (2021). Analysis of machine learning algorithms with feature selection for intrusion detection using UNSW-NB15 dataset. Available at SSRN 3784406.

Kotsiantis, S. B., Zaharakis, I., & Pintelas, P. (2007). Supervised machine learning: A review of classification techniques. Emerging artificial intelligence applications in computer engineering, *160*(1), 3-24

Krawczyk, B. (2016). Learning from imbalanced data: open challenges and future directions. Progress in artificial intelligence, *5*(4), 221-232

Martínez Torres, J., Iglesias Comesaña, C., & García-Nieto, P. J. (2019). Machine learning techniques applied to cybersecurity. International Journal of Machine Learning and Cybernetics, *10*(10), 2823-2836.

More, S., Idrissi, M., Mahmoud, H., & Asyhari, A. T. (2024). Enhanced intrusion detection systems performance with UNSW-NB15 data analysis. *Algorithms*, *17*(2), 64.

Sarhan, M., Layeghy, S., & Portmann, M. (2021). Feature analysis for machine learning-based IoT intrusion detection. *arXiv preprint arXiv:2108.12732*.

Sharp, R. (2017). An Introduction to Malware.

Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., Chen, S., Liu, D., & Li, J. (2020). Performance Comparison and Current Challenges of Using Machine Learning Techniques in Cybersecurity. *Energies*, *13*(10), 2509.

Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., Chen, S., Liu, D., & Li, J. (2020). Performance comparison and current challenges of using machine learning techniques in cybersecurity. Energies, *13*(10), 2509.

Tsiakos, C.-A. D., & Chalkias, C. (2023). Use of Machine Learning and Remote Sensing Techniques for Shoreline Monitoring: A Review of Recent Literature. Applied Sciences, *13*(5), 3268.

University of New Brunswick, dostupno na: https://www.unb.ca/cic/datasets/ids.html

UNSW Sydney, dostupno na: https://research.unsw.edu.au/projects/unsw-nb15-dataset

Venkatesh, B., & Anuradha, J. (2019). A review of feature selection and its methods. Cybern. Inf. Technol, *19*(1), 3-26.

Walling, S., & Lodh, S. (2024). Enhancing IoT intrusion detection through machine learning with AN-SFS: a novel approach to high performing adaptive feature selection. Discover Internet of Things, *4*(1), 16.

Yin, Y., Jang-Jaccard, J., Xu, W., Singh, A., Zhu, J., Sabrina, F., & Kwak, J. (2023). IGRF-RFE: a hybrid feature selection method for MLP-based network intrusion detection on UNSW-NB15 dataset. *Journal of Big data*, *10*(1), 15.

.

AN EMPIRICAL STUDY OF MACHINE LEARNING TECHNIQUES FOR MALICIOUS ATTACK DETECTION

Abstract: The aim of this paper is to define the learning flow of classification algorithms from datasets describing various types of malicious attacks and to determine individual procedures within that flow. By applying the defined flow, results were obtained that demonstrate the high quality of classification models in detecting malicious attacks, confirming its applicability in the field of cybersecurity, especially in intrusion detection systems. The machine learning algorithms used include: Naive Bayes, k-Nearest Neighbors, Decision Tree, Random Forest, and Logistic Regression. During feature selection, filters with Pearson correlation coefficient, mutual information, and ANOVA F-value were used, as well as the sequential forward selection (SFS) wrapper. For processing imbalanced datasets, random oversampling and undersampling procedures were applied. The Decision Tree algorithm achieved the best results with an F1 score of 1.0 on most datasets, while the Naive Bayes algorithm showed significantly weaker performance, with F1 values ranging from 0.12 to 0.98. Feature selection techniques generally improved performance, with the SFS wrapper being particularly prominent. Among the procedures for reducing data imbalance, random oversampling consistently improved the performance of all algorithms, whereas undersampling led to a significant decrease in performance for some algorithms, with F1 score drops of up to 0.22. The proposed learning flow enables the systematic evaluation of the impact of different data preprocessing methods and classification algorithms, thereby contributing to a better understanding of the process of malicious attack detection in imbalanced and heterogeneous datasets, and can serve as a basis for the development of more effective cybersecurity defense systems in real-world environments.

Keywords: classification, malicious attacks, imbalanced dataset, feature selection, machine learning

Zaprimljen: 10.6.2025.
Odobren za objavu: 23.7.2025.
Izvorni znanstveni rad

PERCEPCIJE UČENIKA O UČENJU TEMELJENOM NA DIGITALNIM IGRAMA

Marijana Zarožinski[1], Ljerka Jukić Matić[2], Maja Čuletić Ćondrić[3]
[1]Industrijsko-obrtnička škola, E. Kumičića 55, 35000 Slavonski Brod
ePošta: marijanazarozinski@gmail.com
[2]Fakultet primijenjene matematike i informatike, Trg Ljudevita Gaja 6, 31000 Osijek
ePošta: ljukic@mathos.hr
[3]Sveučilište u Slavonskom Brodu, Trg I. B. Mažuranić 2, 35000 Slavonski Brod, Hrvatska,
ePošta: mccondric@unisb.hr

Sažetak: Cilj ovog istraživanja je kreirati upitnik za ispitivanje stavova i motivacije učenika trogodišnjih strukovnih škola prema učenju matematike pomoću digitalnih igara (DGBL). Istraživanje je provedeno anketnim ispitivanjem na pilot uzorku od 56 učenika Industrijsko-obrtničke škole u Slavonskom Brodu, koristeći provjerene i pouzdane upitnike koji mjere više dimenzija motivacije i stavova. Rezultati pokazuju da učenici pokazuju statistički značajnu intrinzičnu i ekstrinzičnu motivaciju, s prevladavajućom intrinzičnom. Stavovi učenika prema DGBL-u su pozitivni, osobito u pogledu korisnosti i sklonosti igrama, dok je iskustvo s edukativnim igrama slabije izraženo. Nije utvrđena značajna povezanost stavova i motivacije s ocjenama iz matematike, no utvrđena je jaka pozitivna korelacija između stavova i motivacije. Istraživanje upućuje na važnost razmatranja digitalnih igara kao didaktičkog alata u nastavi matematike u strukovnim školama. Ovo istraživanje je dio istraživanja na razini Republike Hrvatske u kojem će sudjelovati 14 strukovnih škola u kojima se školuju učenici u trogodišnjim zanimanjima.

Ključne riječi: DGBL, digitalne igre, učenje pomoću igara, matematika, motivacija, stavovi

1. Uvod

U uvjetima brzog tehnološkog razvoja i sve veće prisutnosti digitalnih uređaja u svakodnevnom životu učenika, postavlja se pitanje kako digitalne tehnologije mogu unaprijediti obrazovni proces. Prema Labašu i sur. (2019), učenici u Hrvatskoj godišnje u prosjeku provedu 612 sati igrajući digitalne igre, što otvara mogućnost za njihovu svrhovitu primjenu u obrazovanju, osobito u nastavi matematike. Jedan od pristupa koji se razvija u tom smjeru je učenje pomoću digitalnih igara (DGBL – Digital Game-Based Learning), koje uključuje strukturirano obrazovno iskustvo temeljeno na interaktivnim digitalnim igrama s ciljem poticanja učenja i povećanja motivacije.

Digitalne igre predstavljaju inovativan pristup poučavanju jer se mogu dizajnirati tako da odgovaraju raznolikim potrebama učenika (Plass & Pawar, 2020). Pružaju sigurno i poticajno okruženje za učenje u kojem učenici mogu griješiti i učiti iz pogrešaka, što dovodi do uspješnijeg učenja te dodatno potiče motivaciju učenika i osjećaj samoefikasnosti (Plass i sur., 2015). Osim toga, jasno definirani obrazovni ciljevi usklađeni s kurikulumom te implementacija usmjerena na učenika na način da se svaka igra može prilagoditi različitim razinama predznanja i stilovima učenja pojedinog učenika, dodatno povećavaju učinkovitost učenja pomoću digitalnih igara (Pan i sur., 2022).

Sustavni pregledi literature (Pan i sur., 2022; Hussein i sur., 2022; Byun i Joung, 2018) pokazali su da se većina DGBL studija u području matematičkog obrazovanja odnosi na osnovnu školu, dok je broj istraživanja provedenih u srednjoškolskom kontekstu izrazito nizak. Jedan od razloga može biti to što se jednostavniji matematički sadržaji i postupci iz osnovne škole lakše prilagođavaju igrama tipa „uvježbavanje i ponavljanje", dok koncepti iz srednjoškolske matematike predstavljaju veći izazov za ovakav oblik implementacije. U većini studija, digitalne igre su se koristile se kao dopuna tradicionalnim metodama poučavanja, dok je tek manji broj studija istraživao mogućnosti uporabe igara za usvajanje novih znanja.

Unatoč tome, rezultati tih pregleda ukazuju na značajne koristi korištenja DGBL-a u nastavi matematike: digitalne igre pozitivno utječu na znanje i vještine učenika, poboljšavaju njihove perceptivne i kognitivne sposobnosti te potiču pozitivne promjene u stavovima, motivaciji, interesu i angažmanu (Hussein i sur.., 2022; Hui i Mahmud, 2023). Uz to, dokazano je da DGBL može smanjiti kognitivno opterećenje i time povećati učinkovitost učenja (Chang i Yang, 2023).

Vrlo mali broj studija ispitao je stavove učenika o korištenju digitalnih igara kao nastavnog alata i njihovu spremnost na učenje na takav način. Primjerice, Bourgonjon i sur. (2009), pokazali su da učenici koji imaju iskustva u igranju igrica i koji sebe smatraju „gamerima", bolje prihvaćaju primjenu digitalnih igara u obrazovanju. Jedan od općih zaključaka ovog ispitivanja je da učenici prepoznaju edukativni potencijal digitalnih igara.

No, u Republici Hrvatskoj istraživački radovi u kojima se ispituju stavovi i motivacija za učenje pomoću digitalnih igara nisu pronađeni. Posebno, nisu pronađeni radovi koji ispituju stavove i motivaciju za nastavu matematike, kao niti za učenike trogodišnjih zanimanja. Stoga smo za potrebe ovog rada postavili sljedeća istraživačka pitanja:

1) Kakva je motivacija učenika za učenjem matematike pomoću digitalnih igara?
2) Kakvi su stavovi učenika o učenju matematike pomoću digitalnih igara?

2. Metodologija

U ovom istraživanju primijenjena je kvantitativna metodologija, pri čemu je korišten anketni upitnik kao instrument prikupljanja podataka. Upitnik je bio sastavljen od dva dijela. Prvi dio bio je usmjeren na ispitivanje motivacije učenika za učenje matematike pomoću digitalnih igara, s naglaskom na usvajanje matematičkih koncepata. Ovaj dio temelji se na upitniku razvijenom i validiranom u radu Dijanić (2017), uz potrebne prilagodbe za kontekst ovog istraživanja. Drugi dio upitnika odnosio se na stavove učenika prema učenju putem digitalnih igara, a preuzet je i prilagođen iz instrumenta Bourgonjon i sur. (2009), koji je izvorno razvijen za ispitivanje percepcije učenika o obrazovnim digitalnim igrama.

Pilot-istraživanje provedeno je na uzorku od 56 učenika iz tri razredna odjela jedne srednje strukovne škole. Kako bi se umanjio mogući utjecaj nastavnika na odgovore učenika, istraživanje su istovremeno provela tri različita nastavnika matematike, svaki u svom razrednom odjelu. Veće istraživanje provest će se na razini Republike Hrvatske, a u njemu će sudjelovati 14 strukovnih škola u kojima se školuju učenici u trogodišnjim zanimanjima.

Prije administracije upitnika, svim učenicima dana je jasna definicija digitalnih igara za učenje matematike, budući da prethodno nisu imali izravno iskustvo s takvim obrazovnim alatima. Ciljana populacija bili su učenici trogodišnjih strukovnih škola, s obzirom na specifičnu problematiku niske motiviranosti za učenje matematike unutar ove skupine.

Stavovi učenika ispitani su kroz pet dimenzija koje su obuhvatile ukupno 28 čestica, pri čemu su čestice bile usmjerene na učenje matematike

pomoću digitalnih igara. Dimenzije su uključivale: korisnost, jednostavnost upotrebe, mogućnosti za učenje, stavove prema primjeni digitalnih igara u obrazovanju te opću sklonost računalnim igrama. Motivacija za učenje matematike putem digitalnih igara ispitana je putem 13 čestica raspoređenih u dvije dimenzije: intrinzična i ekstrinzična motivacija.

Analiza podataka provedena je pomoću programa IBM SPSS 26. Pouzdanost mjernog instrumenta procijenjena je pomoću Cronbachova alfa koeficijenta, pri čemu je dobivena visoka vrijednost (α = 0.963), što ukazuje na izvrsnu unutarnju konzistentnost upitnika.S obzirom na ordinalnu prirodu podataka i veličinu uzorka (N = 56), korišteni su neparametrijski testovi. Za ispitivanje odstupanja pojedinih tvrdnji od neutralne vrijednosti korišten je jednouzročni Wilcoxonov test. Za usporedbu dviju povezanih dimenzija (intrinzična i ekstrinzična motivacija) primijenjen je Wilcoxonov test za povezane uzorke. Kruskal-Wallisov test korišten je za analizu razlika u motivaciji i stavovima s obzirom na školski uspjeh, a Friedmanov test za ispitivanje razlika između dimenzija stavova. Za ispitivanje povezanosti između stavova i motivacije, kao i njihove povezanosti s ocjenom iz matematike, korišten je Spearmanov koeficijent rang-korelacije (ρ). Statistička značajnost testova određena je na razini $p < 0.05$. Prikazani su i osnovni deskriptivni pokazatelji (aritmetička sredina, medijan, mod).

3. Rezultati

3.1. Motivacija za učenje matematike pomoću digitalnih igara

Rezultati pokazuju da učenici trogodišnjih strukovnih škola općenito iskazuju pozitivnu motivaciju za učenje matematike pomoću digitalnih igara. Od ukupno 13 čestica koje su ispitivale motivaciju, njih 6 pokazalo je statistički značajno odstupanje od neutralne vrijednosti, i to prema višim vrijednostima. Unutar dimenzije intrinzične motivacije, 4 od 6 čestica bile su pozitivno ocijenjene (Tablica 1.), dok su u dimenziji ekstrinzične motivacije 2 od 7 čestica pokazale pozitivno odstupanje (Tablica 2.).

Tablica 1. Pokazatelji za intrinzičnu motivaciju

Čest.	M	Med.	Mod	Z
1	3.60	4	3	3.66*
2	3.38	4	4	2.25*
3	3.47	4	3	2.81*
4	3.07	3	3	0.34
5	3.56	4	3	3.06*
6	3.07	3	3	0.28

*p< 0.05, Med.= medijan, Čest. =čestica

Tablica 2. Pokazatelji za ekstrinzičnu motivaciju

Čest.	M	Med.	Mod	Z
7	3.21	3	4	1.14
8	3.34	4	4	1.95
9	3.33	3	3	2.16*
10	3.45	4	4	2.71*
11	3.32	3	3	1.91
12	3.20	3	3	1.40
13	3.18	3	3	0.78

*p< 0.05, Med.= medijan, Čest. =čestica

Ukupne vrijednosti također pokazuju statistički značajno odstupanje od neutralne vrijednosti za obje dimenzije: intrinzična motivacija (M = 3.50) i ekstrinzična motivacija (M = 3.43), pri čemu učenici izražavaju nešto višu intrinzičnu nego ekstrinzičnu motivaciju. Međutim, Wilcoxonov test pokazao je da razlika između intrinzične i ekstrinzične motivacije nije statistički značajna (p = 0.727), što upućuje na to da učenici iskazuju podjednake razine obje vrste motivacije.

Kruskal-Wallisovim testom nije utvrđena statistički značajna razlika u razini ni intrinzične (p = 0.947) ni ekstrinzične motivacije (p = 0.864) između skupina učenika različitih ocjena. Ni grupiranje ocjena u tri skupine (nedovoljan/dovoljan; dobar; vrlo dobar/odličan) nije pokazalo značajne

razlike (intrinzična p = 0.900; ekstrinzična p = 0.765).

3.2. Stavovi učenika o učenju matematike pomoću digitalnih igara

Stavovi učenika ispitivani su kroz pet dimenzija (Tablica 3). Čestice koje su se odnosile na korisnost (čestice 1–3) sve su statistički značajno odstupale od neutralne vrijednosti i pokazivale srednje vrijednosti iznad 3, što upućuje na to da učenici smatraju kako je učenje matematike putem digitalnih igara korisno.

Unutar dimenzije jednostavnosti korištenja, tri od četiri čestice (čestice 5, 6 i 7) bile su pozitivno ocijenjene, dok je samo jedna (čestica 4) ostala bez statistički značajnog odstupanja. Što se tiče dimenzije mogućnosti za učenje, od 7 čestica njih 4 pokazale su statistički značajno odstupanje (čestice 8, 9, 10 i 12), također prema višim vrijednostima.

Analiza dimenzije „iskustvo u igranju digitalnih igara" pokazala je da učenici preferiraju akcijske, avanturističke, sportske i utrkivačke igre, dok manje preferiraju edukativne ili logičke igre *(Augmented Reality, Digital Inquiry Game, E-Rebuild, Math-Island Game, NanoRoboMath, Quizizz, and Wuzzit Trouble, Triângulo Resgate)*. Zanimljivo je da tvrdnja o igranju strateških igara nije pokazala statistički značajno odstupanje.

Sva tri iskaza iz dimenzije „sklonost digitalnim igrama u nastavi" (čestice 26–28) pokazuju statistički značajno odstupanje od neutralne vrijednosti, što upućuje na izraženu naklonost učenika prema korištenju digitalnih igara u nastavi matematike.

Tablica 3. Dimenzije stavova

Dimenz. stavova	**Broj čest.**	**M**	**Med.**	**Z**
Sklonost	3	3.81	4	4.22
Korisnost	3	3.42	3	3.09
Jednostav. korištenja	4	3.44	3.5	3.26
Mogućnost za učenje	7	3.34	3	2.47
Iskustvo	11	2.99	3	-0.07

*p<0.05, Med.= medijan, čest.=čestica

3.3. Razlike u ocjenama stavova

Kako bi se utvrdilo postoje li statistički značajne razlike među pojedinim dimenzijama stavova učenika o učenju matematike pomoću digitalnih igara, primijenjen je Friedmanov test za povezane uzorke. Rezultati testa pokazali su postojanje značajnih razlika među ocjenama dimenzija ($p < 0{,}001$), što je upućivalo na potrebu daljnje analize kako bi se utvrdilo između kojih konkretnih dimenzija postoje te razlike.

Najviše prosječne ocjene dobile su tvrdnje koje pripadaju dimenziji sklonosti prema digitalnim igrama u nastavi, osobito tvrdnja „Sviđa mi se ideja korištenja računalnih igara u nastavi matematike" (čestica 28). Također, visoku ocjenu dobila je i tvrdnja „Volim igrati računalne igre" (čestica 15) iz dimenzije iskustva. S druge strane, najnižu prosječnu ocjenu zabilježila je tvrdnja „Najčešće igram edukativne igre" (čestica 25), što ukazuje na općenito nizak stupanj prethodnog iskustva učenika s edukativnim igrama.

Kako bi se preciznije identificirale razlike među dimenzijama, provedena je post hoc analiza s Bonferronijevom korekcijom. Rezultati parovnih usporedbi dimenzija prikazani su u Tablici 4. Statistički značajne razlike zabilježene su između sljedećih parova dimenzija:

- iskustvo – sklonost
- iskustvo – jednostavnost korištenja
- iskustvo – korisnost
- mogućnost – sklonost
- korisnost – sklonost

Ove razlike upućuju na to da učenici izražavaju visoku sklonost prema korištenju digitalnih igara u nastavi, te percipiraju njihovu korisnost i jednostavnost upotrebe kao pozitivne, unatoč tome što imaju ograničeno

prethodno iskustvo s edukativnim igrama. Drugim riječima, učenici prepoznaju obrazovni potencijal digitalnih igara čak i ako ih dosad nisu redovito koristili u obrazovnom kontekstu.

Takvi rezultati ukazuju na prostor za pedagoške intervencije kojima bi se digitalne igre sustavnije uključile u nastavni proces, čime bi se dodatno mogle potaknuti motivacija, angažiranost i interes učenika za matematiku.

Preostali parovi dimenzija nisu pokazali statistički značajne razlike ($p > 0.05$), što sugerira da učenici korisnost, jednostavnost i mogućnosti za učenje doživljavaju kao slične i međusobno povezane aspekte primjene digitalnih igara u obrazovanju.

3.4. Povezanost stavova i motivacije

Spearmanovom korelacijskom analizom utvrđena je statistički značajna pozitivna povezanost između ukupnih stavova učenika i njihove motivacije za učenje matematike pomoću digitalnih igara (ρ = 0.765; $p < .001$). Dodatno, utvrđena je pozitivna povezanost između stavova i intrinzične motivacije (ρ = 0.729; $p < .001$), kao i između stavova i ekstrinzične motivacije (ρ = 0.712; $p < .001$). S druge strane, nije utvrđena statistički značajna povezanost između školskog uspjeha (ocjene iz matematike) i bilo koje od dimenzija motivacije (ρ = 0.05, p = 0.714;) niti s ukupnim stavovima učenika (ρ = 0.059, p = 0.663).

Ovi rezultati ukazuju da razina ocjene nije povezana s motivacijom učenika niti sa stavovima učenika u ovom uzorku.

Tablica 4. Veza između dimenzija stavova učenika

Usporedba dimenzija	**Z vrijednost**	***p***	***p* (Bonferroni)**
Iskustvo – Mogućnost	2.111	.035	.348
Iskustvo – Korisnost	-3.106	.002	**.019**
Iskustvo – Jednostavnost	-3.317	< .001	**.009**
Iskustvo – Sklonost	-5.789	< .001	**< .001**
Mogućnost – Korisnost	-0.995	.320	1.000
Mogućnost – Jednostavnost	-1.206	.228	1.000
Mogućnost – Sklonost	-3.678	< .001	**.002**
Korisnost – Jednostavnost	-0.211	.833	1.000
Korisnost – Sklonost	-2.683	.007	**.007**
Jednostavnost – Sklonost	-2.472	.013	.134

4. Rasprava i zaključak

Rezultati ovog pilot-istraživanja upućuju na potencijal implementacije digitalnih igara u nastavu matematike u trogodišnjim strukovnim školama. Prije svega, učenici pokazuju značajnu motivaciju za učenje matematike putem digitalnih igara, pri čemu intrinzična motivacija blago prevladava nad ekstrinzičnom. Ovo je u skladu s rezultatima prethodnih istraživanja koja su pokazala da digitalne igre mogu povećati interes i angažiranost učenika stvaranjem iskustva učenja koje je istovremeno izazovno i zabavno (Plass et al., 2015; Pan et al., 2022).

Unatoč ograničenom prethodnom iskustvu učenika s edukativnim igrama, stavovi učenika prema DGBL-u su vrlo pozitivni. Posebno su izraženi stavovi koji se odnose na korisnost i prihvaćanje digitalnih igara u obrazovanju. Ovo sugerira da i bez izravnog iskustva s ovakvim oblikom nastave, učenici prepoznaju njegov potencijal, što podupire nalaze Bourgonjona i suradnika (2009), koji su pokazali da čak i učenici s ograničenim iskustvom mogu razviti pozitivan stav prema obrazovnim igrama. Digitalne igre u nastavni mogu

utjecati na razvoj kompetencija poput suradnje, rješavanja problema i digitalne pismenosti.

Značajna pozitivna korelacija između stavova i motivacije dodatno podupire važnost percepcije učenika u prihvaćanju inovativnih obrazovnih pristupa. Ovaj nalaz sugerira da pozitivni stavovi prema DGBL-u mogu igrati ključnu ulogu u oblikovanju motivacije učenika za učenje, bez obzira na prethodna akademska postignuća, s obzirom da nije utvrđena povezanost između ocjena iz matematike i bilo koje dimenzije stavova ili motivacije.

Posebno je zanimljivo da učenici, iako rijetko koriste edukativne igre, visoko ocjenjuju njihovu potencijalnu primjenu u nastavi. Ovo ukazuje na tzv. *latentnu spremnost* na promjene u obrazovnim metodama i pruža čvrstu osnovu za daljnju implementaciju DGBL pristupa. S obzirom na to da su dimenzije korisnosti, jednostavnosti korištenja i obrazovnog potencijala međusobno povezane, dizajn budućih digitalnih obrazovnih igara trebao bi biti intuitivan, relevantan i usmjeren na stvarne potrebe učenika, pri čemu je važno istaknuti digitalnu sigurnost učenika te odgovorno korištenja digitalnih igara.

Nadalje, potrebne su pedagoške intervencije koje će transformirati pozitivne stavove i motivaciju učenika u trogodišnjim strukovnim školama u konkretna obrazovna iskustva i alate.

Važno je uzeti u obzir i potencijalne izazove povezane s digitalizacijom nastave, uključujući pitanja kibernetičke sigurnosti. Budući da digitalne igre zahtijevaju povezivanje s internetom, i često se oslanjaju na vanjske digitalne platforme, postoji potreba za sustavnom procjenom sigurnosnih aspekata njihove upotrebe u kontekstu obrazovanja. S obzirom da su učenici u najvećoj mjeri maloljetni, potrebno je osigurati da platforme budu u skladu sa zakonom o zaštiti podataka (npr. GDPR) te da učitelji budu educirani o osnovama digitalne sigurnosti.

Uvođenje DGBL-a mora uključivati i razvoj digitalne pismenosti kod učenika, ali i osvještavanje o sigurnosnim rizicima: zaštiti lozinki, prepoznavanju pokušaja phishinga, te izbjegavanju dijeljenja osobnih informacija tijekom igranja ili prijave u sustav. Integracija kibernetičke sigurnosti kao obrazovne teme, u kombinaciji s korištenjem edukativnih igara, mogla bi poslužiti kao dvostruka pedagoška intervencija tj. povećanje motivacije i razvoj odgovornog digitalnog ponašanja.

Iako unutar ovog istraživanja nije bilo moguće mjeriti razinu digitalne sigurnosne pismenosti učenika, buduća istraživanja uz motivaciju i stavove mogla bi istražiti i dimenziju sigurnosne svijesti i navika u digitalnom okruženju na većem broju ispitanika.

Literatura

Bourgonjon, J., Valcke, M., Soetaert, R., i Schellens, T. (2010). Students' perceptions about the use of video games in the classroom. Computers & Education, 54(4), 1145–1156.https://doi.org/10.1016/j.compedu.2009.10.022

Byun, J., i Joung, E. (2018). Digital game-based learning in mathematics education: A meta-analysis of research findings. *Educational Research Review, 27*, 14-31. https://doi.org/10.1016/j.edurev.2018.01.002

Chang, C.-C., i Yang, S.-T. (2023). Interactive effects of scaffolding digital game-based learning and cognitive style on adult learners' emotion, cognitive load and learning performance. *International Journal of Educational Technology in Higher Education, 20*(1), 16. https://doi.org/10.1186/s41239-023-00385-7

Dijanić, Ž.(2017). Razvoj modela računalno vođenoga učenja otkrivanjem korištenjem programa dinamične geometrije u nastavi matematike [Neobjavljena doktorska disertacija]. Sveučilište u Zagrebu

Hussein, M.H., Ow, S.H., Elaish, M.M., i Jensen, E. O. (2022) Digital game-based learning in K-12 mathematics education: a systematic literature review. *Education and Information Technologies*, *27*(2), 2859–2891. https://doi.org/10.1007/s10639-021-10721-x

Labaš, D.; Marinčić, I., i Mujčinović, A. (2019). Percepcija djece o utjecaju videoigara, *Communication Management Review*, *4*(1). 8–27.

Pan, Y., Ke, F., i Xu, X. (2022). A systematic review of the role of learning games in fostering mathematics education in K-12 settings. *Educational Research Review*. Advanced Online Publication. https://doi.org/10.1016/j.edurev.2022.100448

Plass, J. L., i Pawar, S. (2020). Adaptivity and personalization in game-based learning. In J. L. Plass, R. E. Mayer, & B. D. Homer (Eds.), *Handbook of game-based learning* (pp. 263–281). The MIT Press.

Plass, J. L., Homer, B. D., i Kinzer, C. K. (2015). Foundations of game-based learning. *Educational Psychologist, 50*(4), 258–283. https://doi.org/10.1080/00461520.2015.1122533

STUDENT PERCEPTIONS OF DIGITAL GAME BASED LEARNING

Abstract: The aim of this research is to create a questionnaire to examine the attitudes and motivation of students of three-year vocational schools towards learning mathematics using digital games (DGBL). The research was conducted through a survey on a pilot sample of 56 students of the Industrial and Craft School in Slavonski Brod, using validated and reliable questionnaires that measure multiple dimensions of motivation and attitudes. The results show that students show statistically significant intrinsic and extrinsic motivation, with intrinsic motivation prevailing. Students' attitudes towards DGBL are positive, especially in terms of usefulness and preference for games, while experience with educational games is less pronounced. No significant connection between attitudes and motivation and mathematics grades was found, but a strong positive correlation was found between attitudes and motivation. The research indicates the importance of considering digital games as a didactic tool in teaching mathematics in vocational schools. This research is part of a research at the level of the Republic of Croatia in which 18 vocational schools where students in three-year professions are educated will participate.

Keywords: attitudes, DGBL, digital games, game based learning, mathematics, motivation

Zaprimljen: 29.5.2025.
Odobren za objavu: 23.7.2025.
Prethodno priopćenje

DIGITALNA DEKADA I EKONOMSKI RAST: KVANTIFICIRANJE KORISTI DIGITALNE TRANSFORMACIJE U EUROPSKOJ UNIJI

Tomislav Horvat[1]
[1] Dilj d.o.o. (članica Nexe grupe), Ciglarska 33, 32100 Vinkovci
ePošta: thorvatt@gmail.com

Sažetak: Digitalna dekada predstavlja politiku Europske unije za digitalno desetljeće do 2030. godine s ciljem jačanja strateškog okvira za ubrzanje digitalne transformacije do kraja desetljeća. U radu će se analizirati ekonomske koristi digitalne transformacije na temelju ključnih podataka na razini cijele Europske unije i posebno istražiti razina digitalnog razvoja Republike Hrvatske. Korištenjem sekundarnih podataka Europske komisije, Eurostata analizirati će se rast BDP-a, udio ICT-a u BDP-u te usporediti s razinom digitalne pismenosti stanovništva i njegovog utjecaja na gospodarstvo. Statističkom analizom nastoji se utvrditi postoji li korelacija između razine digitalizacije i gospodarskog rasta te potencijal Republike Hrvatske za daljnji rast. Cilj rada je utvrditi postoji li jasna poveznica između značajnog rasta BDP-a, razvijenosti zemlje i razvojem ICT sektora, odnosno digitalne pismenosti stanovništva.

Ključne riječi: Digitalna dekada, digitalna pismenost, digitalna transformacija, ekonomski rast, ICT sektor

1. Uvod

Digitalna transformacija ima sve veći značaj za rast i oblikovanje gospodarstva, tržišta rada i javnih usluga. Pozitivan utjecaj digitalne transformacije na inovacije i produktivnost široko je dokumentiran, ali još uvijek postoji ograničeni broj istraživanja koji direktno povezuju odnos između razine digitalizacije i gospodarskog rasta. Otvoreno je pitanje u kojoj mjeri politike u sklopu Digitalne dekade EU utječu na gospodarski rast, utječu na rast i razvoj pojedinih gospodarstava zemalja članica. Osnovni smjerovi djelovanja pokazuju kako će EU napredovati s o
bzirom na trenutačne trendove, a zacrtani smjerovi djelovanja pokazuju u kojem se smjeru godišnji napredak treba kretati da bi se ostvarili ciljevi do 2030. Komisija će na temelju razlike između procijenjenih trendova i idealnog smjera djelovanja moći će identificirati područja u kojima je potreban dodatni napor. Komisija će do lipnja 2026. preispitati ciljeve s obzirom na tehnološke, gospodarske i društvene promjene (Europska komisija, 2025). Hrvatska poduzeća su na čelu digitalne otvorenosti, nadmašujući svoje regionalne kolege, i spremno podržavaju digitalne tehnologije, posebno u području e-trgovine i usluga računarstva u oblaku (Milošević et. al., 2018). Zemlje Zapadnog Balkana pokazale su snažnu konvergenciju digitalne transformacije, a glavni pokretač konvergencije bio je ukupni tehnološki napredak u tim gospodarstvima (Broz et. al., 2020). Europsko usklađivanje u ovom području izuzetno je malo vjerojatno zbog povezanosti između radne politike i socijalnog sustava, ali trenutne potrebe mogu se ispuniti uvođenjem zajedničkog općeg stava suočenog s izazovom koji predstavlja digitalno gospodarstvo (Troitiño, 2022). Disruptivne digitalne inovacije mijenjaju tradicionalne operativne modele, zahtijevajući dinamičke sposobnosti za odgovarajući

odgovor. Štoviše, izgradnja mogućnosti digitalne platforme kao dinamičkih sposobnosti smatra se temeljnom u odgovoru na digitalne poremećaje. (Krause et. al., 2021). Još uvijek vrlo malo znamo o ulozi etike u formuliranju i provedbi digitalne strategije kao sredstva za osiguranje da pozitivni utjecaji digitalne transformacije na razini tvrtke ostanu dosljedni na višim razinama. (Vial, 2021). Promjena će biti prepoznatljiva svim relevantnim dionicima. Koliko će se brzo ta promjena konkretizirati ovisi o tome koliko su dionici motivirani i predani kolektivnom cilju, a to je digitalizacija. (Zaoui et. al., 2020). Uspon digitalnog konstitucionalizma predstavlja kraj liberalnog pristupa Unije i potencijalnu osnovu za promicanje demokratskog digitalnog okruženja EU. Međutim, digitalni konstitucionalizam se čini daleko od posljednjeg koraka regulatornog puta EU. (De Gregorio, 2021). Pitanje je je li pojam „europski digitalni identitet" adekvatan budućim ciljevima Europske unije, s obzirom na to da je političko i kulturno pitanje europskog identiteta još uvijek sporno, a koncept europskih vrijednosti nejasan (Ivic and Troitiño, 2022).

Međutim potrebno je konstantno imati na umu da ne uspijevaju sve digitalne transformacije. One koje uspiju, odraz su robusne strategije koja se pridržava definiranih pravila (Lugavić and Rožajac, 2022). Može se zaključiti da je digitalizacija u Hrvatskoj u privatnom sektoru uspjela ostvariti uspjeh sličan onima u drugim novim demokracijama EU-a, dok je u cjelini proces digitalne transformacije zapeo na području poslovnih praksi javnoga i političkoga sektora (Poljanec-Borić, 2021). Za potrebe istraživanja su postavljene hipoteze:

H1: Postoji pozitivna korelacija između razine digitalizacije (mjerene DESI pokazateljima) i gospodarskog rasta (BDP-a) država članica EU.

H2: U razdoblju nakon pandemije COVID-19 (2020.–2024.), ubrzanje digitalne transformacije pozitivno je koreliralo s oporavkom gospodarstava u EU.

H3: *Dostupnost digitalnih javnih usluga pozitivno korelira s osnovnom digitalnom pismenošću građana.*

2. Metodologija

Korišteni su sekundarni kvantitativni podaci dobiveni putem službenih stranica Eurostata, Europske komisije, Statiste. Fokus analize su podaci vezani za Europsku uniju s naglaskom na Republiku Hrvatsku. Promatrano razdoblje svih podataka je od 2019.-2025. godine, s obzirom da podaci za određene godine nisu dostupni. Analizirani su sljedeći pokazatelji: stopa rasta BDP-a, udio ICT sektora u BDP-u, razina digitalnih vještina stanovništva, DESI indeks, digitalna dekada. Analiza je provedena na dvije razine:

1. Usporedna analiza Europske unije i Republike Hrvatske
2. Unutarnja povezanost pokazatelja Republike Hrvatske

U analizi su primijenjene metode deskriptivne statistike te Pearsonova korelacija radi ispitivanja odnosa između varijabli i potvrde postavljenih hipoteza, pri tome uzimajući u obzir ograničeni broj dostupnih godina (N=3-5). Jedno od glavnih ograničenja istraživanja jest ograničen broj dostupnih podataka po godinama, što može utjecati na statističku validnost rezultata i mogućnost generalizacije zaključaka. Potencijalna pristranost proizlazi iz odabira sekundarnih izvora podataka, iako su službeni, mogu imati metodološke razlike u obradi ili klasifikaciji pokazatelja među državama članicama EU. Statistička obrada podataka provedena je u programu Microsoft Excel, koji je korišten za izračune korelacija i prikaz deskriptivnih vrijednosti.

3. Rezultati i rasprava

Rezultati se temelje na korelacijskoj i deskriptivnoj analizi za razdoblje 2019. do 2024. s ciljem utvrđivanja obrazaca i

odnosa između digitalnih parametara i rasta BDP-a. Usporedba Republike Hrvatske i Europske unije je relevantna zbog povezivanja smjera kretanja pojedinih faktora, ali i zbog usporedbe zemlje s prosjekom EU. Zbog složenosti i opsega dostupnih podataka, analiza je fokusirana na jedan ključni čimbenik kako bi se osigurala metodološka konzistentnost.. Tablica 1. prikazuje analizu ključnih faktora digitalne dekade.

Tablica 1. Analiza ključnih faktora digitalne dekade

	2019		2020		2021		2022		2023		2024	
	EU	RH	EU	RH	EU	RH	EU	RH	EU	RH	EU	RH
Upotreba interneta	81,57	72,69	83,90	77,12	85,84	77,55	87,18	80,32	88,55	80,65	90,27	82,46
ICT diplomanti	3,50	5,50	3,80	4,00	3,90	4,40	3,90	4,70	4,20	4,80	4,50	5,20
ICT specijalisti	3,80	3,50	4,00	3,20	4,30	3,70	4,50	3,60	4,60	3,70	4,80	4,30
Osnovne digitalne vještine	-	-	-	-	-	-	53,92	63,37	53,92	63,37	55,56	58,95
Iznadprosječne digitalne vještine							26,46	31,18	26,46	31,18	27,32	25,00
Digitalne javne usluge za pravne subjekte			87,72	61,61	84,4	72,65	81,71	68,06	83,73	66,81	85,42	66,18
Digitalne javne usluge za fizičke osobe	73,13	52,08	76,9	58,05	74,93	60,29	74,63	69,02	77,03	71,12	79,44	67,17

Izvor: Digitalna dekada, 2025.

Zabilježen je pozitivan rast upotrebe interneta na razini Europske unije i Republike Hrvatske. Europska unija raste s 81,57% na 90,27% (2019-2024), te u istom periodu Republika Hrvatska bilježi porast 72,69% na 82,46%. Dostupnost internetskih usluga, pametnih telefona, rast životnog standarda i potreba za korištenjem komunikacijskih aplikacija pridonijeli su i uključivanju dijela populacije koji se ranije nije koristio internetskim uslugama.

Diplomanti, odnosno osobe koje su završile određeni ICT stupanj akademskog obrazovanja su laganom padu. Promatrajući promjenu na razini Europske unije (2019-2024) vidljiv je pad s 5,5% na 3,5%, dok u Republici Hrvatskoj 5,2% na 4,5% što je manji pad u odnosu na prosjek Europske unije. Navedeni podatak je direktno povezan s brojem ICT specijalista upravo zbog istraživanja koliko formalna edukacija utječe na broj ICT stručnjaka. Iako na razini Europske unije broj diplomanata ICT struke pada, broj ICT stručnjaka je u porastu s 3,80% na 4,80%, a Republika Hrvatska s 3,50% na 4,30%. Diskrepancija između broja diplomanata i broja zaposlenih ICT stručnjaka može se objasniti faktorima poput ekonomske migracije i nesklada između obrazovanja i tržišnih potreba. Dodatno istraživanje na razini Republike Hrvatske u suradnji s Hrvatskim zavodom za zapošljavanje može ponuditi navedene odgovore. Republika Hrvatska bilježi veću razinu osnovnih digitalnih vještina kod svojih građana (2024. godina – 58,9%) u odnosu na prosjek Europske unije (55,56%). Razlika je vidljiva kod naprednih digitalnih vještina, Republika Hrvatska (2024. godina – 25,00%), a prosjek Europske unije (27,30%). Iako je RH bila ispred prosjeka u 2022. godini, u narednim godinama se dogodila stagnacija i pad u odnosu na prosjek EU. Ponovno se kao razlog može promatrati

migracija stanovništva, ali i potencijalni uzrok u obrazovnom sustavu te tržištu rada. Navedena digitalna pismenost se direktno preslikava i na poslovni sektor. Digitalne javne usluge za pravne subjekte u Republici Hrvatskoj su na niskoj razini (2024. godina – 66,18%) u odnosu na prosjek Europske unije (2024. godina – 85,42%). Digitalne javne usluge za fizički sektor isto zaostaju za prosjekom Europske unije (2024. godina – 79,44%), Republika Hrvatska (2024. godina – 67,17%). Uočen je pozitivan trend u povećanju dostupnosti digitalnih javnih usluga za fizičke osobe, u razdoblju od 2019. do 2024. godine, u Republici Hrvatskoj zabilježen je porast od 15,09%, je porast na razini Europske unije 2019-2024 u iznosu 6,31%. Analiza pokazuje da s porastom upotrebe interneta, rasta digitalnih vještina i iznadprosječnih digitalnih vještina dolazi i do porasta korištenja digitalnih javnih usluga (pravnih i fizičkih) što potvrđuje hipotezu H3: Dostupnost digitalnih javnih usluga pozitivno korelira s osnovnom digitalnom pismenošću građana. Prosjek Europske unije čine zemlje visokog stupnja razvijenosti i zbog toga podatak djeluje dosta visok, ali prilikom usporedbe sa pojedinačnim zemljama Europske unije, Republika Hrvatska nije na začelju i pozitivno je što ne zaostaje previše postotnih poena. Tablica 2. prikazuje analizu BDP-a na razini Republike Hrvatske i Europske unije.

Tablica 2. Rast BDP-a na razini EU i Republike Hrvatske

	2020	2021	2022	2023	2024	2025	2026
Europska unija	5,60	6,30	3,50	0,40	1,00	1,10	1,5
Republika Hrvatska	8,30	12,60	7,30	3,30	3,90	3,20	2,9

Izvor:Economy finance, 2025.

Republika Hrvatska u zadnje 5 godine ima veći rast u odnosu na prosjek Europske unije. Tijekom pandemijske 2020. Godine je imala nižu stopu rasta u odnosu na prosjek Europske unije, ali je već iduće godine ponovno imala veći rast. Razlog tome je ovisnost o turističkom sektoru, koji je doživio značajan pad za vrijeme pandemije COVID-19 virusa. Upravo u takvom tipu gospodarstva ICT sektor donosi stabilni odio BDP-a koji neće ovisiti o regionalnim previranjima i turističkom potencijalu zemlje. Projekcija za 2025. i 2026. godinu pokazuju zadovoljavajući rast. U obzir treba uzeti prethodne godine koje nisu navedene u tablici, gdje Republika Hrvatska ima slabije stope rasta te je duže bila u recesiji nego ostale zemlje Europske unije. Tablica 3. Analizira udio ICT industrije u ukupnom BDP-u.

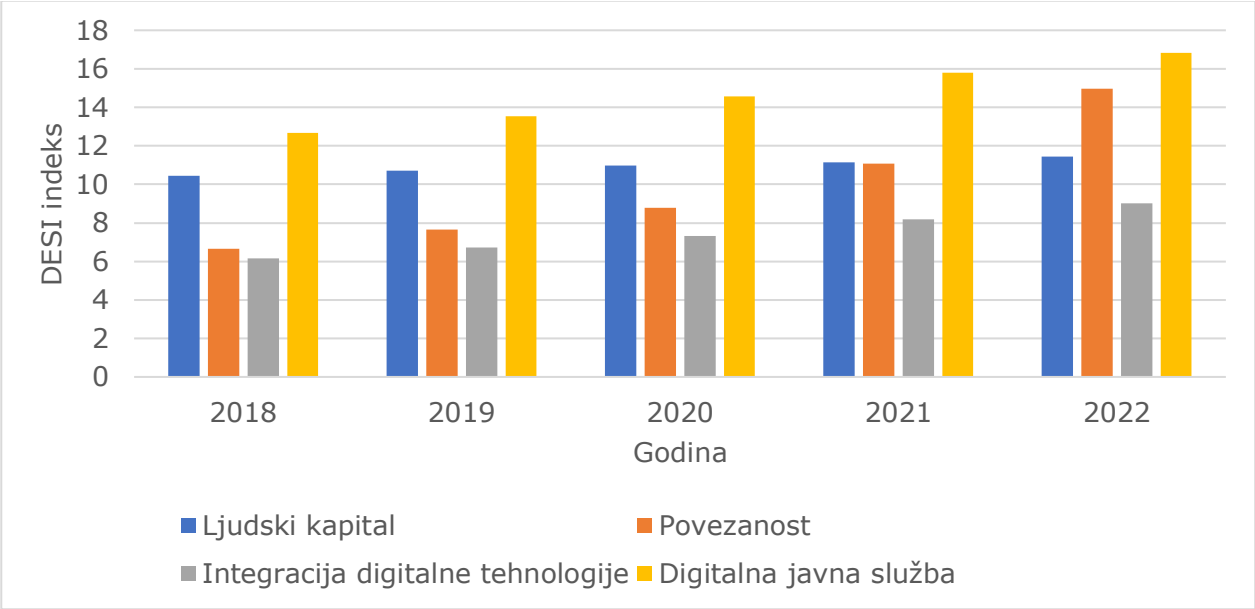
Tablica 3. Analiza udjela ICT industrije u ukupnom BDP-u

	2019	2020	2021	2022
Europska unija	4,86	5,19	5,46	5,46
Republika Hrvatska	4,52	5,02	5,31	5,32

Izvor: Eurostat, 2025.

Pozitivni pokazatelj je udio ICT industrije u ukupnom BDP-u, gdje se jasno zaključuje da je Republika Hrvatska blizu prosjeka Europske unije te da pomalo nadoknađuje zaostatak. Europska unije je bilježila rast od 4,86% u 2019. godini na 5,46% u 2022. Godini. U isto vrijeme, Republika Hrvatska je zabilježila rast s 4,52% u 2019. godini na 5,32% u 2022. Godini. Navedeni podaci vezani za rast BDP-a se mogu povezati s povećanjem digitalne pismenosti stanovništva (upotreba interneta, osnovna I iznadprosječna razina digitalnih vještina) te zaključiti da umjerena pozitivna korelacija postoji. Korelacijska analiza pokazuje umjerenu pozitivnu povezanost između udjela ICT sektora i

gospodarskog rasta u RH (r = 0,476), dok EU pokazuje sličan trend (r = 0,411), što djelomično potvrđuje hipotezu H1. Postoji pozitivna korelacija između razine digitalizacije (mjerene DESI pokazateljima) i gospodarskog rasta (BDP-a) država članica EU. Za potpunu potvrdu je potrebno promatrati veći niz godina, zbog toga treba podatak promatrati kao indikativan, ograničeno je statistički značajan. Graf 1. Prikazuje DESI indeks od 2017.-2020. godine.



Graf 1. Digital Economy and Society Index (DESI)
Izvor: Statista, 2025.

Europska komisija prati digitalni napredak država članica putem izvješća o indeksu digitalnog gospodarstva i društva (DESI) od 2014. Od 2023., i u skladu s Programom politike digitalnog desetljeća 2030., DESI je sada integriran u izvješće o stanju digitalnog desetljeća i koristi se za praćenje napretka prema digitalnim ciljevima. (Web stranica, Digital Strategy EU, 2025). Prognoza izvedena iz DESI indeksa je od velike važnosti, prvo zato što je sam indeks privukao značajnu pozornost europskih vlasti, a drugo zato što bi se predložena metodologija prognoziranja mogla primijeniti na veći uzorak zemalja, stvarajući klastere zemalja prema njihovim (prognoziranim) rezultatima. (Laitsou, 2020). Digitalne tehnologije sve više postavljaju nove zahtjeve i očekivanja javnom sektoru. Ostvarivanje punog potencijala ovih tehnologija ključni je izazov za vladine organizacije (Turuk et. al., 2022). Usporedbom pokazatelja za EU prije i poslije pandemije zaključuje se da je pozitivno ubrzavanje digitalne javne službe s 14,58 u 2020. Godini na 16,84 u 2022. Godini. BDP nakon pada u 2020. Godini raste u 2021. godini za 6,3% i 3,5% u 2022. godini. U navedenom period se bilježi i pozitivan rast digitalnih pokazatelja – upotreba interneta i digitalne vještine uz rast BDPa. Navedeno podupire hipotezu H2: U razdoblju nakon pandemije COVID-19 (2020.–2024.), ubrzanje digitalne transformacije pozitivno je koreliralo s oporavkom gospodarstava u EU.

4. Zaključak

Istraživanjem su potvrđeni pozitivne korelacije između gospodarskog rasta i udjela ICT sektora u BDP-u. Republika Hrvatska bilježi napredak u promatranim komponentama digitalne transformacije, posebno u dijelu osnovne informatičke pismenosti i dostupnih digitalnih usluga za fizičke i pravne osobe. Zaostaje za prosjekom Europske unije na gotovo svim promatranim parametrima, osim u slučaju osnovne informatičke pismenosti

stanovništva. Istraživanje prikazuje ekonomske koristi digitalizacije, rezultati impliciraju da rast digitalne infrastrukture i digitalnih javnih usluga nužno povlači i potrebu za usmjeravanjem edukacije i opreza prema jačanju sigurnosnih mehanizama, osobno na području privatnih podataka i zaštite digitalnog identiteta. Otpornost na kibernetičke prijetnje postaje značajni idući korak razvoja digitalnog društva. Doprinos ovoga rada je u analizi i prikazu digitalnih politika i ekonomskog učinka te korelaciji između digitalnih politika I BDP-a. Ograničenja prilikom izrade rada je manjak javno dostupnih podataka za duži vremenski period za sve zemlje članice Europske unije, ujedno određeni promatrani indeksi su se počeli promatrati unazad 5-10 godina što čini kratak vremenski period za ozbiljno statističko istraživanje. Buduća istraživanja mogu obuhvatiti razloge zbog kojih ICT sektor ne bilježi značajniji rast kao i broj zainteresiranih mladih osoba za pohađanjem IT studija. Utjecaj umjetne inteligencije će sigurno utjecati na IT sektor, istraživanje može prikazati procjenu hoće li povećati udio BDP-a ili smanjiti.

5. Literatura

Broz, T., Buturac, G., i Parežanin, M. (2020). Digitalna transformacija i gospodarska suradnja: slučaj zemalja zapadnog Balkana. Zbornik radova Ekonomskog fakulteta u Rijeci, 38(2), str. 697-722

De Gregorio, G., (2021). The rise of digital constitutionalism in the European Union. International Journal of Constitutional Law, 19(1), pp.41-70.

Digital strategy portal (2025). https://digital-strategy.ec.europa.eu/en/policies/desi

Economy finance (2025). https://economy-finance.ec.europa.eu/economic-surveillance-eu-economies/croatia/economic-forecast-croatia_en

Europska komisija (2025). https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_hr

Eurostat, (2025). https://ec.europa.eu/eurostat/databrowser/view/isoc_bde15ag/default/table?lang=en

Ivic, S. and Troitiño, D.R., (2022). Digital sovereignty and identity in the European union: A challenge for building Europe. European Studies, 9(2), pp.80-109.

Kraus, S., Jones, P., Kailer, N., Weinmann, A., Chaparro-Banegas, N. and Roig-Tierno, N., (2021). Digital transformation: An overview of the current state of the art of research. Sage Open, 11(3), p.21582440211047576.

Laitsou, E., Kargas, A. and Varoutas, D., (2020). Digital competitiveness in the European Union era: The Greek case. Economies, 8(4), p.85.

Lugavić, Z., i Rožajac, A. (2022). Digitalna transformacija: multidisciplinarno upravljanje promjenama. tranzicija, 25.(50.), str. 43-64.

Milošević, N., Dobrota, M., i Barjaktarović Rakočević, S. (2018). Digitalna ekonomija u Europi: procjena performansi zemalja. Zbornik radova Ekonomskog fakulteta u Rijeci, 36(2), str. 861-880.

Poljanec-Borić, S. (2021). Kvalitativni uvid u obilježja digitalnoga poduzeća, sadržaj i stanje procesa digitalne transformacije u Hrvatskoj. Društvena istraživanja, 30(1), str. 115-134

Statista (2024). https://www.statista.com/statistics/1371887/eu-digitalization-digital-economy-and-society-index-average

Troitiño, D.R., (2022). The European Union Facing the 21st Century: The Digital Revolution. TalTech Journal of European Studies, 12(1).

Turuk, M., Turčić, I., i Stjepić, A. (2022). Analiza indikatora digitalnog poduzetništva na primjeru odabranih članica Europske unije. Zbornik Ekonomskog fakulteta u Zagrebu, 20(1), str. 111-127

Vial, G., (2021). Understanding digital transformation: A review and a research agenda. Managing digital transformation, pp.13-66.

Zaoui, F. and Souissi, N., (2020). Roadmap for digital transformation: A literature review. Procedia Computer Science, 175, pp.621-628.

THE DIGITAL DECADE AND ECONOMIC GROWTH: QUANTIFYING THE BENEFITS OF DIGITAL TRANSFORMATION IN THE EUROPEAN UNION

Abstract: The Digital Decade represents the European Union's policy for the digital decade until 2030, aiming to strengthen the strategic framework for accelerating digital transformation by the end of the decade. This paper will analyze the economic benefits of digital transformation based on key data at the EU level, and specifically investigate the level of digital development in the Republic of Croatia. Using secondary data from the European Commission and Eurostat, the paper will analyze GDP growth, the share of ICT in GDP, and compare these with the level of digital literacy among the population and its impact on the economy. Statistical analysis will be employed to determine if there is a correlation between the level of digitalization and economic growth, as well as Croatia's potential for further growth. The aim of this paper is to establish whether there is a clear link between significant GDP growth, a country's development, and the development of the ICT sector, i.e., the digital literacy of the population.

Keywords: Digital Decade, digital literacy, digital transformation, economic growth, ICT sector

Zaprimljen: 10.6.2025.
Odobren za objavu: 23.7.2025.
Prethodno priopćenje

ANALIZA ZAPOŠLJAVANJA I DOPRINOSA ICT SEKTORA BDP-U EUROPSKE UNIJE I REPUBLIKE HRVATSKE

Matej Galić[1]
[1] Veleučilište "Lavoslav Ružička" u Vukovaru
ePošta: mgalic@vevu.hr

Sažetak: Informacijsko-komunikacijski sektor u današnjoj ekonomiji značajno oblikuje smjer i kretanje gospodarstva. Istražiti će se uloga ICT-a u oblikovanju tržišta rada i doprinos gospodarskom rastu Europske unije i Republike Hrvatske. Glavno istraživanje je fokusirano na broj zaposlenih u ICT sektoru, kretanje zaposlenosti prema vrstama radnih mjesta u ICT-u, ukupan broj zaposlenih i projekcija broja zaposlenih. Sekundarni podaci će se koristiti za detaljnu analizu, uključujući Eurostat, Hrvatski zavod za statistiku i European Centre for the Development of Vocational Training. Primjenom deskriptivne statistike i komparativne analize analizirani su udjeli zaposlenih u ICT sektoru, stope nezaposlenosti po zanimanjima i očekivani rast sektora. Rezultati ukazuju na linearan rast udjela ICT zaposlenih u RH, nisku nezaposlenost ICT profesionalaca te povezanost između projekcija rasta ICT sektora i udjela ICT-a u BDP-u zemalja EU. Cilj je prikazati postoji li jasna korelacija između ekonomskog rasta i razvoja ICT sektora te koje su razlike u zapošljivosti ICT profesionalaca na razini Europske unije.

Ključne riječi: demografski trendovi, gospodarski rast, ICT sektor, tržište rada, zapošljavanje

1. Uvod

Digitalna transformacija predstavlja ključni faktor rasta u modernim gospodarstvima. Povećana potražnja za ICT stručnjacima i viskom razinom digitalnih kompetencija predstavlja izazove za tržište rada diljem Europske Unije. Glavni cilj je utvrditi dinamiku zapošljavanja u ICT sektoru te njegov doprinos BDP-u uz poseban fokus na korelaciju između digitalnog razvoja i gospodarskog rasta. Postavljenje su tri hipoteze:
H1. Udio ICT sektora u ukupnom broju zaposlenih u Republici Hrvatskoj raste linearnim trendom iz godine u godinu.
H2. U zemljama s većim projekcijama rasta ICT sektora do 2035. očekuje se veći udio ICT-a u BDP-u.
H3 Broj nezaposlenih ICT profesionalaca značajno je manji od prosjeka ostalih zanimanja, što ukazuje na visoku razinu zapošljavanja ICT sektora.

Nedostatak stručnjaka obrazovanih u području ICT-a utjecat će na smanjenje konkurentnosti cijelog gospodarstva, smanjenje globalnog inovacijskog potencijala, a to bi moglo započeti degeneraciju našeg stanovništva (Maryska et. al, 2012). Povezujući ovo zapažanje s kontekstom razvoja ICT-a, potražnja za radnicima bez osnovnih ili niskih ICT vještina vjerojatno će se smanjiti. Nekoliko čimbenika, poput ekonomskih šokova ili brzog tehnološkog napretka, moglo bi ubrzati taj proces (Pichler i Stehrer, 2021). Harmonizacija upravljanja informacijama, sustavi za razmjenu informacija, modularizacija, sustavi za ponovnu upotrebu iskustva, pokazatelji učinkovitosti itd. trebali bi se promovirati pokretanjem programa istraživanja i razvoja u području međunarodne standardizacije proizvoda i procesa (Ekholm i Molnar, 2009). Iako se čini da se većina malih i srednjih tvrtki u

području informacijske i komunikacijske tehnologije odlučila za kratkoročna rješenja za nedostatak vještina, poput korištenja privremenih radnika ili outsourcinga, postojao je podskup tvrtki koje su pokazale strateški pristup više razine upravljanja karijerom osmišljen kako bi izgradile jače veze sa zaposlenicima (Scholarios et. al., 2008). Mlada poduzeća koja razvijaju i implementiraju nove proizvode i tehnologije, često ovise o visokoobrazovanoj radnoj snazi i menadžerskim talentima. Taj zahtjev za kvalitetom radne snage ovisan je o sustavu obrazovanja (Kovačević i Vuković, 2006). Tehnološke promjene mogu utjecati na zaposlenost u oba smjera, i na povećanje kapitala i na povećanje rada. Učinak također može biti različit ovisno o komplementarnosti između kapitala i rada (Ju, 2014). Tvrtke koje su uspjele prenijeti svoje aktivnosti i komunikaciju s potrošačima na mrežu, prvenstveno zahvaljujući aktivnom uvođenju informacijsko-komunikacijskih tehnologija, uspjele su održati svoje konkurentske pozicije (Dubyna et. al., 2022). Bez obzira na krizu, broj tvrtki i zaposlenih raste u svim istočnohrvatskim županijama (Sebalj et. al., 2017). Ulaganje na razini EU-28 u dijelove ICT sektora kao što su širenje širokopojasnog interneta, rast e-trgovine i poticanje online aktivnosti povoljno je za gospodarski razvoj. S druge strane, zemlje EU trebale bi početi poticati ljude da ulažu svoje znanje i resurse u vlastite zemlje, tj. da rade u zemlji, kao i da smanje državnu potrošnju na ulaganja u e-usluge ili njihovu prenamjenu, budući da rezultati pokazuju negativne učinke na gospodarski razvoj (Petrić i Šimundić, 2020). Analiza dokazuje da postoji pozitivna veza između e-financija i povezivosti, što znači da u zemljama u kojima su e-financije dosegle razinu koja bi trebala dovesti do bržeg rasta, razina povezivosti čini se da objašnjava točku uzleta (Shamim, 2007). ICT sektor, osobito segment koji proizvodi ICT usluge, ukazuju na potencijal koji bi mogao imati efekte na ekonomski rast i rast produktivnosti u hrvatskom gospodarstvu (Kovačević i Vuković, 2007). Strukturne i dinamičke osobitosti ICT industrija u Hrvatskoj pokazuju heterogenost ICT sektora. Heterogenost je utvrđena promatranjem sljedećih karakteristika industrija: distribucije poduzeća i distribucije zaposlenih u poduzećima različitih kategorija veličine, tržišnih udjela (s pomoću ukupnih prihoda), produktivnosti, profita i profitnih stopa, ulaznih barijera (intenzivnost kapitalom i minimalna efikasna veličina poduzeća), preživljavanja poduzeća (Kovačević i Vuković, 2006). Transformacijsko vodstvo od posebne je važnosti u djelatnostima koje karakterizira kompleksnost i visoka dinamika promjena, posebno tehnoloških, a što je značajno za IT sektor (Rupčić i Milisavljević, 2022). Uloga ICT-a u društvenom životu zemalja EU-a u budućnosti će se povećavati. To je posljedica kako objektivnih razloga povezanih s globalnim procesima tehnološkog napretka, tako i provedbe ekonomskih pretpostavki EU-a, prema kojima bi ona postala najinovativnije područje na svijetu (Postula et. al., 2021). Važno je razviti skup mjera koje će zaposlenici prepoznati i koje su izravno motivirane na bolju suradnju s drugim zaposlenicima, ali i na opću izgradnju kulture podrške, motivacije i poboljšanja poslovanja među zaposlenicima (Galić et. al., 2021). Argumenti u raspravi o kapitalno intenzivnoj naspram radno intenzivne proizvodnje su očiti: u raspravi o kapitalno intenzivnoj naspram radno intenzivne proizvodnje, kapitalno intenzivna proizvodnja ima prednosti u smanjenju rizika od gubitka posla i nezaposlenosti zbog utjecaja digitalnog restrukturiranja na poslu (Krutova et. al., 2022).

2. Metodologija

Za potrebe istraživanja je korišten kvantitativni pristup temeljen na analizi sekundarnih podataka prikupljenih iz

relevantnih europskih (Eurostat, Cedefop) i nacionalnog izvora (Državni zavod za statistiku Republike Hrvatske). Podaci se odnose na razdoblje 2019.-2024. godina. Primarni cilj istraživanja bio je utvrditi dinamiku zapošljavanja u ICT sektoru te njegov doprinos u BDP-u Europske unije i Republike Hrvatske. Naglasak je stavljen na istraživanje međuovisnosti između rasta ICT sektora, zapošljivosti i ekonomskih indikatora. Korištene su komparativne analize i analize trendova dostupnih podataka deskriptivnom statistikom. Istraživanje nije obuhvatilo mikroekonomsku analizu, fokusira se na trendove na razini makroekonomije. Ograničenja prilikom istraživanja su prisutna uslijed različitih vremenskih raspona podataka po zemljama i varijablama, ograničena dostupnost podataka po zemljama te manjak dugoročnosti podataka (nedostatak podataka za duži vremenski period - 20 godina). Za potrebe analize podataka i izradu vizualnih elemenata korišten je MS Excel.

3. Rezultati i rasprava

Razumijevanje pozicije i značaja u ICT sektora unutar gospodarstva Europske unije i Republike Hrvatske je prikazano kroz tablicu 1. koja kroz detaljnu analizu pokazuje broj kretanja ukupnog broja zaposlenika te se prikazuje usporedba s ICT sektorom. Jasan je uvid razvojnih trendova i specifičnosti tržišta rada koji se detaljnije analiziraju i u ostalim tablicama u radu.

Tablica 1 . Kretanja ukupnog broja zaposlenih u RH i prikaz udjela ICT sektora

Godina	Ukupan broj zaposlenih	ICT sektor	Udio ICT %	% promjena	% rast broja zaposlenih
2024	1.476.819	59.625	4,04%	-0,03%	3,91%
2023	1.421.296	57.786	4,07%	0,17%	2,42%
2022	1.387.654	54.042	3,89%	0,37%	3,60%
2021	1.339.431	47.271	3,53%	0,14%	3,14%
2020	1.298.611	43.962	3,39%	Nema podataka	Nema podataka

Izvor: Državni zavod za statistiku, 2025

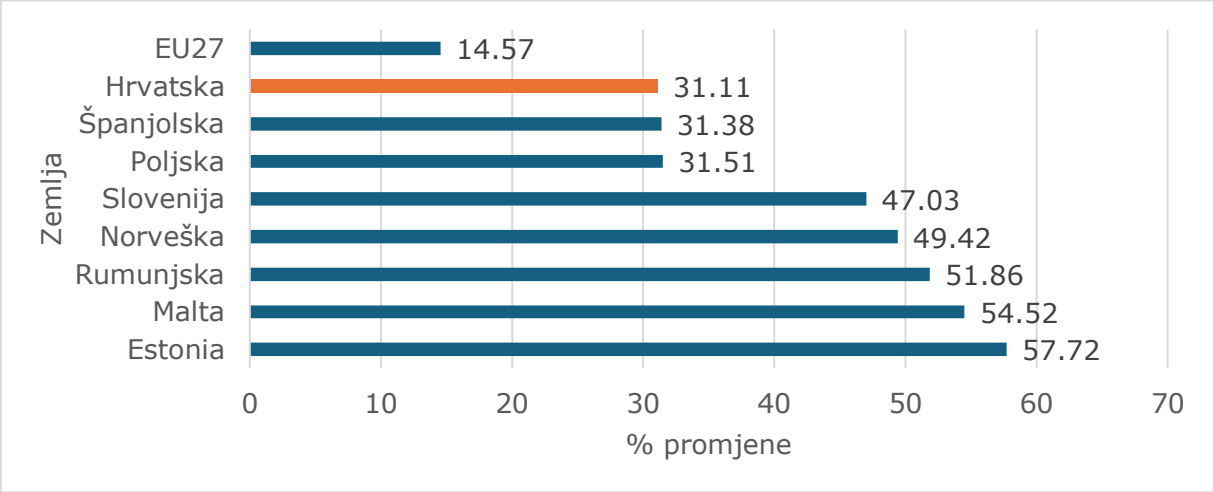
Udio zaposlenih u ICT sektoru raste s 3,39 % u 2020. godini na 4,07 % u 2023. te 4,04 % u 2024. godini. Unatoč blagom smanjenju udjela u 2024. u odnosu na prethodnu godinu (−0,03 %), apsolutni broj ICT zaposlenih i dalje bilježi rast. Ovo smanjenje relativnog udjela posljedica je intenzivnijeg zapošljavanja u ostalim gospodarskim sektorima. Rast ICT sektora u apsolutnim brojkama (od 43.962 na 59.625 zaposlenih) iznosi 35,63 %, što potvrđuje hipotezu H1: Udio ICT sektora u ukupnom broju zaposlenih u Republici Hrvatskoj raste linearnim trendom iz godine u godinu. Potvrđuje se pozitivna dinamika udjela ICT sektora, što pokazuje sve veću važnost na tržištu rada Republike Hrvatske. Tablica 2. prikazuje postotak nezaposlenih osoba prema zanimanjima, uspoređuju se najzastupljenija zanimanja te ICT sektor.

Tablica 2 . Nezaposleni prema zanimanjima u EU – top 5 najzastupljenijih i usporedba s ICT sektorom (%)

Radna mjesta	2020	2021	2022	2023
Radnici u poljoprivredi	19,29	10,88	10,06	9,14
Tehnički radnici	10,35	7,71	6,36	7,53
Ugostiteljstvo	14,82	8,84	7,55	7,03
Jednostavna zanimanja	10,47	7,59	6,4	6,55
Ostala jednostavna zanimanja	8,65	7,53	6,32	6,15
ICT profesionalci	1,59	1,23	1,14	1,37

Izvor: Cedefop, 2025

Prikazana je raspodjela nezaposlenih prema radnim mjestima u razdoblju 2020. – 2023. godine, u ovome slučaju je fokus na usporedbu s ICT profesionalcima. Zbog velike količine podataka i skupina, odabrano je top 5 zanimanja. U svim promatranim skupinama zanimanja se vidi jasan pad nezaposlenih osoba, u ICT se broj zaposlenih kreće od 1,59% u 2020. godini te dolazi do pada na 1,37% u 2023. godini. Postotak nezaposlenosti u top 5 zanimanja je višestruko veći u odnosu na ICT sektor. Dobiveni podaci potvrđuju Hipotezu 3 (H3): Broj nezaposlenih ICT profesionalaca značajno je manji od prosjeka ostalih zanimanja, što ukazuje na visoku zapošljivost u ICT sektoru. Slika 1. prikazuje postotnu procjenu budućeg rasta ICT sektora u razdoblju 2022-2035.



Slika 1. Procjena budućeg rasta iCT sektora 2022-2035

Izvor: Cedefop, 2025

Najveći očekivani rast bilježe Estonija (57,72%), Malta (54,52%) i Rumunjska (51,86%), Republika Hrvatska se nalazi na 31,11% što je znatno iznad prosjeka Eu27 (14,57%). Takva pozicija Republike Hrvatske sugerira da digitalna strategija pridonosi pozitivnim očekivanjima rasta u ICT sektoru. Kombiniranjem podataka u Grafu 1. i podataka iz Tablice 3. moguće je testirati Hipotezu 2 (H2): U zemljama s većim projekcijama rasta ICT sektora do 2035. očekuje se veći udio ICT-a u BDP-u. Primjećuje se da zemljama s visokim projekcijama rasta, poput Malte i Estonije, imaju i relativno visoke udjele ICT sektora u BDP-u. Tablica 3. prikazuje udio ICT sektora u ukupnom BDP-u i projekciju rasta za 2026. godinu.

Tablica 3 . Udio ICT sektora u ukupnom BDP-u i očekivani rast u 2026. u %

Zemlja	2019	2020	2021	2022	Očekivani rast BDP 2026
Irska	-	-	-	34,78	2,50
Malta	-	7,43	9,89	10,14	0,40
Bugarska	6,65	7,34	7,43	7,42	2,10
Latvija	5,57	5,92	6,36	6,45	2,00
Švedska	6,51	7,12	:	6,24	1,90
Estonija	5,81	6,72	5,77	5,97	2,30
Finska	4,98	5,89	:	5,81	1,30
Mađarska	6,08	5,95	5,76	5,48	2,50

EU - 27	4,86	5,19	5,46	5,46	1,50
Hrvatska	4,52	5,02	5,31	5,32	2,90

Izvor: Eurostat, 2025, Economy finance Europa, 2025

Irska se ističe s izuzetno visokim udjelom ICT-a u udjelu BDP-a (2022. godina – 34,78%), posljedica je koncentracija ICT korporacija na njezinom teritoriju. Malta (2022. godina – 10,14%), Bugarska (2022. godina – 7,42%), Latvija (2022. godina – 6,45%) i Estonija (2022. godina – 5,97%) također bilježe značajne iznadprosječne udjele, ukoliko usporedimo s EU 27 – 5,46%. Republika Hrvatska zaostaje za prosjekom EU27, odnosno bilježi postotak u 2022.godini 5,32%. Može se potvrditi da postoji pozitivna veza između očekivanog rasta ICT sektora i njegova gospodarskog doprinosa. Ekonomije s razvijenijim digitalnim gospodarstvom imaju veću šansu za rastom ICT sektora i u budućnosti.

4. Zaključak

Istraživanjem provedeno u ovome radu pokazuje značajan utjecaj informacijsko-komunikacijskog (ICT) sektora na tržište rada i BDP, na razini Europske unije, ali i na razini Republike Hrvatske. Analiza vremenskih podataka pokazuje stabilan i pristupan rast udjela zaposlenih u ICT sektoru u Republici Hrvatskoj, čime se potvrđuje H1 hipoteza. Usporedba nezaposlenosti po zanimanjima pokazala je da ICT profesionalci čine znatno manji udio među nezaposlenima u odnosu na ostala zanimanja te se potvrdila hipoteza H3. Usporedba projekcija rasta ICT sektora i udjela ICT sektora u BDP-u bilježi iznadprosječne projekcije rasta što je pokazatelj potencijala za daljnje jačanje sektora. Identificirani trendovi pozivaju na nužnost strateškog ulaganja u obrazovne politike, razvoj digitalnog gospodarstva i kompetencija i tehnoloških ulaganja. ICT sektor pokazuje potencijal da postane ključan nositelj konkurentnosti i otpornosti na području digitalne tranzicije. Buduća istraživanja mogu obuhvatiti analizu digitalizacije na produktivnost i poslovne rezultate ICT poduzeća u Republici Hrvatskoj te regionalne razlike te utjecaj na lokalni razvoj.

5. Literatura

Boban, M. i Babić, A. (2014). Utjecaj internetskih tehnologija na gospodarski rast, poslovni rezultat i stopu rasta profita poduzeća u republici hrvatskoj. Elektronički zbornik radova Veleučilišta u Šibeniku, 8 (1-2), 59-82

Cedefop (2024). https://www.cedefop.europa.eu/en/tools/skills-intelligence/sectors?sector=05.10#1
Državni zavod za statistiku (2024). https://podaci.dzs.hr/

Dubyna, M., Kholiavko, N., Zhavoronok, A., Safonov, Y., Krylov, D. E. N. Y. S., & Tochylina, Y. (2022). The ICT sector in economic development of the countries of Eastern Europe: a comparative analysis.

Economy finance Europa (2025), https://economy-finance.ec.europa.eu/economic-forecast-and-surveys/economic-forecasts/spring-2025-economic-forecast-moderate-growth-amid-global-economic-uncertainty_en

Ekholm, A., & Molnar, M. (2009). ICT development strategies for industrialisation of the building sector. Journal of Information Technology in Construction (ITcon), 14(28), 429-444.

Eurostat (2024), https://ec.europa.eu/eurostat/databrowser/view/isoc_bde15ag/default/table?lang=en

Galić, M., Mrvica Mađarac, S., Horvat, T. (2021). The importance of cross-functional cooperation for business growth on the example of a large

agricultural enterprise. Međunarodni znanstveni simpozij Gospodarstvo istočne Hrvatske – jučer, danas, sutra, 728-743

Ju, J. (2014). The effects of technological change on employment: The role of ICT. Korea and the World Economy, 15(2), 289-307.

Kovačević, Z. i Vuković, K. (2006). Performanse poduzeća u hrvatskom sektoru informacijsko-komunikacijske tehnologije (ict). Ekonomska misao i praksa, 15 (2), 217-240.

Kovačević, Z. i Vuković, K. (2007). Industrija informacijsko-komunikacijske tehnologije (ict) u hrvatskom gospodarstvu. Poslovna izvrsnost, 1 (1), 97-112.

Krutova, O., Koistinen, P., Turja, T., Melin, H., & Särkikoski, T. (2022). Two sides, but not of the same coin: digitalization, productivity and unemployment. International Journal of Productivity and Performance Management, 71(8), 3507-3533.

Maryska, M., Doucek, P., & Kunstova, R. (2012). The importance of ICT sector and ICT university education for the economic development. Procedia-Social and Behavioral Sciences, 55, 1060-1068.

Petrić, M., Garbin Praničević, D., & Šimundić, B. (2020). Impact of ICT sector deployment on the economic development of the European Union. In FEB Zagreb 11th International Odyssey Conference on Economics and Business (pp. 491-503). University of Zagreb, Faculty of Economics & Business.

Pichler, D., & Stehrer, R. (2021). Breaking through the digital ceiling: ICT skills and labour market opportunities (No. 193). WIIW Working Paper.

Postuła, M., Chmielewski, W., Puczyński, P., & Cieślik, R. (2021). The impact of information and communication technologies (ICT) on energy poverty and unemployment in selected European Union countries. Energies, 14(19), 6110.

Rupčić, N. i Milisavljević, E. (2022). Transformacijsko vodstvo u IT sektoru. ET²eR – ekonomija, turizam, telekomunikacije i računarstvo, 4 (2), 18-25.

Scholarios, D., Van der Heijden, B. I., Van der Schoot, E., Bozionelos, N., Epitropaki, O., Jedrzejowicz, P., ... & Van der Heijde, C. M. (2008). Employability and the psychological contract in European ICT sector SMEs. The International Journal of Human Resource Management, 19(6), 1035-1055.

Sebalj, D., Mesaric, J., & Franjkovic, J. (2017). Research of development and growth perspectives of the local ICT sector. Economic and Social Development: Book of Proceedings, 29-38.

Sein, M. K., & Harindranath, G. (2004). Conceptualizing the ICT artifact: Toward understanding the role of ICT in national development. The information society, 20(1), 15-24.

Shamim, F. (2007). The ICT environment, financial sector and economic growth: a cross-country analysis. Journal of economic studies, 34(4), 352-370.

ANALYSIS OF EMPLOYMENT AND ICT SECTOR CONTRIBUTION TO GDP IN THE EUROPEAN UNION AND THE REPUBLIC OF CROATIA

Abstract: The information and communication technology (ICT) sector significantly shapes the direction and movement of the economy today. This paper will investigate the role of ICT in shaping the labor market and its contribution to economic growth in the European Union and the Republic of Croatia. The primary research focuses on the number of people employed in the ICT sector, employment trends by type of ICT job, the total number of employed, and employment projections. Secondary data will be used for a detailed analysis, including sources from Eurostat, the Croatian Bureau of Statistics, and the European Centre for the Development of Vocational Training. Using descriptive statistics and comparative analysis, the paper analyzes the share of employed persons in the ICT sector, unemployment rates by occupation, and the expected growth of the sector. The results indicate a linear growth in the share of ICT employees in Croatia, low unemployment among ICT professionals, and a correlation between ICT sector growth projections and the share of ICT in the GDP of EU countries. The aim is to demonstrate whether there is a clear correlation between economic growth and the development of the ICT sector, and to highlight the differences in the employability of ICT professionals across the European Union.

Keywords: demographic trends, economic growth, ICT sector, labor market, employment

Zaprimljen: 10.6.2025.
Odobren za objavu: 23.7.2025.
Prethodno priopćenje

ETIČNOST NA DRUŠTVENIM MREŽAMA

Anita Kulaš Mirosavljević[1], Nikolina Matić[2], Branka Martić[3]
[1] Sveučilište u Slavonskom Brodu, Trg I. B. Mažuranić 2, 35000 Slavonski Brod, Hrvatska
ePošta: akmirosavljevic@unisb.hr
[1] Sveučilište u Slavonskom Brodu, Trg I. B. Mažuranić 2, 35000 Slavonski Brod, Hrvatska
ePošta: nmatic@unisb.hr
[3]Služba za unutarnju reviziju, Brodsko-posavska županija, Petra Krešimira IV 1, 35000 Slavonski Brod, Hrvatska
ePošta: branka.martic2@gmail.com

Sažetak: Društvene mreže su postale dio suvremenog života, način na koji se danas komunicira, dijele informacije i formiraju odnosi. Svrha i cilj rada je istražiti utjecaj društvenih mreža na etičke norme te na koji način iste oblikuju ponašanje i stavove pojedinaca. Stoga je nužna analiza etičkih dilema koje se pojavljuju prilikom korištenja društvenih mreža, kao što su pitanje privatnosti, širenje dezinformacija, govor mržnje i cyberbullying. U kontekstu etičkog ponašanja na društvenim mrežama posebna pažnja je posvećena ulozi kibernetičke sigurnosti. U radu su korištene deskriptivna metoda, kvantitativna metoda, induktivna metoda, anketa i metoda analiza i sinteze. Rezultati istraživanja kojima je cilj bio ispitati utjecaj društvenih mreža na etičke norme s naglaskom na ulogu kibernetičke sigunosti pokazali su raznolike rezultate. U prosjeku ispitanici se nisu susreli sa povredom osobnih podataka, ali niti jesu niti nisu uvjereni u prepoznavanje pokušaja prevare na Internetu te nisu sigurni u svoju informiranost o kibernetičkoj sigurnosti. Rad je doprinio saznanju da se ljudi trebaju dodatno educirati o važnosti kibernetičke sigurnosti kako bi znali prepoznati prijetnje s kojima će se nekada susresti.

Ključne riječi: društvene mreže, etika, kibernetička sigurnost

1. Uvod

Društvene mreže transformirale su način za komunikaciju, zabavu i posao postavši nezaobilaznim dijelom svakodnevice ljudi diljem svijeta. Sveprisutnost i dinamičan razvoj društvenih mreža nameće pitanja koja zadiru duboko u tkivo društvenih odnosa, etičkih normi i kulturnih vrijednosti nadilazeći svoje tehnološke aspekte. Etičke norme, kao pisana i/ili nepisana pravila usmjeravaju ponašanje ljudi prema onome što se smatra ispravnim unutar određene zajednice. Neki od fenomena vezanih uz društvene mreže koji (in)direktno utječu na primjenu etičkih načela i njihovu percepciju su globalni doseg, mogućnost anonimnosti, stvaranje virtualnih zajednica te brzina širenja. Ovaj rad[1] bavi se kompleksnim i višeslojnim odnosom između etičkih normi i društvenih mreža. Osnovno istraživačko pitanje jest percepcija utjecaja društvenih mreža na etičke norme korisnika. Polazi se od pretpostavke da se radi o dinamičkoj interakciji, a ne jednosmjernom utjecaju. Ta dinamika omogućuje da društvene mreže postanu moćan instrument koji će oblikovati i mijenjati već uspostavljene etičke standarde.

[1] Diplomski rad „Utjecaj društvenih mreža na etičke norme", studentica Nikolina Matić, mentor doc. dr. sc. Anita Kulaš Mirosavljević, 17.6.2025., SDS Menadžment, ODHZ, Sveučilište u Slavonskom Brodu

Cilj rada je višestruk: (1) odrediti ključne pojmove kao što su društvene mreže, etika i etičke norme, (2) razmotriti kako postojeće etičke norme usmjeravaju ponašanje pojedinaca u online okruženju te (3) analizirati načine na koje društvene mreže utječu na etička pitanja (sigurnost, istinitost informacija, privatnost, međuljudski odnosi, govor mržnje). Pored toga, posebna pažnja bit će posvećena problemu kibernetičke sigurnosti.

2. Metodologija

U svrhu empirijske obrade rada provedeno je anketno istraživanje o utjecaju društvenih mreža na etičke norme. Nedostatak anketnog istraživanja je kako dobivene rezultate uzorka preslikati na populaciju, ali dobiveni zaključci na temelju uzorka mogu indikativno pokazati realno stanje istraživačkog problema. Temeljni problem rada bio je istražiti utjecaj društvenih mreža na etičke norme te koliko društvene mreže mogu utjecati na promjene etičkih vrijednosti. U anketnom istraživanju primijenjene su tri metode: (1) kvantitativna metoda istraživanja na temelju koje se ispitanike strukturirano ispitivalo putem anketnog upitnika, (2) metoda nezavisnog induktivnog zaključivanja na temelju koje su dobiveni zaključci te (3) metoda analize i sinteze na temelju koje su se povezale teorijske odrednice i provjerili dobiveni rezultati u praksi. Konačno, u istraživanju je primijenjena metoda prikupljanja podataka koji predstavljaju primarne podatke o obradi i donošenju zaključaka ankete, a iste predstavljaju mišljenja ispitanika.

3. Pojmovno određenje društvenih mreža i etike

Društvene mreže su digitalni komunikacijski alati koji svojim korisnicima omogućuju dijeljenje i stvaranje različitih vrsta sadržaja, izražavanje mišljenja, povezivanje s drugim korisnicima i interakciju u stvarnom vremenu (Cadushin, 2011). Društvene mreže djeluju kao virtualne zajednice gdje organizacije i pojedinci dijele informacije, izgrađuju svoj identitet i formiraju društvene odnose, neovisno o međusobnoj fizičkoj udaljenosti (Borgatti, 2014). Popularnost platformi ovisi o demografskim skupinama poput dobi, spola i interesa korisnika te njihovom geografskom području. Platforme poput WhatsAppa, Facebooka, YouTubea i Instagrama broje na milijarde aktivnih korisnika (Boyd & Ellison, 2017). U Hrvatskoj je na prvome mjestu YouTube (početkom 2025. imao oko 2,68 milijuna korisnika, a Facebook oko 1,85 milijuna korisnika, Instagram oko 1,40 milijuna korisnika, TikTok oko 1,12 milijuna korisnika u dobi od 18 i više godina, LinkedIn oko 1,10 milijuna „članova", Messenger oko 1,30 milijuna korisnika, Snapchat oko 645 tisuća korisnika, X oko 419 tisuća korisnika (Digital 2025: Croatia). No, prema dostupnim podacima sa Facebook-a, on je i dalje jedna od najkorištenijih platformi, a slijede ga Instagram, YouTube, WhatsApp i Viber, iako i TikTok bilježi značajan rast popularnosti posebno među mlađom populacijom (Facebook, 2025).

Razumijevanje popularnosti i specifičnosti pojedinih platformi smatra se ključnim za analizu njihovog utjecaja na etičke norme. Naime, različite platforme potiču različite oblike ponašanja te otvaraju specifične etičke dileme.

Kako bi se analizirala povezanost društvenih mreža i etičkih normi, najprije je potrebno definirati temeljne pojmove etike i etičkih normi, ali i razumjeti njihovu ulogu unutar društva. Etika je filozofska disciplina koja se bavi proučavanjem morala, moralnih načela, vrijednosti i sudova (Bebek & Kolumbić, 2005). Etičke norme su standardi ponašanja i/ili pravila koji proizlaze iz moralnih načela i vrijednosti. One određuju što se unutar neke zajednice, odnosno kulture smatra poželjnim, prihvatljivim ili obvezujućim

ponašanjem. Uloga etičkih normi je ključna za funkcioniranje društva, odnosno regulaciju ponašanja, očuvanje društvenog poretka, zaštitu temeljnih vrijednosti, promicanje općeg dobra, izgradnja povjerenja te formiranje identiteta (Vuksanović, 1993). Etičke norme nisu statične, mijenjaju se tijekom vremena pod utjecajem kulturnih, ekonomskih, društvenih i tehnoloških promjena. Pojava novih tehnologija, među njima i društvenih mreža, često preispituje postojeće etičke norme i traži stvaranje novih.

4. Povezanost društvenih mreža sa etičkim normama

Društvene mreže isprepletene su s etičkim normama te na taj način stvaraju složen međuodnos u kojem se istovremeno oblikuju i bivaju oblikovane postojeće norme. One su aktivni prostori koji omogućuju testiranje, preispitivanje, jačanje, a ponekad i narušavanje postojećih etičkih normi.

4.1. Prednosti i izazovi učinaka društvenih mreža na etičke norme

Iako su često pod kritikama, društvene mreže imaju potencijal za promicanje etičkih vrijednosti i pozitivnih društvenih promjena (Vuksanović, 1993):

Podizanje svijesti i društveni aktivizam

Platforme kao što su Facebook i Instagram postale su moćni alati za podizanje svijesti o ekološkim, političkim i socijalnim problemima. Globalni pokreti pokazali su kako se putem društvenih mreža mogu mobilizirati mase, organizirati prosvjedi i zahtijevati društvena pravda i odgovornost. Na taj se način jačaju etičke norme građanske participacije i odgovornosti.

Promicanje transparentnosti i odgovornosti

Društvene mreže su postale mjesto gdje pojedinci izvještavaju i dokumentiraju o nastalim događajima u stvarnom vremenu te na taj način povećavaju transparentnost rada institucija i korporacija, tzv. „građansko novinarstvo".

Solidarnost i humanitarni rad

Društvene mreže u kriznim situacijama služe za brzo širenje informacija, organiziranje pomoći i prikupljanje sredstava za ugrožene. Kao primjeri, mogu se navesti kampanje grupnog financiranja (*crowdfunding*) za liječenje bolesnih ili pomoć siromašnima.

Naravno, društvene mreže stvaraju i etičke izazove koji mogu negativno utjecati na postojeće norme (Vuksanović, 1993):

Širenje dezinformacija i lažnih vijesti

Brzina širenja informacija putem društvenih mreža omogućuje masovno širenje dezinformacija, lažnih vijesti i teorija zavjere. Na taj se način narušava istinitost etičkih normi, potkopava se povjerenje u medije i institucije i može dovesti do ozbiljnih posljedica na javno zdravlje, političke procese i društvenu stabilnost.

Govor mržnje, online nasilje (cyberbullying) i toksičnost

Nedostatak izravne fizičke interakcije i relativna anonimnost na društvenim mrežama može dovesti do smanjivanja inhibicije te porasta prijetnji, uvredljivih komentara, govora mržnje i sustavnog online zlostavljanja. To direktno krši etičke norme nenasilja i poštovanja dostojanstva osobe.

Erozija privatnosti

Poslovni modeli društvenih mreža često se temelje na prikupljanju i analizi osobnih podataka korisnika bez njihovog razumijevanja ili svjesnog pristanka. Ovo otvara pitanja o pravu na privatnost, nadzoru i mogućoj zlouporabi podataka.

Stvaranje nerealnih standarda i utjecaj na mentalno zdravlje

Vrlo često se na društvenim mrežama promiču nerealne slike života, izgleda i uspjeha. To može dovesti do stvaranja još većih razlika između pojedinaca jer se isti često uspoređuju te na taj način dolazi do smanjenja samopoštovanja, anksioznosti, depresije i poremećaja slike o vlastitom tijelu.

4.2. Kibernetička sigurnost

Pod kibernetičkom sigurnosti na društvenim mrežama smatra se zaštita informacijskih sustava, podataka i mreža od neovlaštenog pristupa, otkrivanja, izmjene, korištenja ili uništenja. Kibernetička sigurnost je neraskidivo povezana s etičnosti na društvenim mrežama. Etički izazovi u području kibernetičke sigurnosti na društvenim mrežama su (Hlača, 2018):

Privatnost i nadzor podataka

Prikupljanje i korištenje osobnih podataka

Društvene mreže prikupljaju velike količine osobnih podataka poput osnovnih identifikacijskih informacija, biometrijskih podataka do detalja o interesima, komunikaciji, navikama i lokaciji korisnika. Postavlja se etičko pitanje vlasništva nad podacima koji se prikupljaju, obrađuju, koriste i čuvaju.

Nadzor

Nadzor od strane državnih agencija, samih platformi i/ili trećih strana (npr. poslodavaca) postavlja etičko pitanje o granicama dopuštenog nadzora.

Sigurnost podataka i povrede sigurnosti

Društvene platforme imaju etičku, a često i zakonsku obvezu adekvatne zaštite osobnih podataka korisnika od neovlaštenog pristupa, krađe ili curenja. Neadekvatne sigurnosne mjere mogu dovesti do ozbiljnih posljedica za korisnika (financijski gubici, krađa identiteta, narušavanje reputacije).

Dezinformacije, manipulacija i zlonamjerni akteri

Putem lažnih profila, botova i koordiniranih kampanja na društvenim mrežama (ne)državni akteri šire dezinformacije, propagande i operacije utjecaja. Na taj način mogu utjecati na izborne procese, destabilizirati društvo i narušiti povjerenje.

Cyberbullying, online uznemiravanje i eksploatacija

Cyberbullying, online uznemiravanje i eksploatacija imaju i kibernetičko-sigurnosnu dimenziju iako su širi etički problem. Društvene mreže trebaju osigurati mehanizme za prijavu i uklanjanje sadržaja koji su neetični poput zlostavljanja, prijetnji, ucjena ili seksualne eksploatacije.

Odgovornost društvenih mreža naspram odgovornosti korisnika

Društvene mreže imaju odgovornost dizajnirati sigurne sustave, postaviti jasna pravila korištenja, transparentno upravljati podacima i moderirati sadržaj. Istovremeno, korisnici nose dio odgovornosti za vlastitu kibernetičku sigurnost putem korištenja jakih lozinki, prepoznavanja phishing napada, opreza pri dijeljenju osobnih informacija, ali i za etično ponašanje prema drugima. Ključno je educirati korisnike o sigurnosnim rizicima i etičkom ponašanju na društvenim mrežama.

Sigurnosne ranjivosti softvera i infrastrukture

Društvene mreže imaju etičku obvezu da kontinuirano rade na identificiranju i otklanjanju sigurnosnih propusta u svom softveru i infrastrukturi kako ne bi došlo do njihovog zlonamjernog iskorištavanja. Kibernetička sigurnost na društvenim mrežama nije samo tehničko već i temeljno etičko pitanje koje zahtijeva stvaranje balansa između poslovnih interesa, inovacija, općeg društvenog dobra i korisničkih prava. Nedostatak pažnje može dovesti do smanjenja povjerenja, povećanja ranjivosti korisnika i negativnih društvenih posljedica (Hlača, 2018).

5. Rezultati empirijskog istraživanja

Društvene mreže postale su dio svakodnevice u suvremenom digitalnom okruženju te na taj način oblikuju načine na koje ljudi komuniciraju, informiraju se i izražavaju. Kako imaju snažan utjecaj na međuljudske odnose i ponašanje ljudi, otvorilo se pitanje utjecaja društvenih mreža na etičke norme. U tu svrhu autori su proveli anketno istraživanje na uzorku od 232 ispitanika. Cilj istraživanja bio je utvrditi koliko su korisnici društvenih mreža svjesni opasnosti cyberbullyinga, povrede privatnosti i kibernetičkih prijetnji, prepoznaju li etičke izazove

digitalne komunikacije i kako gledaju na etičke norme koje se promoviraju na društvenim mrežama.
U provedenoj anketi sudjelovalo je 55,2 % žena i 44,8 % muškaraca. Oko 70 % ispitanika je u dobi između 25 i 54 godina. Ove skupine predstavljaju ključnu populaciju kada se analiziraju stavovi utjecaja društvenih mreža na etičke norme jer su obično profesionalno aktivne te su često izložene različitim društvenim i digitalnim utjecajima. Većina ispitanika su zaposlene osobe što pokazuje da se rezultati istraživanja temelje primarno na radno aktivnoj populaciji. No, pored njih uključene su i druge skupine te se na taj način postiže veća širina u razumijevanju utjecaja društvenih mreža na etičke norme.
Većina sudionika ne promatra društvene mreže kao prostor za promicanje etičkih vrijednosti. Unatoč tome što postoji znatan broj neutralnih odgovora, udio onih koji se slažu s tvrdnjom značajno je manji u odnosu na one koji se ne slažu. To vodi do zaključka da ispitanici na društvene mreže najčešće gledaju kao na prostor konflikata, površne komunikacije i etičkih izazova, a ne kao na alat za širenje tolerancije, poštovanja i odgovornosti. Takvi rezultati dodatno naglašavaju potrebu za obrazovanjem korisnika, ali i aktivniju ulogu platformi u promicanju pozitivnih vrijednosti.
Većina ispitanika doživljava digitalni nadzor kao zadiranje u privatnost i smatra da to nije u skladu s etičkim normama. Takvi stavovi proizlaze iz nepovjerenja prema poslodavcu ili osjećaja ugrožene autonomije na radnom mjestu.
Iako 16,4 % ispitanika prepoznaje promjenu u ponašanju pod utjecajem društvenih mreža, većina ne prepoznaje. Takvi rezultati stvaraju prostor za daljnja kvalitativna istraživanja koja bi istražila načine kako društvene mreže oblikuju samopouzdanje, izražavanje mišljenja, komunikaciju i donošenje odluka.
Oko 42 % ispitanika se osjeća dovoljno informirano o najčešćim vrstama kibernetičkih prijetnji dok je oko 39 % ispitanika neutralno, a to može sugerirati neodlučnost ili nedostatak samopouzdanja u znanje o kibernetičkoj sigurnosti.
Iako većina ispitanika (52,6 %) pokazuje samopouzdanje u prepoznavanju kibernetičkih prijetnji, dobiveni rezultati naglašavaju potrebu za kontinuiranim provođenjem edukacija korisnika. Na taj bi se način osnažila njihova praktična sposobnost reagiranja na prijetnje u digitalnom okruženju.
Oko 60 % ispitanika smatra da u određenoj mjeri primjenjuju dobre prakse kibernetičke sigurnosti, dok ih manje od 16% to otvoreno negira.

4. Zaključak

Društvene mreže su u potpunosti promijenile način komunikacije te postale neizostavnim dijelom svakodnevnog života ljudi diljem svijeta. Njihova sveprisutnost i dinamičan razvoj nametnula su brojna pitanja nadilazeći tehnološke aspekte te zadirući duboko u tkivo društvenih odnosa i etičkih normi. Stoga se etičke norme svakodnevno nalaze pred novim izazovima digitalnog doba. Provedeno istraživanja temelji se na višeslojnim i složenim odnosima između društvenih mreža i etičkih normi. Polazi se od pretpostavke da je utjecaj društvenih mreža i etičkih normi u dinamičkoj interakciji.
Većina ispitanika ocjenjuje etičke norme koje se promoviraju na društvenim mrežama kao slabe ili srednje vrijednosti. Dok relativno mali broj ispitanika smatra da etičke norme pozitivno utječu na njihov osobni etički sustav. Veliki broj ispitanika smatra da društvene mreže nisu promijenile njihovo ponašanje i da ne utječu na njihova etička uvjerenja, ali to može značiti da nisu svjesni utjecaja društvenih mreža na njih te nedostatak samorefleksije. Znatan postotak pokazuje nesigurnost ili neutralnost u svoju sposobnost prepoznavanja digitalnih prijetnji. Oko 50 % ispitanika smatra da nije dovoljno informirano o najčešćim vrstama kibernetičkih prijetnji.

Postoji etički jaz između potencijala i prakse društvenih mreža. Prema tome, preporuča se uvođenje edukativnih sadržaja ili programa o etičkom ponašanju na internetu u škole i fakultete te kroz javne kampanje. Društvene mreže također bi trebale preuzeti veću odgovornost u moderiranju sadržaja koji se objavljuju, isticanju pozitivnih, obrazovnih i solidarnih sadržaja, suzbijanju govora mržnje, širenju dezinformacija, jasnom definiranju pravila ponašanja i sankcioniranju neetičnog ponašanja.
Kako bi se dublje razumio kompleksan utjecaj društvenih mreža na razvoj etičkih normi i moralno ponašanje, u buduća istraživanja bi trebalo uključiti različite pristupe (dubinski intervjui, kvalitativne metode, longitudinalne analize).

5. Literatura

Bebek, B., Kolumbić, A. (2005): Poslovna etika, Sinergija nakladništvo d.o.o., Zagreb.

Borgatti, S. (2014): Analyzing Social Networks, SAGE Publishing, London, UK.

Boyd, D., Ellison, N. (2017). Social Network Sites: Definition, History, and Scholarship, Journal of Computer-Mediated Communication, Vol. 13, No. 1, str. 210 –230

Cadushin, C. (2011): Understanding Social Networks: Theories, Concepts, and Findings, Oxford University Press, Oxford, USA.

Digital 2025: Croatia, dostupno na: https://datareportal.com/reports/digital-2025-croatia, (lipanj 2025.)

Facebook (2025): About us, dostupno na www.facebook.com, (02.06.2025.)

Hlača. S. (2018). Kibernetička sigurnost u hrvatskim medijima: između normativnog i empirijskog. Diplomski rad. Sveučilište u Zagrebu. Filozofski fakultet, Odsjek za sociologiju

Vukasović, A. (1993). Etika i moral osobnosti. Školska knjiga

ETHICS ON SOCIAL NETWORKS

Abstract: Social networks have become an integral part of modern life, revolutionizing the way we communicate, share information, and form relationships. The purpose and goal of the paper is to explore the profound influence of social networks on ethical norms, examining how platforms such as Facebook, Instagram, and YouTube shape the moral behaviour and attitudes of individuals. Therefore, it is necessary to analyze various ethical dilemmas that arise from the use of social networks, including issues of privacy, disinformation, hate speech, and cyberbullying. Special attention is paid to the role of cybersecurity in the context of ethical behaviour on social networks. The paper used descriptive methods, quantitative methods, inductive methods, surveys, and methods of analysis and synthesis. The results of the research aimed at examining the influence of social networks on ethical norms with an emphasis on the role of cybersecurity showed diverse results. On average, respondents did not encounter a breach of personal data, but they were neither convinced nor convinced of recognizing fraud attempts on the Internet, and they were not confident in their information about cybersecurity. The work contributed to the realization that people need to be further educated about the importance of cybersecurity so that they can recognize the threats they will someday encounter.

Keywords: cybersecurity, ethics, social network

Zaprimljen: 12.6.2025.
Odobren za objavu: 23.7.2025.
Prethodno priopćenje

IZGRADNJA OTPORNOSTI PODUZEĆA S OSVRTOM NA POSLOVNE KRIZE U DIGITALNOM DOBU

Lena Sigurnjak[1], Sanja Knežević Kušljić[1], Ivana Sluganović[2]
[1] Sveučilište u Slavonskom Brodu, Trg I. B. Mažuranić 2, 35000 Slavonski Brod, Hrvatska,
ePošta: lsigurnjak@unisb.hr
[1] Sveučilište u Slavonskom Brodu, Trg I. B. Mažuranić 2, 35000 Slavonski Brod, Hrvatska,
ePošta: sknezevic@unisb.hr
[1] Studentica - Sveučilište u Slavonskom Brodu, Trg I. B. Mažuranić 2, 35000 Slavonski Brod, Hrvatska,
ePošta: isluganovic@unisb.hr

Sažetak: Radom se analizira otpornost poduzeća s posebnim naglaskom na poslovne krize u digitalnom dobu. Suočena s nepredvidivim i promjenjivim okruženjem, poduzeća moraju razviti otpornost kako bi se prilagodila tržišnim promjenama i očuvala stabilnost. Teorijski okvir poslovne krize u digitalnom dobu uključuje analizu različitih vrsta poslovnih kriza, jer su krizne situacije jedan od glavnih pokretača neravnoteže na tržištu.
Stoga, svrha rada je da poduzeća moraju adekvatno prilagoditi svoje poslovne strategije kako bi uspješno odgovorili na krizu u kojoj su se našli. Za kvalitetnu prilagodbu kriznim situacijama važno je na vrijeme uočiti problem te razviti poslovne strategije za rješavanje istog. Cilj rada je detaljno obrazložiti opasnosti koje poslovne krize mogu donijeti poduzećima te način na koji digitalizacija poslovanja može utjecati na nastanak krize kao i upravljanje istom. Digitalizacija je sve zastupljenija u poduzećima zbog brojnih prednosti koje donosi poslovanju, stoga je za izgradnju otpornosti poduzeća izuzetno važno uvođenje tehnoloških rješenja i inovacija.
U radu se koriste metode analize, sinteze, indukcije, dedukcije, te deskriptivan metoda za prikaz istraženih pojmova. U istraživačkom djelu rada se provodi istraživanje putem ankete provedeno među 62 ispitanika, a kojim se nastoji istaknuti važnost cyber sigurnost u digitalnom poslovanju te načine na koje se ona može ostvariti.

Ključne riječi: cyber sigurnost, digitalizacija, otpornost, poslovna kriza, tehnologija

1. Uvod

Predmet ovog rada je otpornost poduzeća, odnosno važnost izgradnje otpornosti sustava za uspješno sprječavanje negativnih posljedica poslovne krize. U radu se naglasak stavlja na digitalizaciju sustava koja može pojednostaviti svakodnevne aktivnosti, ali može biti i uzročnik kriznih situacija. Ova tema je izuzetno aktualna za poduzeća jer nastoji istaknuti prednosti digitalizacije sustava te način na koji ona doprinosi izgradnji otpornosti poduzeća. Cilj ovog rada detaljno razložiti i analizirati pojam otpornosti poduzeća, poslovne krize i digitalizacije te prikazati njihov međusobni utjecaj. Za izradu ovog rada bilo je nužno primijeniti niz znanstvenih metoda pomoću kojih se došlo do najrelevantnijih podataka i informacija o navedenom problemu. Najznačajnija metoda je primarno istraživanje kojim se došlo do podataka o strategijama uvođenja digitalizacije poslovanja te načina na koji ona povećava otpornost poduzeća. Budući da krizna situacija, kao i otpornost poduzeća obuhvaća sve dionike unutar poduzeća, metoda dedukcije omogućit će čitatelju sagledavanje šire slike te shvaćanje njihove relevantnosti.

2. Otpornost poduzeća i upravljanje poslovnim rizicima – pregled literature

Poduzeće predstavlja „samostalnu gospodarsku, društvenu i tehničku cjelinu čija je glavna svrha proizvodnja roba i usluga uz racionalnu upotrebu resursa radi ostvarenja dobiti."(Grubišić, 2013., str. 75) Poduzeća organiziraju svoje poslovanje na način da usmjere „prodaju prema maksimalizaciji koristi kako bi ostvarili što veći profit, odnosno kapitalni dobitak" (Benić, 2014., str 7) Može se reći kako su poduzeća generatori poduzetničkih aktivnosti kroz koje poduzetnik razvija svoje ideje i stvara inovacije. Za poduzetnike se stoga može zaključiti kako su oni osobe koje pokreću inovacije i korištenje „tehnologije u poslovanju kako bi unaprijedili postojeću tehnološku strukturu" (Buble, 2006., str. 5) svog poduzeća.

Zbog očuvanja stabilnosti sustava poduzeća najprije moraju „utvrditi vjerojatnost krize, a zatim razmotriti posljedice iste za organizaciju ili mogući učinak na poslovanje." (Tafra-Valović, 2011., str 73) Na taj način poduzeća mogu stvoriti razinu otpornosti koja će im omogućiti neometano poslovanje bez gubitaka.

Organizacijska otpornost važna je kako bi poduzeća osigurala prilagodljivost i sposobnost oporavka dok prolaze kroz poslovne krize, poremećaje ili promjene.(Premiere continuum) Može se zaključiti kako je otpornost poduzeća strateški imperativ za organizacije jer omogućuje poduzećima dugoročno poslovanje i napredovanje, posebice u usporedbi s organizacijama koje ne ulažu u otpornost.

Poduzeća koja ulažu u otpornost poslovanja usmjerena su na „zaštitu i svijest od rizika, konkurentsku prednost, strateško upravljanje te otpornost u opskrbnim lancima." (Reinmoeller, 2005.) Zaštita i svijest o rizicima omogućuju poduzećima pravovremeno prepoznavanje prijetnji te ublažavanje tržišnih rizika putem različitih „internih i eksternih strategija." (Duchek, 2016.)

Organizacijska otpornost se tako sastoji od „faze aktivacije, odgovora i organizacijskog učenja." (Duchek , Raetze, 2019.) Ove faze zapravo predstavljaju životni vijek trajanja otpornosti. „Otpornost ne nastaje nužno kao rezultat krize, ona se može svjesno razvijati" (Karabatić, Skendrović, 2020.) kroz odgovarajuće organizacijske strategije čime postaje ključan resurs za dugoročni uspjeh. Stoga se organizacijska otpornost ne treba shvaćati isključivo kao reakcija na izvanredne okolnosti već kao strateška sposobnost koju treba graditi prije same krizne situacije. Otpornost osigurava poduzećima stabilnost, održava konkurentnost te prilagodljivost dinamičnom poslovnom okruženju.

Organizacijsko učenje jedna je od najvažnijih faza u razvoju otpornosti jer se uočava „djelovanje organizacije u kriznoj situaciji na svim razinama."(Jugo, 2017., str 231) Poduzeća nakon krize trebaju iznova analizirati aktivnosti koje su poduzete u fazi aktivacije i tijekom krize u fazi odgovora, na taj način organizacije se mogu brže prilagoditi i učvrstiti svoju otpornost.

Organizacijska otpornost ne samo da pomaže poduzećima u izlasku iz krize nego „potiče stratešku prilagodbu i korištenje takvih izazova za rast i razvoj organizacijske strukture." (Mancini, 2021.) Organizacije koje prihvaćaju otpornost mogu napredovati, tako što pretvaraju potencijalne slabosti u prilike što osigurava povećanje konkurentske prednosti i dugoročni napredak.

3. Utjecaj digitalizacije na nastanak i upravljanje poslovnom krizom

U digitalnom dobu, otpornost poduzeća poprilično ovisi o njihovoj sposobnosti primjene tehnoloških rješenja koja omogućuju bržu prilagodbu tržišnim promjenama, unapređenje poslovnih procesa i osiguravanje kontinuiteta poslovanja. Osim povećanja brzine u komuniciranju i obavljanju svakodnevnih poslovnih aktivnosti, digitalizacija također povećava sigurnost podataka i

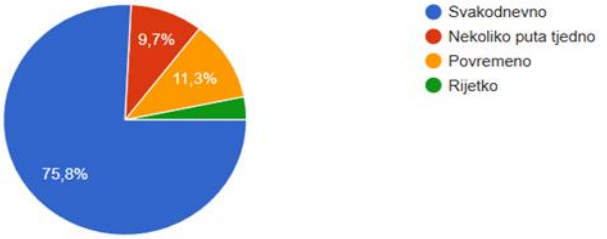
smanjenje operativnih troškova. (Raunaq, 2024.) Sigurnost poslovanja jedan je od temeljnih elemenata otpornosti poduzeća jer se na taj način osigurava zaštita osjetljivih informacija i smanjenje rizika od vanjskih prijetnji posebice kibernetičkih napada. Glavne vrste kibernetičkih napada odnose se na „prijetnje ucjenjivačkim softverom, povrede podataka i probleme sa cloud tehnologijom." (Sprčić, Lacković, str 174) Svaki od navedenih napada može ozbiljno naštetiti povjerljivim podatcima poduzeća te ograničiti njihovu otpornost. Kako bi poduzeća osigurala kvalitetnu implementaciju tehnoloških rješenja potrebno je poduzeti „ključne korake za tehnološku otpornost." (Pozhueva, 2024.) Prvi korak jest prepoznavanje najkritičnijih poslovnih procesa na osnovu kojih se prikuplja i analizira podatke kako bi se procijenila otpornost promatranih elemenata i odredili prioriteti za poboljšanje.

4. Metodologija istraživanja

U ovom poglavlju bit će navedeni i prikazani podatci koji su prikupljeni na temelju anketnog upitnika koji je proveden online. Rezultati istraživanja prikupljeni su putem 62 uzoraka, pri čemu uzorak predstavlja dio osnovnog statističkog skupa koji služi za dobivanje rezultata koji se kasnije može analizirati i prikazati. Anketa je bila sastavljena od slijeda logičnih pitanja pri čemu je korištena Likertova skala putem koje ispitanici mogu izraziti negativan ili pozitivan stav prema nekom od ponuđenih odgovora. Kroz odgovore ispitanika vidljivo je njihovo slaganje, to jest ne slaganjem s određenim pitanjem ili tvrdnjom. Kako bi se ispitanicima pružila mogućnost detaljnijih odgovora, korištena je i Thurstonova skala pomoću koje su se dobili precizniji odgovori i mišljenja ispitanika.

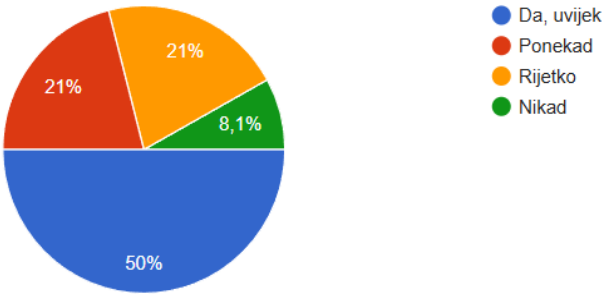
5. Rezultati istraživanja

U istraživanju su sudjelovala 62 ispitanika, od kojih je 21% muškog spola, a 79% ženskog spola. Dobna skupina ispitanika: 48% je u dobi 18-25 godina, ispitanici od 35-45 35-45, te 55 i više godina su najmanje zastupljeni samo 8,1% po razredu, a ispitanici u dobi od 25-35 godina su zastupljeni u postotku od 29%. 58% ispitanika su zaposleni, 35,5% je studentska populacija, a ostali spadaju u populaciju učenika, umirovljenika i nezaposlenih. U nastavku slijedi grafički prikaz podataka.



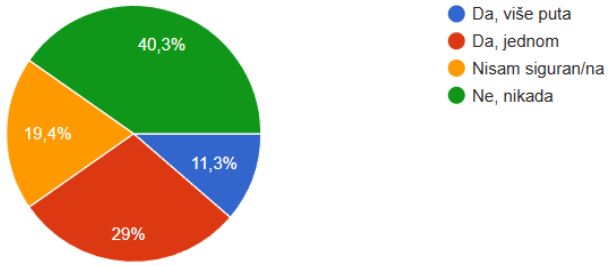
Grafikon 1. razina korištenja internetskih usluga

Grafikon 1. prikazuje razinu korištenja Interneta i internetskih usluga od strane ispitanika. Vidljivo je kako čak 75,8% ispitanika svakodnevno koristi Internet za različite potrebe, dok 11,3% njih Internet koriste povremeno. Najmanji broj ispitanika od svega 3,2% rijetko koriste Internet, a 9,7% koriste usluge nekoliko puta tjedno.



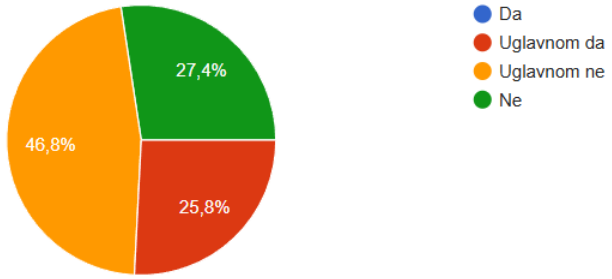
Grafikon 2. Zaštita podataka

Grafikon 2 ukazuje na to kako je broj ispitanika koji su oprezni prilikom korištenja interneta čak 50%, dok njih 42% rijetko ili ponekad štite svoje podatke putem antivirusnih ili drugih softvera. 8,1% ispitanika nikad ne koriste zaštitne softvere na svojim podatcima, stoga postoji povećana opasnost od krađe i zlouporabe osobnih podataka.



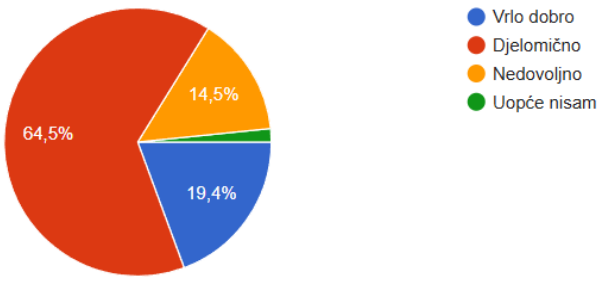
Grafikon 3. Zlouporaba osobnih podataka

Podatci iz grafikona 3. ukazuju na to kako je čak 40 % ispitanika doživjelo krađu ili zlouporabu podataka barem jednom (29%) ili više puta (11,3%). Takvi rezultati upućuju na rastući broj hakera i kradljivaca koji koriste Internet kako bi došli do povjerljivih podataka. Međutim 40% ispitanika nikad se nije susrelo s krađom podataka, bilo radi dobre zaštite ili opreza prilikom dijeljenja istih, dok 19,4% ispitanika nije sigurno jesu li ikad doživjeli zlouporabu osobnih podataka.



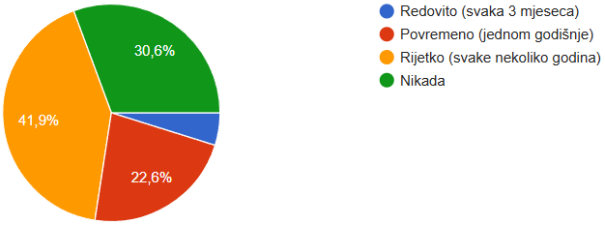
Grafikon 4. Razina sigurnosti podataka na društvenim mrežama

Najveći broj ispitanika, odnosno njih 46,8% slaže se kako online platforme uglavnom ne pružaju dovoljnu sigurnost za osobne podatke, dok 25,8% njih smatra kako su podatci uglavnom sigurni. Prema tome se može zaključiti kako su ispitanici upoznati s rastućim brojem online prijevara te kako se ne osjećaju sigurno prilikom korištenja online platformi i društvenih mreža.



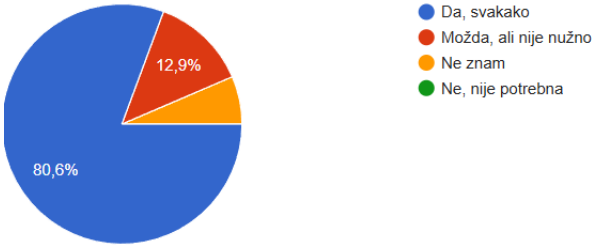
Grafikon 5. Privatnost i zaštita podataka na internetu

Prema podatcima prikazanim na grafikonu 5. može se iščitati kako je većina ispitanika samo djelomično upoznata s zaštitom podataka na internetu (64,5%), dok je njih 19,4% vrlo dobro informirano o navedenoj tematici. 14,5% ispitanika prepoznaje kako su nedovoljno upoznati sa privatnošću i zaštitom podataka, a 1,6% ispitanika uopće nisu upoznati s navedenim. Rezultati ukazuju na to kako su ispitanici u većini samo djelomično svjesni značenja privatnosti i zaštite osobnih podataka te da na tome trebaju poraditi kako bi izbjegli moguće opasnosti.



Grafikon 6. Sigurnosne lozinke

Većina ispitanika svoje sigurnosne lozinke ne mijenjaju nikada (30,6%) ili rijetko (41,9%), odnosno svakih nekoliko godina. 22,6% ispitanika svoje lozinke mijenja na godišnjoj razini, dok samo 4,8% njih mijenja lozinke svaka 3 mjeseca. Ovi rezultati mogu ukazati na to kako su ispitanici previše sigurni u jačinu svojih lozinki te postoji pretpostavka da koriste iste lozinke za više različitih uređaja ili platformi.



Grafikon 7. Edukacija o cyber sigurnosti

Posljednji grafikon odnosi se na edukaciji o cyber sigurnosti, pri čemu je dio ispitanika izrazio kako je edukacija

svakako potrebna (80%), dok su drugi ispitanici neodlučni (6,5%) ili smatraju kako je edukacija poželjna, ali nije nužna (12,9%). Prema rezultatima vidljivo je kako većina ispitanika stavlja edukaciju na prvo mjesto kad je riječ o korištenju interneta i dijeljenju podataka.

6. Rasprava

Na osnovu svega izrečenog prilikom provedenog istraživanja može se zaključiti kako je cyber sigurnost relevantno nov pojam stoga većina ljudi nije u potpunosti upoznata s njegovim značenjem. Međutim s obzirom na to da skoro svi ispitanici svakodnevno koriste internet u različite svrhe, potrebno je povećati svijest o važnosti ove tematike. Može se zaključiti kako je cyber sigurnost zastupljen pojam, ali ima prostora za napredak.

7. Zaključak

Na osnovu rezultata istraživanja može se zaključiti kako je cyber sigurnost relevantno nov pojam stoga većina ljudi nije u potpunosti upoznata s njegovim značenjem. Međutim s obzirom na to da skoro svi ispitanici svakodnevno koriste internet u različite svrhe, potrebno je povećati svijest o važnosti ove tematike. Ono što je važno napomenuti jesu iskustva s krađama identiteta jer je istraživanje pokazalo da je čak 40% ispitanika doživjelo takve situacije jednom ili više puta. Zbog toga je važno educirati se o zaštiti podataka te koristiti različite mjere sigurnosti poput antivirusnih softvera koji će pravovremeno ukazati na potencijalnu opasnost.

8. Literatura

Benić, Đ. (2014). Uvod u ekonomiju, Zagreb, Školska knjiga

Buble, M. (2006). Poduzetništvo: realnost sadašnjost i izazov budućnosti, Split, RRiF-plus d.o.o.

Duchek S., Raetze S.: The Role of Diversity in Organizational Resilience: A Theoretical Framework, (2019.) preuzeto s: https://link.springer.com/article/10.1007/s40685-019-0085-7 Pristupljeno (05.04.2025.)

Duchek S.: Organizational resilience: a capability-based conceptualization, (2019.) preuzeto s: https://link.springer.com/article/10.1007/s40685-019-0085-7 Pristupljeno (05.04.2025.)

Grubišić, D. (2013). *Poslovna ekonomija*, Split, Ekonomski fakultet Sveučilišta u Splitu

Jugo, D. (2017). *Menadžment kriznog komuniciranja*, Zagreb, Školska knjiga

Karabatić, M., Skendrović, K.: Kompetencije zaposlenika kao ključan čimbenik otpornosti poslovanja, (2020.) Preuzeto s: https://dku.hr/wp-content/uploads/2020/10/DKU2020_zbornik-v2.pdf Pristupljeno (08.04.2025.)

Mrnjavac, Ž., Kordić, L., Šimunović, B. (2019). *Osnove ekonomije 2*, Zagreb, ALKA

Osmanagi Bedenik, N.: CRISIS MANAGEMENT: THEORY AND PRACTICE, (2010.) preuzeto s: https://hrcak.srce.hr/file/87513 Pristupljeno (10.04.2025.)

Pozhueva, T.: Digital Innovation for Crisis Management, (2024.). preuzeto s: https://www.researchgate.net/publication/384004881_Digital_technologies_in_crisis_managemen t Pristupljeno (10.05.2025.)

Premiere continuum: What is organizational resilience and why is it important? Preuzeto s: https://www.premiercontinuum.com/resources/organizational-resilience-definition Pristupljeno (02.04.2025.)

Raunaq R.,: Role of Technology in Building Resilient Companies of the Future, (2024.) preuzeto s: https://www.aranca.com/knowledge-library/articles/business-research/role-of-technology-in-building-resilient-companies-of-the-future?utm Pristupljeno (17.04.2025.)

Reinmoeller P.: The Link Between Diversity and Resilience, (2005.), preuzeto s https://www.researchgate.net/publication/40968887_The_Link_Between_Diversity_and_Resilience Pristupljeno (04.04.2025.)

Sprčić Miloš, D, Lacković I.: U*pravljanje rizicima: teorijski koncepti i primjena u poslovnoj praksi,* Zagreb. Naklada SLAP
Tafra-Vlaović, M. (2011). *Upravljanje krizom,* Zaprešić

BUILDING CORPORATE RESILIENCE WITH A FOCUS ON BUSINESS CRISES IN THE DIGITAL AGE

Abstract: The paper analyzes corporate resilience with a special emphasis on business crises in the digital age. Faced with an unpredictable and changing environment, companies must develop resilience in order to adapt to market changes and maintain stability. The theoretical framework of business crises in the digital age includes the analysis of different types of business crises, because crisis situations are one of the main drivers of market imbalance.
Therefore, the purpose of the paper is that companies must adequately adjust their business strategies in order to successfully respond to the crisis they find themselves in. For quality adaptation to crisis situations, it is important to identify the problem in time and develop business strategies to solve it. The aim of the paper is to explain in detail the dangers that business crises can bring to companies and the way in which the digitalization of business can affect the emergence of a crisis as well as its management. Digitization is increasingly common in companies due to the numerous advantages it brings to business, therefore, the introduction of technological solutions and innovations is extremely important for building the resilience of companies.
The paper uses methods of analysis, synthesis, induction, deduction, and a descriptive method to present the researched concepts. In the research part of the work, a survey is conducted among 62 respondents, which aims to highlight the importance of cyber security in digital business and the ways in which it can be achieved.

Keywords: business crisis, cyber security digitization, resilience, technology

Zaprimljen: 10.6.2025.
Odobren za objavu: 23.7.2025.
Pregledni rad

STROJNO UČENJE ZA DETEKCIJU MREŽNE KRAĐE IDENTITETA ANALIZOM URL ADRESA

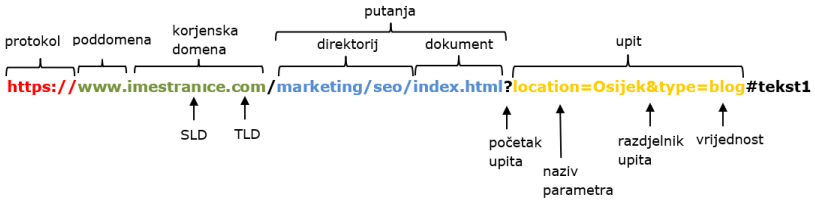
Ivana Hartmann Tolić[1], Mirta Vujnovac[2]
[1] Fakultet elektrotehnike, računarstva i informacijskih tehnologija Osijek, Kneza Trpimira 2b, 31000 Osijek, Hrvatska
[2] III. gimnazija Osijek, Kamila Firingera 14, 31000 Osijek, Hrvatska
ePošta: ivana.hartmann@ferit.hr, mirta.vujnovac@gmail.com

Sažetak: U posljednje vrijeme phishing napadi i mrežne krađe identiteta predstavljaju značajnu prijetnju kibernetičke sigurnosti koristeći lažne web stranice kako bi prevarili korisnike u otkrivanju osjetljivih podataka. Phishing je oblik društvenog inženjeringa u kojem napadači daju pogrešne informacije putem lažnih web stranica kako bi prevarili žrtvu da ustupi osobne podatke radi dobivanja dodatnih informacija ili ostvarivanja financijske koristi. Zbog brzog razvoja tehnologije i taktika krađe identiteta te sve češće razmjene informacija putem interneta, potrebne su učinkovite metode za otkrivanje lažnih URL-ova. Cilj ovog rada bio je procijeniti učinkovitost različitih modela strojnog i dubokog učenja u klasifikaciji zlonamjernih i sigurnih web adresa bez analize sadržaja stranica. Eksperimentalni rezultati pokazuju da konvolucijske neuronske mreže (CNN) mogu postići točnost do 98,7 %, dok ensemble modeli poput Random Foresta i XGBoosta također bilježe visoku točnost iznad 96 %, čime se značajno nadmašuju tradicionalni pristupi poput logističke regresije.
Kako se strategije krađe identiteta nastavljaju razvijati, tako će adaptivni modeli poput ensemble tehnika učenja i arhitektura dubokog učenja biti ključni za zaštitu online sigurnosti te za razumijevanje učinkovitog suzbijanja novonastalih kibernetičkih prijetnji.

Ključne riječi: društveni inženjering, ensemble modeli, kibernetički napadi, klasifikacija URL adresa, SMOTE

1. Uvod

Phishing napadi ubrajaju se među najčešće prijetnje u kibernetičkoj sigurnosti jer iskorištavaju povjerenje korisnika i ranjivosti internetskih protokola. Prema *Anti-Phishing Working Group* (APWG) u četvrtom tromjesečju 2024. godine zabilježeno je 989.123 *phishing* napada, što predstavlja znatan porast u odnosu na prethodna tromjesečja te ukazuje na kontinuirani rast ove prijetnje.
Ovi napadi rabe zavaravajuće URL-ove kako bi žrtve preusmjerili na lažne stranice koje oponašaju legitimne servise. Tradicionalni pristupi obrani, kao što su crne liste i heuristike, ne mogu pratiti dinamične taktike napadača. Primjerice, autori u (Karim et al., 2023) pokazali su učinkovitost hibridnih modela temeljenih na kombinaciji klasičnih klasifikatora i dubokih mreža, dok Khan i suradnici u (Khan et al., 2024) ističu prednost dubokih modela u prepoznavanju skrivenih obrazaca u URL-ovima. Stoga se sve više primjenjuju metode strojnog i dubokog učenja koje na temelju karakteristika URL-a mogu predvidjeti radi li se o legitimnoj ili *phishing* adresi, te svojom učinkovitošću nadilaze tradicionalne metode.



Slika 1: Struktura URL-a s označenim elementima

2. Metodologija

Razvoj pouzdane metode za detekciju *phishing web* stranica zahtijeva pažljivo planiran eksperimentalni okvir koji obuhvaća prikupljanje, obradu, selekciju i modeliranje podataka. Ova faza od ključnog je značaja jer kvaliteta i relevantnost ulaznih značajki izravno utječu na točnost predviđanja. Cilj je metodologije identificirati reprezentativne značajke URL-ova, pravilno pripremiti podatke za algoritme te primijeniti optimalne modele uz preciznu evaluaciju. Analiza se temelji na javno dostupnim skupovima podataka koji sadrže tisuće označenih URL-ova (Slika 1). Svaki je URL predstavljen kao vektor značajki koje uključuju strukturne, simboličke i domenske informacije. Prije treniranja modela provodi se obrada podataka koja uključuje čišćenje i dekodiranje URL znakova, kodiranje kategoriziranih značajki, standardizaciju numeričkih vrijednosti (npr. duljina URL-a), eliminaciju redundantnih značajki korištenjem analiza korelacije i RFE-a (*Recursive Feature Elimination*). Odabir značajki dodatno se provodi pomoću testova značajnosti poput *chi-squared* i ANOVA testa te izračuna informacijske mjere kao što je uzajamna informacija (engl. *mutual information*), čime se osigurava da u model ulaze samo one varijable koje najviše doprinose klasifikaciji (Hajizada & Jahan, 2023). Standardizacija odabira značajki uključuje transformaciju podataka kako bi svi atributi bili u istom rasponu (npr. 0–1) i jednako ponderirani. Time se izbjegava dominacija značajki s većim numeričkim rasponima i omogućuje stabilnije treniranje modela. Zbog neravnoteže između broja *phishing* i legitimnih URL-ova koristi se SMOTE (*Synthetic Minority Over-sampling Technique*) metoda koja generira sintetičke uzorke manjinske klase i tako sprječava pristranost modela (Omari, Taoussi, & Oukhatar, 2025).

2.1. Značajke URL-ova i njihova uloga u detekciji

U analizi *phishing web* stranica značajke URL-ova igraju ključnu ulogu jer zlonamjerne adrese često slijede specifične obrasce dizajnirane kako bi zavarale korisnike. Analizom tih obrazaca moguće je identificirati sumnjive URL-ove bez potrebe za otvaranjem stranice što znatno ubrzava i osigurava proces detekcije.

Jedna od najčešće korištenih skupina značajki strukturne su značajke pri čijoj se analizi ispituju elementi kao što su ukupna duljina URL-a, broj točaka i specijalnih znakova te prisutnost IP adrese umjesto naziva domene. *Phishing* URL-ovi često imaju iznimno dugu strukturu ili sadrže nasumične nizove znakova kako bi prikrili pravi identitet dok je korištenje IP adrese umjesto domene pokušaj da se zaobiđu domenski filtri (Karim et al., 2023).

Druga su važna skupina značajke povezane s domenom uključujući duljinu same domene, broj poddomena, vršnu domenu (TLD – *top-level domain)* i prisutnost HTTPS protokola. *Phishing* adrese često rabe dugačke domene s višestrukim poddomenama kako bi oponašale legitimne *web* stranice.

Također, iako HTTPS protokol implicira sigurnost, zlonamjerne ga stranice često rabe kako bi stekle povjerenje korisnika što znači da prisutnost HTTPS-a sama po sebi nije jamstvo sigurnosti (Hajizada & Jahan, 2023).

Treća su kategorija semantičke značajke koje analiziraju sadržaj samog URL-a, poput prisutnosti riječi kao što su *login*, *verify*, *secure* ili *update*. Ove se riječi često rabe kako bi potaknule korisnika na djelovanje (npr. prijavu ili ažuriranje podataka) i stoga su česte u *phishing* kampanjama. Također se promatra broj ponavljanja znakova jer zlonamjerni URL-ovi ponekad rabe ponavljanje slova ili znakova kako bi vizualno zavarali korisnika (Almomani et al., 2022).

Značajke koje se temelje na WHOIS podatcima, a posebno starost domene i trajanje registracije, dodatno pomažu u prepoznavanju sumnjivih URL-ova. *Phishing* stranice često rabe novoosnovane domene koje su registrirane na kratak period što ih razlikuje od legitimnih *web* stranica koje obično imaju dužu povijest i stabilnu registraciju.

Modeli strojnog učenja s visokom preciznošću temeljem analize značajki URL-ova razlikuju legitimne od zlonamjernih bez potrebe za ulaskom u samu stranicu čime se povećava učinkovitost sustava za detekciju *phishing* napada.

2.2. Klasični modeli

Klasični modeli strojnog učenja već su dugi niz godina temelj pristupa u detekciji phishing napada. Njihova popularnost proizlazi iz jednostavne implementacije, visoke interpretabilnosti rezultata te relativno niskih računalnih zahtjeva što ih čini osobito prikladnima za sustave s ograničenim resursima ili kao polazište u fazama prototipiranja i istraživanja. Kada su podatci uravnoteženi, a značajke kvalitetno odabrane i dobro pripremljene, ovi modeli mogu imati visoku preciznost.

Klasični modeli strojnog učenja, poput logističke regresije, Naivnog Bayesovog klasifikatora i stabla odlučivanja, široko su rabljeni za binarnu klasifikaciju phishing i legitimnih URL-ova. Njihova točnost u recentnim istraživanjima najčešće doseže od 92 % do 96 %, ovisno o izboru značajki i kvaliteti obrade podataka (Alam et al., 2020; Almomani et al., 2022; Omari et al., 2023). Logistička regresija temelji se na linearnoj kombinaciji značajki za procjenu vjerojatnosti pripadnosti klasi, Naivni Bayes pretpostavlja neovisnost značajki dok stabla odlučivanja grade hijerarhijsku strukturu odluka. Iako su ovi modeli interpretabilni i brzi za treniranje, ensemble pristupi poput Random Foresta i Gradient Boostinga u više su radova postigli najvišu točnost, često iznad 96 %, zahvaljujući robusnosti i boljem prepoznavanju složenih obrazaca (Alam et al., 2020; Almomani et al., 2022; Omari et al., 2023). Primjerice, Random Forest je u navedenim istraživanjima redovito ostvarivao točnost od 96 % do 97,7 % dok su Gradient Boosting modeli postizali slične ili nešto više vrijednosti što ih čini najpouzdanijim izborom za detekciju phishing web stranica (Almomani et al., 2022; Omari et al., 2023).

2.3 Modeli temeljeni na dubokom učenju

S obzirom na sve veću složenost obrazaca *phishing* napada i kontinuirani rast količine dostupnih podataka, duboko učenje afirmiralo se kao izuzetno učinkovit pristup za klasifikaciju zlonamjernih URL-ova. Za razliku od tradicionalnih algoritama koji se oslanjaju na ručno definirane značajke, duboki modeli omogućuju automatsko učenje reprezentacija iz podataka čime se otkrivaju kompleksni i nelinearni odnosi među atributima što je osobito važno za detekciju prikrivenih obrazaca karakterističnih za phishing (Khan et al., 2024; Sahingoz et al., 2024).

Ključna prednost dubokih modela leži u njihovoj višeslojnoj arhitekturi koja omogućuje hijerarhijsko učenje značajki. Višeslojni perceptron (MLP) tretira sve

značajke URL-a kao ulazni vektor dok konvolucijske neuronske mreže (*CNN*) prepoznaju lokalne obrasce u nizovima znakova poput neuobičajenih domena ili zamjene slova brojevima što su česti obrasci u phishing adresama (Khan et al., 2024; Sahingoz et al., 2024). Rekurentne neuronske mreže, uključujući LSTM i GRU varijante, posebno su učinkovite u analizi sekvencijalnih podataka omogućujući prepoznavanje semantičkih i sintaktičkih obrazaca duž cijelog URL-a. Autoenkoderi omogućuju nenadzirano učenje komprimiranih reprezentacija URL-ova što može dodatno unaprijediti performanse kasnijih klasifikatora osobito u uvjetima ograničenih označenih podataka.

Empirijska istraživanja dosljedno potvrđuju da duboki modeli, osobito *CNN*, nadmašuju klasične pristupe s točnostima koje dosežu ili premašuju 98 % (Sahingoz et al., 2024; Khan et al., 2024). Unatoč povećanim zahtjevima za količinom podataka i računalnim resursima, njihova sposobnost generalizacije i prilagodbe novim prijetnjama čini ih temeljem suvremenih sustava za detekciju *phishing* napada.

2.4. Ensemble i hibridni modeli

Ensemble i hibridni modeli sve se češće rabe za poboljšanje točnosti, robusnosti i otpornosti sustava za detekciju *phishing* URL-ova. Osnovna je ideja da kombinacija više klasifikatora iskorištava njihove komplementarne prednosti i smanjuje slabosti čime se povećava ukupna učinkovitost modela (Karim et al., 2023).

Ensemble modeli, poput *Random Foresta*, *Gradient Boostinga* i *XGBoosta*, integriraju predikcije više osnovnih klasifikatora u jedinstvenu odluku. *Random Forest* kombinira predviđanja brojnih stabala odlučivanja dok *XGBoost* rabi *boosting* za sekvencijalno ispravljanje pogrešaka prethodnih modela. *Stacking* dodatno rabi predikcije različitih modela kao ulaze za meta-klasifikator čime se postiže dodatna robusnost. Hibridni modeli integriraju različite faze obrade, primjerice koristeći duboke modele (CNN) za automatsku ekstrakciju značajki, a klasične klasifikatore (*Random Forest*, MLP) za završnu odluku (Karim et al., 2023). Iako zahtijevaju više resursa i složeniju validaciju, istraživanja pokazuju da ensemble i hibridni modeli dosljedno nadmašuju pojedinačne pristupe osobito u okruženjima s neuravnoteženim klasama.

3. Rezultati i rasprava

Empirijska analiza potvrđuje da duboki modeli, značajno nadmašuju klasične pristupe u detekciji *phishing* URL-ova. Prema rezultatima Sahingoz i sur. (2024), *CNN* arhitektura postigla je najvišu točnost od 98,74 % na velikom, uravnoteženom skupu od više od pet milijuna URL-ova. RNN i druge duboke arhitekture također su pokazale visoku učinkovitost, ali s nižom točnošću i znatno duljim vremenima treniranja.

Klasični modeli poput logističke regresije i *Random Foresta* i dalje su relevantni zbog nižih računalnih zahtjeva i jednostavnosti implementacije, ali postižu znatno nižu točnost – primjerice, logistička regresija doseže 93,8 %, a *Random Forest* 87,7 % na istom skupu podataka (Sahingoz et al., 2024). Ensemble pristupi poput *XGBoosta* u drugim studijama također pokazuju visoku stabilnost i otpornost na neuravnotežene podatke s točnostima koje često prelaze 97 % (Karim et al., 2023; Omari et al., 2025). Hibridni modeli, koji kombiniraju duboke mreže za ekstrakciju značajki i klasične klasifikatore za završnu odluku, postižu optimalnu ravnotežu između točnosti i učinkovitosti (Karim et al., 2023). Primjena tehnike SMOTE za balansiranje klasa dodatno poboljšava performanse modela osobito u uvjetima neuravnoteženih podataka (Omari et al., 2025).

Analiza eksperimentalnih rezultata pokazuje da ne postoji univerzalno najbolje rješenje – izbor optimalnog

modela ovisi o karakteristikama podatkovnog skupa, dostupnim računalnim resursima i zahtjevima za interpretabilnošću i brzinom izvođenja. Buduća istraživanja trebala bi se usmjeriti na daljnje kombiniranje različitih pristupa i razvoj interpretabilnih sustava temeljenih na umjetnoj inteligenciji (Sahingoz et al., 2024). Usporedba točnosti različitih modela iz relevantne literature prikazana je u (Tablici 1).

Tablica 1. Usporedba točnosti modela prema izvorima iz literature

Model/Metoda	**Točnost**	**Autori**
CNN	98,7	Tang (2021)
Decision Tree	91,9-96,3	Omari (2023) Alam (2020) Karim (2023)
Logistic regression	87,1-98,89	Hajizada (2023) Sahingoz (2024) Tang (2021)
Naive Bayes	54,9-70,34	Khan (2024) Karim (2023) Omari (2025)
Random Forest	87,7-97,1	Alam (2020) Tang (2021) Khan (2024) Karim (2023) Omari (2023) Yang(2021)
Support Vector Machine	60,78-98,85	Hajizada (2023) Omari (2025) Tang (2021)

4. Zaključak

Analiza URL adresa pokazala se kao brz i pouzdan način za rano otkrivanje *phishing web* stranica, osobito kada analiza sadržaja nije moguća ili je preskupa. U radu su uspoređeni klasični i duboki modeli strojnog učenja za detekciju *phishing* URL-ova. Klasični modeli, poput logističke regresije i stabala odlučivanja, prikladni su u okruženjima s ograničenim resursima zbog jednostavnosti, interpretabilnosti i brze implementacije, dok duboke arhitekture poput CNN-a i RNN-a omogućuju prepoznavanje kompleksnih obrazaca i postižu točnost veću od 98 %, što ih čini pogodnim za sustave kojima je prioritet visoka preciznost. Ensemble i hibridni pristupi povećavaju robusnost kombiniranjem prednosti različitih modela. Ove se metode već koriste u komercijalnim sigurnosnim rješenjima kao što su filtri za *e-poštu*, sigurnosni dodaci za preglednike i zaštita korisnika tijekom pretraživanja. Implementacija modela omogućuje automatsku detekciju *phishing* pokušaja u stvarnom vremenu. Ipak, pristupi temeljeni na strojnom učenju suočavaju se s određenim ograničenjima, uključujući pristranost podataka koja može smanjiti učinkovitost na stvarnim, raznolikim URL-ovima, kao i izazove generalizacije na nepoznate vrste napada koji nisu bili zastupljeni u treniranju modela. Stoga je ključno kontinuirano ažurirati skupove podataka i nadzirati performanse modela. Buduća istraživanja trebaju razvijati interpretabilne duboke modele i multimodalne pristupe koji kombiniraju

URL analizu s dodatnim podacima poput DNS zapisa i WHOIS informacija, čime bi se izgradili otporniji i skalabilniji sustavi za prevenciju *phishing* napada u stvarnom vremenu. Posebno je važno ugraditi etička načela u dizajn i korištenje sustava strojnog učenja kako bi se osigurala transparentnost, pravednost i zaštita privatnosti korisnika, čime se jača povjerenje u pouzdanost rješenja za kibernetičku sigurnost.

5. Literatura

Alam, M. N., Sarma, D., Lima, F. F., Saha, I., Ulfath, R.-E., & Hossain, S. (2020). Phishing attacks detection using machine learning approach. In 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT) (pp. 1173–1179). IEEE. https://doi.org/10.1109/ICSSIT48917.2020.9214225

Almomani, A., Alauthman, M., Shatnawi, M. T., Alweshah, M., Alrosan, A., Alomoush, W., & Gupta, B. B. (2022). Phishing website detection with semantic features based on machine learning classifiers: a comparative study. International Journal on Semantic Web and Information Systems (IJSWIS), 18(1), 1-24.

Hajizada, A., & Jahan, S. (2023, February). Feature selections for phishing urls detection using combination of multiple feature selection methods. In Proceedings of the 2023 15th International Conference on Machine Learning and Computing (pp. 444-450).

Karim, A., Shahroz, M., Mustofa, K., Belhaouari, S. B., & Joga, S. R. K. (2023). Phishing detection system through hybrid machine learning based on URL. IEEE Access, 11, 36805-36822.

Khan, M. A., et al. (2024). Phishing website detection using deep learning models. Information Security Journal, 33(1), 12–28.

Omari, K. (2023). Comparative study of machine learning algorithms for phishing website detection. International Journal of Advanced Computer Science and Applications, 14(9).

Omari, K., Taoussi, C., & Oukhatar, A. (2025). Comparative Analysis of Undersampling, Oversampling, and SMOTE Techniques for Addressing Class Imbalance in Phishing Website Detection. International Journal of Advanced Computer Science & Applications, 16(2).

Sahingoz, O. K., BUBE, E., & Kugu, E. (2024). Dephides: Deep learning based phishing detection system. IEEE Access, 12, 8052-8070.

Tang, L., & Mahmoud, Q. H. (2021). A deep learning-based framework for phishing website detection. IEEe Access, 10, 1509-1521.

Yang, R., Zheng, K., Wu, B., Wu, C., & Wang, X. (2021). Phishing website detection based on deep convolutional neural network and random forest ensemble learning. Sensors, 21(24), 8281.

MACHINE LEARNING APPROACHES FOR PHISHING DETECTION BASED ON URL ANALYSIS

Abstract: Phishing attacks have posed a significant threat to cybersecurity in recent years. Phishing is a form of social engineering in which attackers provide misleading information via fake websites in order to trick the victim into disclosing private information to obtain further information or gain a financial advantage. With the rapid development of technology and phishing tactics, access to information and the frequent exchange of information, effective methods for detecting fake URLs are needed. The goal is to evaluate the effectiveness of different models in classifying malicious and legitimate web addresses without analyzing the content of the page. This study aimed to evaluate the effectiveness of various machine learning and deep learning models in classifying malicious and legitimate web addresses without analyzing page content. Experimental results show that convolutional neural networks (CNNs) can achieve accuracy rates of up to 98.7%, while ensemble models such as Random Forest and XGBoost also demonstrate high accuracy, exceeding 96%, significantly outperforming traditional approaches like logistic regression.
As phishing strategies continue to evolve, adaptive models such as ensemble learning techniques, deep learning architectures will be fundamental to securing online security and crucial to understanding how to effectively counter emerging cybersecurity threats.

Keywords: Cyber attacks, Ensemble models, SMOTE, Social engineering, URL classification

Zaprimljen: 9.6.2025.
Odobren za objavu: 23.7.2025.
Stručni rad

SIGURNOSNI IZAZOVI IoT UREĐAJA

Ivan Matasović [1], Mato Galović [2], Mato Kokanović [3], Zoran Crnac [4]
[1] Tehnička škola, Eugena Kumičića 55, Slavonski Brod 35000, Republika Hrvatska, imatasovic@unisb.hr
[2] Tehnička škola, Eugena Kumičića 55, Slavonski Brod 35000, Republika Hrvatska, mgalovic@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: Internet stvari (IoT) predstavlja sveprisutnu tehnologiju modernog doba koja omogućuje međusobnu komunikaciju uređaja i razmjenu podataka putem interneta. S obzirom na sve širu primjenu u pametnim kućama, industriji i kritičnoj infrastrukturi, sigurnost IoT uređaja postaje ključno pitanje. Zbog svoje povezanosti i često nedovoljne razine zaštite, IoT uređaji predstavljaju značajnu metu za različite oblike kibernetičkih napada.
Cilj ovog rada je analizirati osnovne prijetnje koje se odnose na sigurnost IoT uređaja, identificirati ranjivosti, te prikazati moguće metode zaštite i dobre prakse u području kibernetičke sigurnosti. U sklopu praktičnog dijela rada provedeno je testiranje sigurnosti jedne pametne WiFi kamere, kako bi se kroz konkretan primjer pokazale potencijalne slabosti i načini zaštite.
Rad donosi pregled aktualnih sigurnosnih prijetnji, metode sigurnosnog testiranja, kao i prijedloge tehničkih i organizacijskih mjera zaštite u skladu s relevantnim sigurnosnim standardima.

Ključne riječi: Internet stvari, IoT, kibernetička sigurnost, WiFi kamera, ranjivosti, sigurnosno testiranje

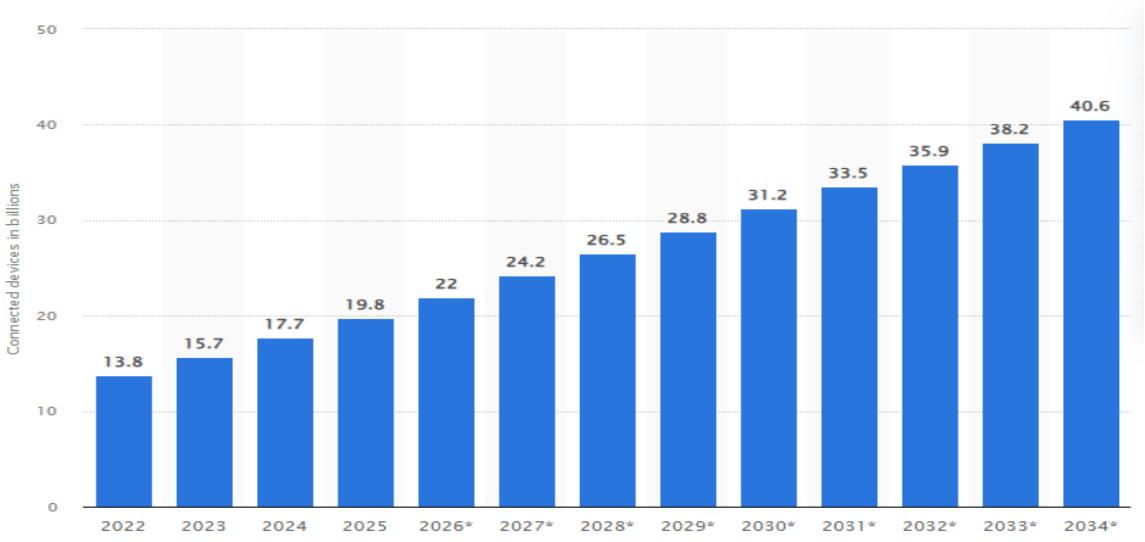
1. Uvod

Internet stvari (Internet of Things, IoT) predstavlja mrežu fizičkih uređaja opremljenih senzorima, softverom i mogućnostima povezivanja putem interneta radi razmjene podataka i upravljanja. Među najraširenijim IoT uređajima nalaze se Wi-Fi nadzorne kamere koje se koriste u pametnim domovima, poslovnim prostorima i industrijskim okruženjima (Sicari i sur., 2015). Iako omogućuju jednostavan i pristupačan videonadzor, sve je veća zabrinutost zbog sigurnosnih rizika koje takvi uređaji predstavljaju.
Prethodna istraživanja pokazala su da mnogi IoT uređaji, uključujući Wi-Fi kamere, često sadrže značajne softverske i hardverske ranjivosti, kao što su nezaštićeni pristupni portovi, slaba enkripcija, korištenje zadano postavljenih lozinki i nepostojanje mehanizama za ažuriranje (Alrawi i sur., 2019). U kombinaciji s činjenicom da su ovi uređaji stalno spojeni na internet, čak i manji propusti mogu rezultirati ozbiljnim kompromitiranjem privatnosti korisnika ili omogućavanjem udaljenog pristupa napadačima (Roman i sur., 2011).
Cilj ovog rada je istražiti i testirati softverske i hardverske ranjivosti konkretne Wi-Fi kamere, kako bi se utvrdila razina njezine sigurnosti. Fokus je stavljen na identifikaciju potencijalno iskoristivih propusta, analizu načina

njihove zloupotrebe i izradu prijedloga za poboljšanje sigurnosti uređaja.
Zadaće koje vode prema ostvarenju ovog cilja uključuju:

- Analizu poznatih sigurnosnih problema povezanih s Wi-Fi nadzornim kamerama;
- Istraživanje specifikacija i arhitekture testiranog modela;
- Provođenje testova sigurnosti softvera (firmware, mrežni servisi, API sučelja);
- Analizu fizičkog sklopa i mogućih hardverskih ulaznih točaka (npr. UART, JTAG);
- Izradu tehničkog izvještaja s preporukama za unaprjeđenje sigurnosti.

Iako je problem sigurnosti IoT uređaja prepoznat u znanstvenoj i industrijskoj zajednici, u praksi i dalje postoji velik broj nesigurnih proizvoda na tržištu. U ovom radu istražuje se konkretan primjer kako bi se na praktičan način ilustrirala širina i ozbiljnost prijetnji koje proizlaze iz nedostatne zaštite Wi-Fi nadzornih uređaja.
Trenutno se procjenjuje da postoji oko 17 milijardi povezanih IoT uređaja, s projekcijama koje predviđaju rast na 22 milijardi do 2026. godine i gotovo 32 milijardi do 2030. godine (https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/). Ovaj rast potaknut je sve većom integracijom IoT rješenja u svakodnevni život i industrijske procese. U kućanstvima, pametni uređaji poput Wi-Fi kamera, termostata i kućanskih aparata postaju sve prisutniji, dok industrijski sektor koristi IoT za optimizaciju proizvodnje, održavanja i logistike.



Slika 1. Broj spojenih IoT uređaja i predikcija za naredne godine (izvor: Statista 2025)

2. Sigurnosne prijetnje u IoT okruženju

U ovome poglavlju opisat ćemo ranjivosti, prijetnje i napade na IoT uređaje. Ranjivosti IoT uređaja možemo podijeliti na četiri kategorije (Mukhtar i sur., 2023):

- Ranjivosti uzrokovane korisničkim rukovanjem
- komunikacijske ranjivosti
- ranjivosti firmwarea i softwarea
- fizička ranjivost uređaja

Što se tiče ranjivosti uzrokovane korisničkim rukovanjem tu se misli na slabe lozinke i zanemarivanje ažuriranja. Mnogi IoT uređaji dolaze s unaprijed postavljenim i jednostavnim lozinkama (Li i Da Xu, 2017), što predstavlja ozbiljan sigurnosni rizik. Iako se preporučuje njihova promjena pri prvom

korištenju, korisnici tu uputu često zanemaruju ili lozinke zamijene lako pamtljivim, ali slabim kombinacijama. Takav pristup značajno povećava rizik od neovlaštenog pristupa i kompromitacije uređaja.

Dodatni problem predstavlja ignoriranje sigurnosnih ažuriranja. Iako proizvođači povremeno izdaju nadogradnje kojima se ispravljaju poznate ranjivosti, korisnici ih često ne instaliraju. Kada se ta ažuriranja dulje vrijeme sustavno izbjegavaju, uređaji ostaju nezaštićeni od poznatih prijetnji, čime se otvara prostor za iskorištavanje propusta putem zlonamjernog softvera ili ciljanih napada.

Uporaba nesigurnih komunikacijskih protokola predstavlja komunikacijsku ranjivost. U IoT okruženjima uređaji su često međusobno povezani unutar iste lokalne mreže, što znači da kompromitacija jednog uređaja može omogućiti širenje napada i na ostale povezane komponente sustava. Ovakva povezanost povećava rizik od lateralnog kretanja napadača unutar mreže.

Dodatno, zbog ograničenih resursa (procesorske snage, memorije i potrošnje energije), proizvođači često odabiru mrežne protokole koji nude bolje performanse i manji zahtjev za resursima, ali uz kompromis u sigurnosti. Takvi protokoli mogu sadržavati ranjivosti koje otvaraju vrata potencijalnim napadima.

Stoga je nužno pronaći ravnotežu između učinkovitog korištenja dostupnih resursa i implementacije sigurnosnih mehanizama koji mogu zaštititi uređaje i podatke u mreži od zlonamjernih aktivnosti (Li i Da Xu, 2017)

Komunikacijsku ranjivost može uzrokovati i nedostatak enkripcije tijekom prijenosa podataka. Sigurnost IoT sustava u velikoj mjeri ovisi o zaštiti podataka koje prikupljaju senzori na sloju percepcije. Korištenjem enkripcije moguće je zaštititi prijenos podatkovnih paketa i spriječiti neovlašteni pristup osjetljivim informacijama.

Ipak, mnogi IoT uređaji komuniciraju putem nepouzdanih bežičnih medija, a zbog ograničenih hardverskih resursa često nisu u mogućnosti implementirati snažne kriptografske algoritme. Kao rezultat, podaci se ponekad prenose u nešifriranom obliku, što ih čini ranjivima na presretanje, manipulaciju ili neovlašteni pristup (Anand i sur., 2020). Takva ograničenja čine ove uređaje posebno osjetljivima na napade usmjerene na krađu podataka i narušavanje privatnosti korisnika, što dodatno naglašava potrebu za sigurnosno svjesnim dizajnom već u fazi razvoja IoT sustava.

Još jednu vrstu ranjivosti je potrebno spomenuti, a to je ranjivost firmwarea i softwarea. Sigurnost IoT sustava u velikoj mjeri ovisi o pouzdanosti firmwarea i softvera koji omogućuju komunikaciju između hardverskih komponenti i aplikacijskih slojeva. Firmware, kao temeljna programska podrška pohranjena u trajnoj memoriji uređaja, ključan je za njegovo osnovno funkcioniranje. Međutim, mnogi IoT uređaji ne primaju redovita ažuriranja, što ih čini ranjivima na napade koji iskorištavaju poznate sigurnosne propuste. Za razliku od tradicionalnih IT sustava, IoT uređaji često ostaju bez podrške za sigurnosne nadogradnje, čime se povećava vjerojatnost kompromitacije.

Dodatnu prijetnju predstavlja način na koji se nadogradnje provode. U slučajevima kada uređaji koriste nesigurne ili neprovjerene mehanizme ažuriranja, postoji rizik od instalacije zlonamjernog softvera putem korumpiranih datoteka. Takve situacije mogu dovesti do potpunog preuzimanja kontrole nad uređajem, što ima ozbiljne posljedice i za privatne korisnike i za poslovne sustave. Kako bi se izbjegle takve prijetnje, važno je koristiti digitalno potpisana ažuriranja i distribuirati ih preko sigurnih, enkriptiranih kanala.

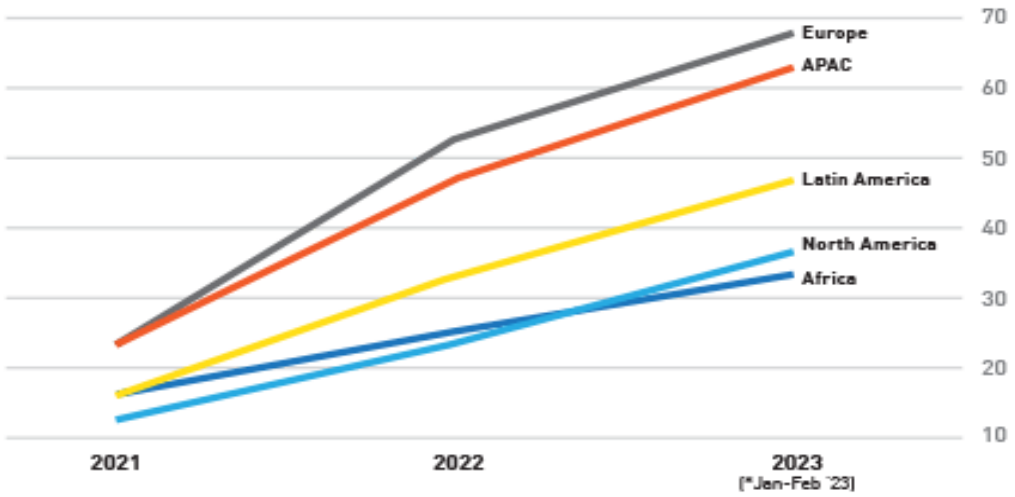
Uz ranjivosti povezane s firmwareom i softverom, značajnu prijetnju predstavljaju i nesigurna web sučelja koja se često koriste za upravljanje IoT uređajima. Ova sučelja ponekad

uključuju slabu autentifikaciju i autorizaciju, što omogućava neovlaštenim osobama pristup osjetljivim funkcijama uređaja. Dodatno, izostanak HTTPS protokola omogućuje presretanje i manipulaciju podacima tijekom prijenosa. Uređaji koji nemaju zaštitu od ponavljanih pokušaja prijave posebno su osjetljivi na napade, čime se dodatno povećava rizik od kompromitacije.
Kombinacija nepouzdanog firmwarea, rijetkih ili nesigurnih ažuriranja i ranjivih web sučelja čini IoT sustave atraktivnim metama za napadače. Stoga je nužno već u fazi dizajna osigurati provjerene sigurnosne mehanizme, kontinuirano održavanje softvera i jasno definirane sigurnosne protokole za upravljanje uređajima.
Fizička sigurnost predstavlja ključni, ali često zanemareni aspekt zaštite IoT sustava. Za razliku od serverskih ili mrežnih komponenti koje se nalaze u zaštićenim prostorima, mnogi IoT uređaji instalirani su na lako dostupnim lokacijama — u kućama, na ulicama, industrijskim postrojenjima ili prometnoj infrastrukturi — što ih čini izloženima fizičkim prijetnjama. Napadač koji fizički pristupi IoT uređaju može izvršiti niz potencijalno destruktivnih ili špijunskih aktivnosti.

Jedan od najčešćih rizika fizičkog pristupa je mogućnost povezivanja s dijagnostičkim sučeljima kao što su UART ili JTAG. Preko tih portova moguće je izravno komunicirati s uređajem, čitati i mijenjati firmware, zaobići autentifikacijske mehanizme ili čak zamijeniti originalni firmware zlonamjernim inačicama. Ovakvi napadi mogu rezultirati potpunim preuzimanjem kontrole nad uređajem bez potrebe za mrežnim iskorištavanjem ranjivosti.

Također, fizički pristup omogućuje napadaču vađenje pohranjenih podataka iz memorije uređaja, uključujući osjetljive informacije poput lozinki, autentifikacijskih tokena ili kriptografskih ključeva. Ako uređaj ne koristi enkripciju memorije, podaci su lako dostupni i mogu se zloupotrijebiti za daljnje napade.

Još jedna prijetnja odnosi se na manipulaciju samim komponentama uređaja. Napadač može fizički onesposobiti senzore, zamijeniti ih ili preusmjeriti njihove ulazne/izlazne signale, što može dovesti do krivih očitanja, donošenja pogrešnih odluka u sustavu ili lažnih alarma. U nekim slučajevima moguće je ugraditi dodatni mikroupravljač ili špijunski modul koji neprimjetno bilježi komunikaciju ili manipulira podatkovnim tokovima (ENISA, 2019)



Slika 2. Porast napada na IoT uređaje (izvor: Check Point Research, 2023)

Na slici 2. se može vidjeti da je Europa trenutno regija koja trpi najviše napada usmjerenih na IoT uređaje, s prosjekom od gotovo 70 takvih napada po organizaciji tjedno. Slijedi regija Azija-Pacifik s 64 napada, Latinska Amerika s 48, Sjeverna Amerika s 37 (uz najveći porast u odnosu na 2022. godinu – 58%) te Afrika s 34 tjedna IoT kibernetička napada po organizaciji (Check Point Research, 2023).

3. Metodologija sigurnosnog testiranja

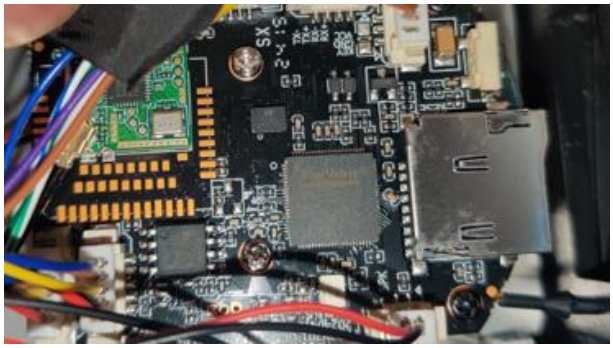
Za testiranje korištena je jedna bežična kamera bez vidljive oznake proizvođača kao što se može vidjeti na slici ispod.

Slika 3. Korištena Wi-Fi kamera za testiranje

Sigurnosno testiranje Wi-Fi kamere provedeno je kroz dva glavna segmenta: hardversko testiranje i softversko testiranje. Ovim pristupom cilj je detaljno identificirati ranjivosti i sigurnosne nedostatke kako na fizičkoj i firmware razini, tako i u mrežnoj komunikaciji uređaja.

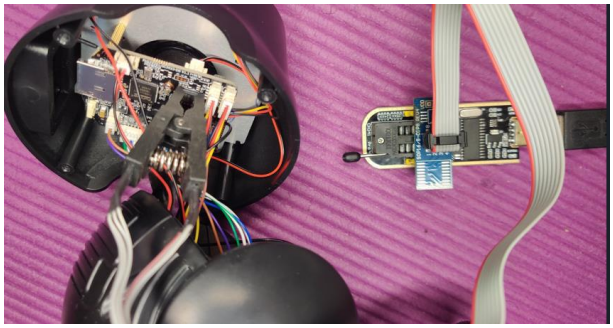
3.1. Hardversko testiranje

Ovo testiranje fokusira se na analizu fizičkih komponenti uređaja i njegove interne programske podrške (firmwarea), s ciljem otkrivanja mogućih sigurnosnih propusta koji proizlaze iz hardverske konstrukcije i implementacije. Prvi korak bio je pažljivo otvaranje kućišta kamere i detaljna inspekcija tiskanih pločica (PCB). Identificirani su ključni čipovi kao što su mikrokontroler, memorijski čipovi i Wi-Fi modul. Fotografiranjem i bilježenjem oznaka omogućena je daljnja analiza proizvođača i modela komponenti, kao i njihova tehnička specifikacija.

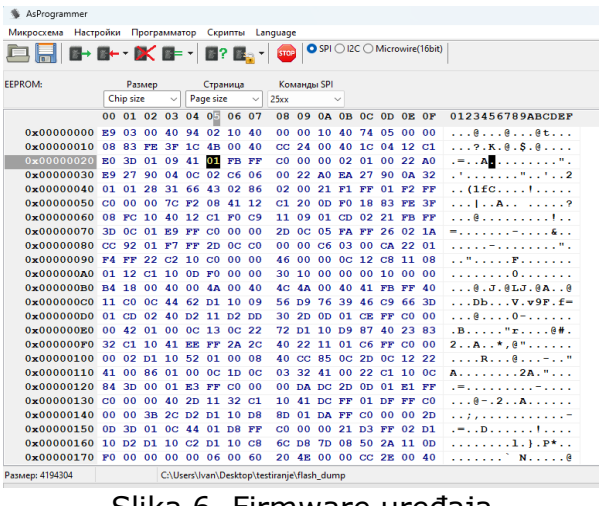


Slika 4. PCB pločica rastavljene kamere

Kamera koristi FH885V201 integrirani krug (SoC) koji ima ugrađeni audio/video podršku, USB podršku, CPU, memoriju, Wi-Fi modul te EEPROM integrirani krug s oznakom FM25Q128A. U EEPROM-u se nalazi firmware uređaja te ga korištenjem specijalizirane opreme možemo „izvući" iz uređaja te detaljnije analizirati kao što je prikazano na slici ispod.

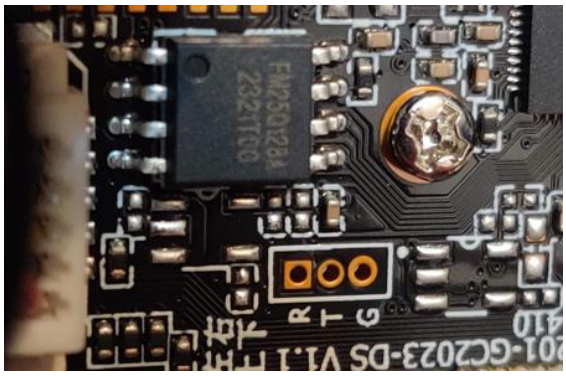


Slika 5. „Izvlačenje" firmwarea uređaja



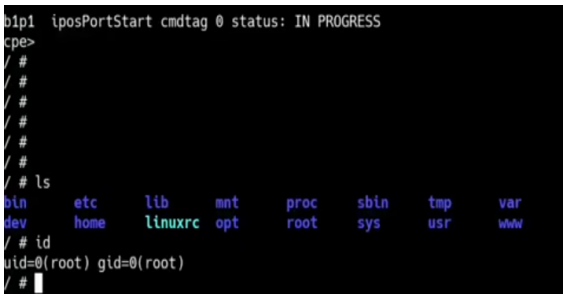
Slika 6. Firmware uređaja

Kada je firmware na raspolaganju može se detaljnije analizirati alatima poput binwalk. U firmwareu se može naći lozinke, SSH/Telnet pristup, web sučelja itd.
Još se može primijetiti pristup serijskoj konzoli, proizvođač nam je olakšao dodatnon pristup time što je označio pinove: R (receive), T (transmit), G (ground).



Slika 7. Pristup serijskoj konzoli

Istom opremom koju smo koristili da dođemo do firmwarea možemo iskoristiti da gledamo tzv. boot poruke i dođemo do root pristupa.



Slika 8. Glavni (root) pristup

3.2. Softversko testiranje

Softversko testiranje fokusira se na analizu mrežnog prometa uređaja i njegove interakcije s ostalim komponentama mreže, s ciljem identificiranja ranjivosti u protokolima i prijenosu podataka. Korištenjem alata Wireshark (verzija 3.4.8) snimljen je promet koji Wi-Fi kamera generira tijekom različitih operacija (povezivanje, prijenos videa, komunikacija s aplikacijom ili oblakom). Analiza snimljenog prometa obuhvatila je provjeru korištenja sigurnih protokola, prisutnost nezaštićenih ili nešifriranih prijenosa, te potencijalne napade presretanja ili manipulacije podacima.
Prilikom snimanja mrežnog prometa s u Wiresharku (verzija 3.4.8) mogu se uočiti sljedeće vrste komunikacije:

- Nešifrirani protokoli i običan tekst: HTTP i RTSP bez enkripcije
- Korištenje zastarjelih ili nesigurnih protokola: Telnet

4. Rezultati i rasprava

U ovom istraživanju korištena je bežična Wi-Fi kamera nepoznatog proizvođača, čije kućište i unutarnji sklop predstavljaju tipičan primjer jeftinijih IoT uređaja na tržištu. Sigurnosno testiranje uređaja provedeno je kroz dva komplementarna segmenta, hardversko i softversko testiranje, s ciljem što detaljnijeg otkrivanja sigurnosnih ranjivosti. Otvaranjem kućišta i analizom tiskane pločice identificirani su ključni hardverski elementi uređaja, među kojima se ističe integrirani krug FH885V201, koji obuhvaća procesorsku jedinicu, Wi-Fi modul, audio/video podršku i memoriju. Također je prisutan EEPROM s firmwareom uređaja, koji je uspješno „izvučen" korištenjem specijalizirane opreme.
Pristup serijskoj konzoli dodatno je olakšan fizičkim označavanjem pinova za primanje (R), prijenos (T) i masu (G), što je omogućilo nadzor boot poruka i stjecanje root pristupa uređaju. Ovakva razina pristupa potvrđuje mogućnost fizičkog iskorištavanja ranjivosti na firmware razini, što ukazuje na slabosti u zaštiti uređaja protiv neovlaštenog pristupa.
Softverska analiza usmjerena je na mrežni promet generiran od strane kamere tijekom različitih funkcionalnosti poput povezivanja, prijenosa video zapisa i komunikacije s upravljačkim aplikacijama ili oblakom. Korištenjem Wiresharka detektirani su različiti protokoli, među kojima su istaknuti nešifrirani protokoli poput HTTP i RTSP koji se koriste bez adekvatne enkripcije.

Također je uočeno korištenje zastarjelih i nesigurnih protokola poput Telneta, što dodatno ugrožava sigurnost uređaja.

5. Zaključak

Internet stvari (IoT) značajno mijenja način na koji upravljamo svakodnevnim uređajima, uključujući i Wi-Fi nadzorne kamere, koje su sveprisutne u kućanstvima i industriji. Međutim, provedeno istraživanje i testiranje konkretne Wi-Fi kamere otkrilo je brojne sigurnosne ranjivosti, kako na hardverskoj tako i na softverskoj razini. Slaba zaštita pristupnih portova, prisutnost nešifriranih komunikacijskih protokola te lakoća stjecanja root pristupa putem fizičkog priključka ukazuju na ozbiljne sigurnosne propuste. Ovi nalazi potvrđuju da nedostatna zaštita IoT uređaja može ugroziti privatnost korisnika i sigurnost mrežnih sustava. Stoga je nužno da proizvođači unaprijede sigurnosne mehanizme, redovito izdaju i implementiraju ažuriranja te educiraju korisnike o sigurnosnim praksama, kako bi se smanjili rizici od kibernetičkih napada u rastućem IoT ekosustavu.

6. Literatura

Alrawi, O., Lever, C., Antonakakis, M., & Monrose, F. (2019). SoK: Security Evaluation of Home-Based IoT Deployments. IEEE Symposium on Security and Privacy. https://doi.org/10.1109/SP.2019.00031

Anand, P., Singh, Y., Selwal, A., Alazab, M., Tanwar, S., Kumar, N. (2020). IoT vulnerability assessment for sustainable computing: threats, current solutions, and open challenges. IEEE Access, 8, 168825-168853, https://ieeexplore.ieee.org/document/9189773

Check Point Research, https://blog.checkpoint.com/security/the-tipping-point-exploring-the-surge-in-iot-cyberattacks-plaguing-the-education-sector/

ENISA. (2019). Good Practices for Security of Internet of Things in the context of Smart Manufacturing. European Union Agency for Cybersecurity, https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot

Li, S., Da Xu, L. (2017). Securing the internet of things. Syngress.

Mukhtar, B. I., Elsayed, M. S., Jurcut, A. D., Azer, M. A. (2023). IoT vulnerabilities and attacks: SILEX malware case study, https://www.mdpi.com/2073-8994/15/11/1978

Roman, R., Najera, P., & Lopez, J. (2011). Securing the Internet of Things. Computer, 44(9), 51–58. https://doi.org/10.1109/MC.2011.291

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer Networks, 76, 146–164. https://doi.org/10.1016/j.comnet.2014.11.008

Statista.com, https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

SECURITY CHALLENGES OF IoT DEVICES

Summary: The Internet of Things (IoT) represents a ubiquitous modern technology that enables communication between devices and the exchange of data via the internet. Given its widespread use in smart homes, industry, and critical infrastructure, the security of IoT devices has become a key concern. Due to their connectivity and often insufficient levels of protection, IoT devices are a significant target for various forms of cyberattacks.
The aim of this paper is to analyze the main threats related to the security of IoT devices, identify vulnerabilities, and present possible protection methods and best practices in the field of cybersecurity. As part of the practical section, a security test was conducted on a smart WiFi camera to demonstrate potential weaknesses and methods of protection through a concrete example.
This paper provides an overview of current security threats, methods of security testing, and offers proposals for technical and organizational protection measures in accordance with relevant security standards.

Keywords: Internet of Things, IoT, cybersecurity, WiFi camera, vulnerabilities, security testing

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)

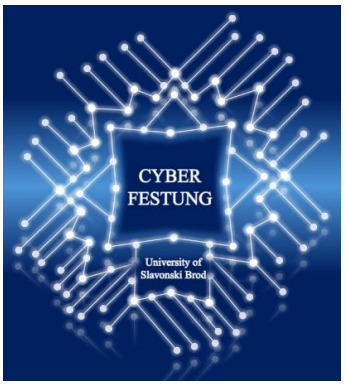
11pt
Opseg rada u pravilu bi trebao biti od 4 do 6 stranica, uključujući tekst, crteže, tablice, dijagrame, fotografije sa popisom literature bez priloga.
11pt
Tekst pisanog dijela rada treba pisati u dva stupca, Verdana 11, jednostruki prored kao što je pisan i ovaj tekst. Rečenice trebaju biti stručno 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

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

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